ID: 357103
Sample Name: PO AAN2102002-V020.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:57:17
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

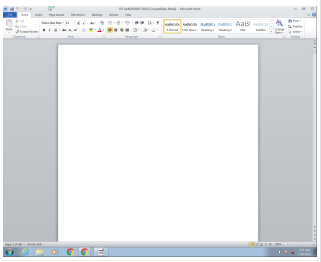
Analysis Report PO AAN2102002-V020.doc

Overview

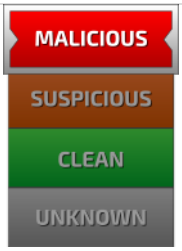
General Information

Sample Name:	PO AAN2102002-V020.doc
Analysis ID:	357103
MD5:	71e541e756ee25..
SHA1:	f7f6c91b2673d88..
SHA256:	b3104dab0a4fd15.
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



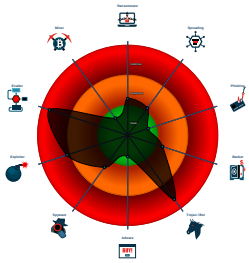
Nanocore GuLoader

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

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e…
- Yara detected GuLoader
- Yara detected Nanocore RAT
- Connects to a URL shortener service
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 252 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 1204 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - 69577.exe (PID: 896 cmdline: C:\Users\Public\69577.exe MD5: ACFCBD916FA04787E4388B339592DD78)
    - RegAsm.exe (PID: 2428 cmdline: C:\Users\Public\69577.exe MD5: 246BB0F8D68A463FD17C235DEB5491C0)
      - schtasks.exe (PID: 2988 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp1A35.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - schtasks.exe (PID: 2980 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp678.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- taskeng.exe (PID: 1688 cmdline: taskeng.exe {DA6299CA-95CA-4E9D-8945-2CC05321254C} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - smtpsvc.exe (PID: 2380 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0 MD5: 246BB0F8D68A463FD17C235DEB5491C0)
- filename1.exe (PID: 2152 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: ACFCBD916FA04787E4388B339592DD78)
- smtpsvc.exe (PID: 2500 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' MD5: 246BB0F8D68A463FD17C235DEB5491C0)
- filename1.exe (PID: 1480 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: ACFCBD916FA04787E4388B339592DD78)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2342821040.00000000005 62000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2342294404.00000000000 80000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000005.00000002.2342294404.00000000000 80000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000005.00000002.2342304047.00000000000 90000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000005.00000002.2342304047.00000000000 90000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.RegAsm.exe.80000.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
5.2.RegAsm.exe.80000.0.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
5.2.RegAsm.exe.90000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
5.2.RegAsm.exe.90000.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
5.2.RegAsm.exe.90000.2.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 6 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

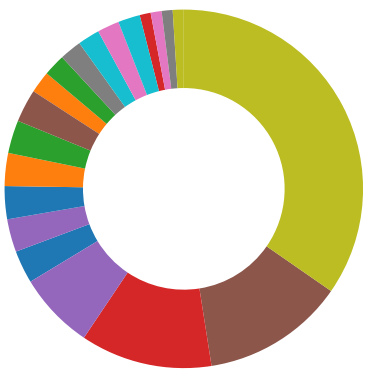
Sigma detected: Scheduled temp file as task from temp location

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
- Spreading
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Exploits:

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

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

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

Connects to a URL shortener service

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

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:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

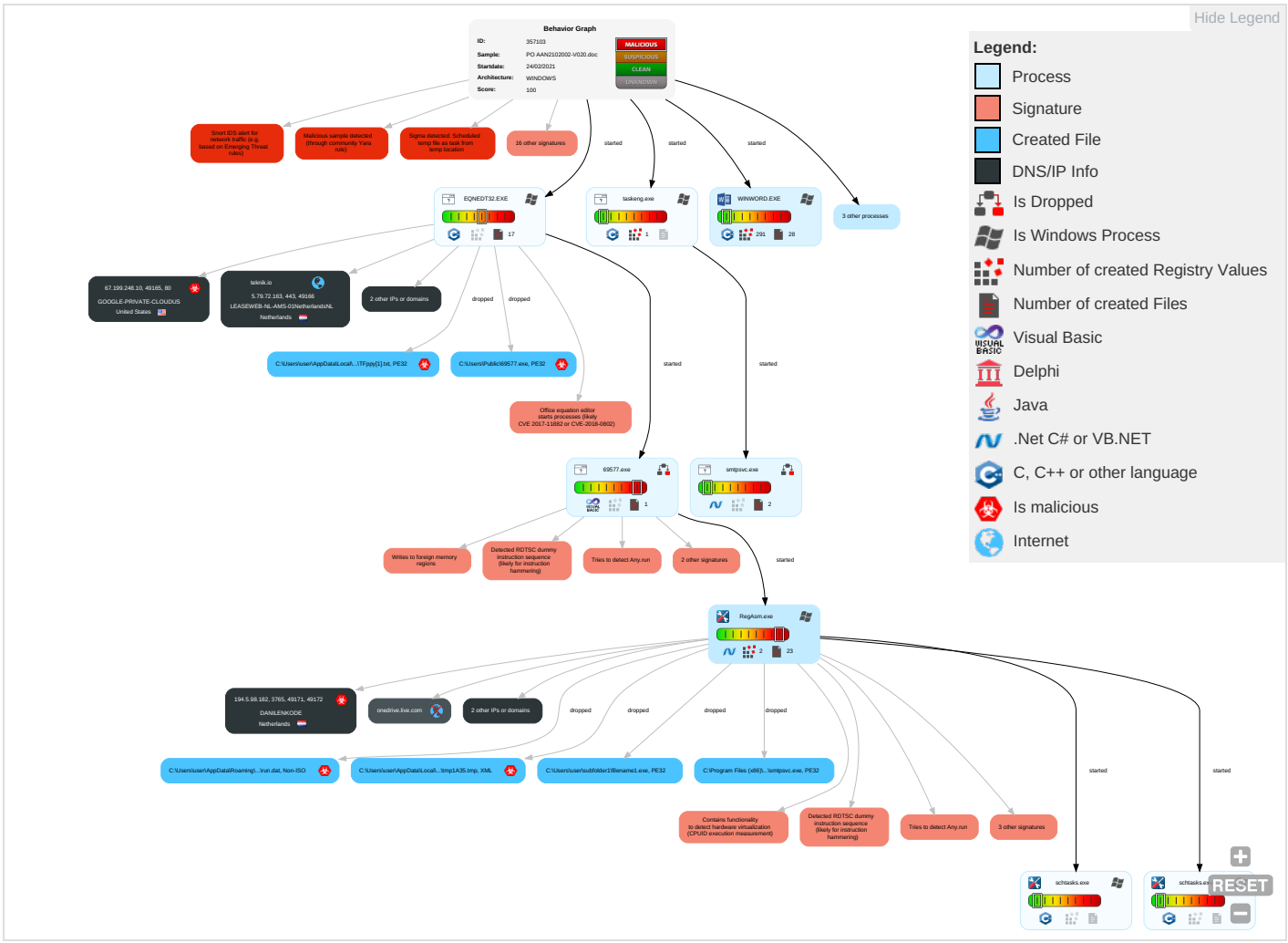
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	
Spearphishing Link 1	Exploitation for Client Execution 1 3	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1 1	Input Capture 1 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2	
Default Accounts	Command and Scripting Interpreter 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Obfuscated Files or Information 1	LSASS Memory	System Information Discovery 3 1 3	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Software Packing 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1 2 2	NTDS	Security Software Discovery 6 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 3	LSA Secrets	Virtualization/Sandbox Evasion 2 3	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 3	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	

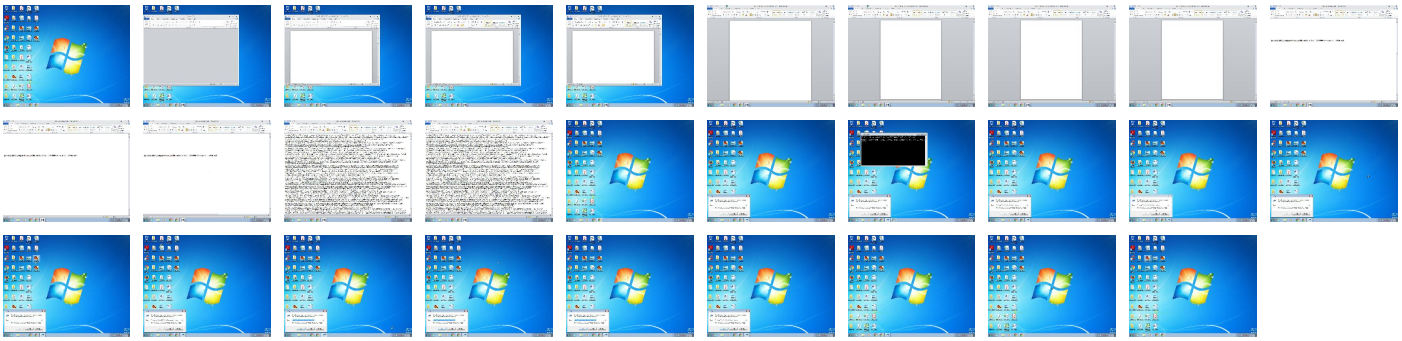
Behavior Graph

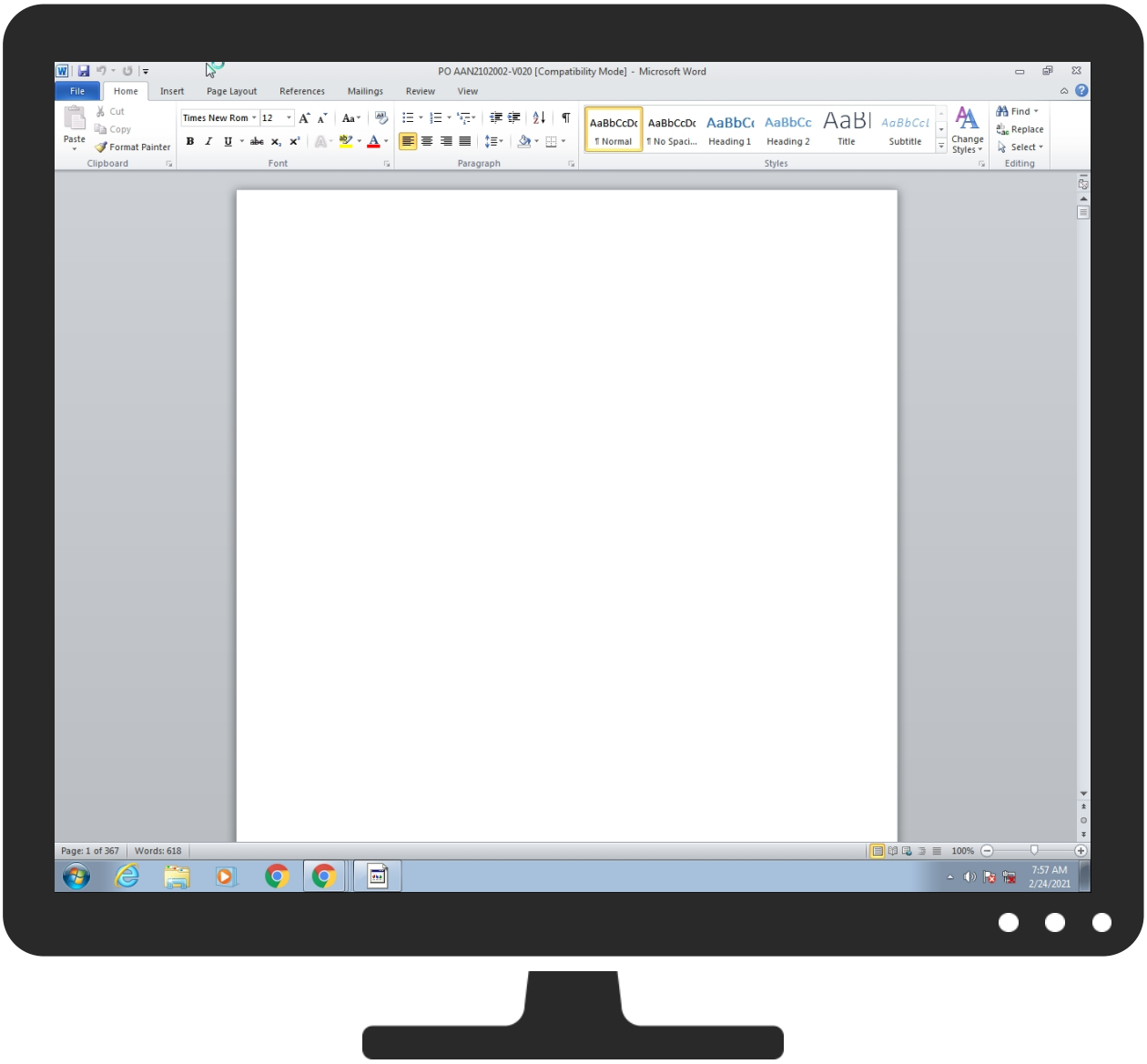


Screenshots

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 AAN2102002-V020.doc	28%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	Virustotal		Browse
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	Metadefender		Browse
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RegAsm.exe.90000.2.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	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://www.%s.comPA	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bit.ly	67.199.248.11	true	false		high
teknik.io	5.79.72.163	true	false		high
onedrive.live.com	unknown	unknown	false		high
cbavwq.bl.files.1drv.com	unknown	unknown	false		high
u.teknik.io	unknown	unknown	false		high

Contacted URLs

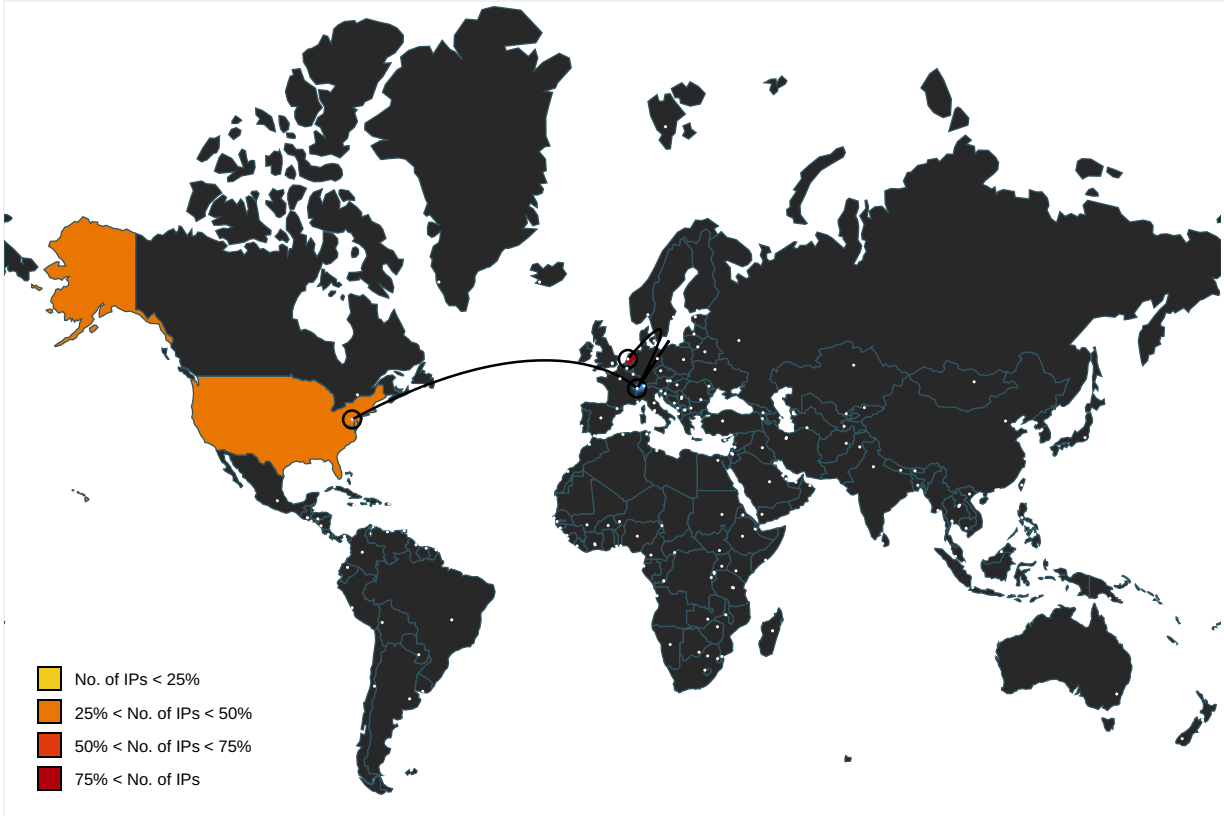
Name	Malicious	Antivirus Detection	Reputation
http://bit.ly/3pNzHgj	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	RegAsm.exe, 00000005.00000002.2354794151.0000000000A98000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	taskeng.exe, 0000000D.00000002.2342784593.0000000001B60000.00000002.00000001.sdmp	false		high
http://https://cbavwq.bl.files.1drv.com/DQ	RegAsm.exe, 00000005.00000002.2354794151.0000000000A98000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/download?cid=F57CEB019EB26E7D&resid=F57CEB019EB26E7D%21106&authkey=AHaSu1X	RegAsm.exe, RegAsm.exe, 00000005.00000002.2342821040.0000000000562000.00000040.00000001.sdmp, RegAsm.exe, 00000005.00000002.2351405264.0000000000A4C000.00000004.00000020.sdmp	false		high
http://crl.entrust.net/server1.crl0	RegAsm.exe, 00000005.00000002.2354794151.0000000000A98000.00000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.entrust.net03	RegAsm.exe, 00000005.00000002.2354794151.0000000000A98000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://u.teknik.io/TFppy.txt	3pNzHgj[1].htm.2.dr	false		high
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	RegAsm.exe, 00000005.00000002.2354794151.0000000000A98000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	taskeng.exe, 0000000D.00000002.2342784593.0000000001B60000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.diginotar.nl/cps/pkioverheid0	RegAsm.exe, 00000005.00000002.2354794151.0000000000A98000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net0D	RegAsm.exe, 00000005.00000002.2354794151.0000000000A98000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cbavwq.bl.files.1drv.com/y4m3v2kEpIV8FbxWjD8IYOSGc9eY7yGumgM5fcT1ikVolWrnqtFykMCYtt6EVe-wNwa	RegAsm.exe, 00000005.00000002.2354794151.0000000000A98000.00000004.00000020.sdmp, RegAsm.exe, 00000005.00000002.2354281853.0000000000A86000.00000004.00000020.sdmp	false		high
http://https://secure.comodo.com/CPS0	RegAsm.exe, 00000005.00000002.2354794151.0000000000A98000.00000004.00000020.sdmp	false		high
http://https://cbavwq.bl.files.1drv.com/O	RegAsm.exe, 00000005.00000002.2354794151.0000000000A98000.00000004.00000020.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	RegAsm.exe, 00000005.00000002.2354794151.0000000000A98000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/	RegAsm.exe, 00000005.00000002.2351405264.0000000000A4C000.00000004.00000020.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.182	unknown	Netherlands		208476	DANILENKODE	true
67.199.248.10	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	true
5.79.72.163	unknown	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357103
Start date:	24.02.2021
Start time:	07:57:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO AAN2102002-V020.doc
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:	20
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.winDOC@16/25@6/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 79.4% (good quality ratio 35.3%) • Quality average: 22.7% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 2.20.142.209, 2.20.142.210, 13.107.43.13, 13.107.42.12 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, odc-web-brs.onedrive.akadns.net, odc-web-geo.onedrive.akadns.net, bl-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, l-0004.dc-msedge.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, l-0003.l-msedge.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, odc-bl-files-brs.onedrive.akadns.net, odc-bl-files-geo.onedrive.akadns.net, apps.identrust.com, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:57:33	API Interceptor	50x Sleep call for process: EQNEDT32.EXE modified
07:58:40	API Interceptor	68x Sleep call for process: 69577.exe modified
07:59:02	API Interceptor	723x Sleep call for process: RegAsm.exe modified
07:59:07	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe
07:59:08	API Interceptor	2x Sleep call for process: schtasks.exe modified
07:59:09	Task Scheduler	Run new task: SMTP Service Task path: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" s>$(Arg0)
07:59:09	API Interceptor	215x Sleep call for process: taskeng.exe modified
07:59:15	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
07:59:23	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
67.199.248.10	PO55004.doc	Get hash	malicious	Browse	• bit.ly/3kioaoe
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• bit.ly/2NUvTNf
	RFQ Document.doc	Get hash	malicious	Browse	• bit.ly/3qOyCWN
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• bit.ly/3qN5fEA
	Order.doc	Get hash	malicious	Browse	• bit.ly/3boWBW4
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• bit.ly/2NScGvD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• bit.ly/3kemdsK
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• bit.ly/2Me6ei3
	swift payment.doc	Get hash	malicious	Browse	• bit.ly/2N mOCRI
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• bit.ly/3qIRVRz
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• bit.ly/3duA4tQ
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• bit.ly/3sdTreK
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	• bit.ly/3d CBRgm
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• bit.ly/3bhrITG
	Quote QU038097.doc	Get hash	malicious	Browse	• bit.ly/3aom5Uu
	IMG_51067.doc__.rtf	Get hash	malicious	Browse	• bit.ly/3djdyUC
	IMG_123773.doc	Get hash	malicious	Browse	• bit.ly/2Nsv9ym
	B62672021 PRETORIA.doc	Get hash	malicious	Browse	• bit.ly/3j OWhDW
	DHL_014073.doc	Get hash	malicious	Browse	• bit.ly/3d dwOmz
	PO00004423.doc	Get hash	malicious	Browse	• bit.ly/3dcJ7zg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bit.ly	PO55004.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	RFQ Document.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 67.199.248.10
	Order.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTE.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 67.199.248.10
	swift payment.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_61061_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• 67.199.248.11
	_a6590.docx	Get hash	malicious	Browse	• 67.199.248.11
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	• 67.199.248.10
	Statement-ID21488878391791.vbs	Get hash	malicious	Browse	• 67.199.248.11
	Statement-ID72347595684775.vbs	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	• 67.199.248.10

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-NL-AMS-01NetherlandsNL	PO55004.doc	Get hash	malicious	Browse	• 5.79.72.163
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 5.79.72.163
	RFQ Document.doc	Get hash	malicious	Browse	• 5.79.72.163
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 5.79.72.163
	SecuriteInfo.com.Trojan.PackedNET.540.1271.exe	Get hash	malicious	Browse	• 213.227.154.188
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 5.79.72.163
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	• 5.79.70.250
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	• 5.79.72.163
	Quotation408S_A02021_AHYAN_group_of_companies.doc	Get hash	malicious	Browse	• 5.79.72.163
	Request For Quotation.PDF.exe	Get hash	malicious	Browse	• 212.32.237.101
	PO#652.exe	Get hash	malicious	Browse	• 5.79.87.207
	Parcel _009887 .exe	Get hash	malicious	Browse	• 212.32.237.92
	PO 20211602.xlsm	Get hash	malicious	Browse	• 82.192.82.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6d0000.exe	Get hash	malicious	Browse	• 213.227.133.129
	SecuriteInfo.com.Trojan.PackedNET.541.9005.exe	Get hash	malicious	Browse	• 62.212.86.139
	New Order 83329 PDF.exe	Get hash	malicious	Browse	• 95.211.208.58
	YTDSetup.exe	Get hash	malicious	Browse	• 82.192.80.226
	g3hMtp06fF.dll	Get hash	malicious	Browse	• 77.81.247.140
	SecuriteInfo.com.Heur.4110.xls	Get hash	malicious	Browse	• 212.32.245.130
	SecuriteInfo.com.Heur.22411.xls	Get hash	malicious	Browse	• 212.32.245.130
DANILENKODE	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 194.5.98.202
	neue bestellung.PDF.exe	Get hash	malicious	Browse	• 194.5.97.48
	Orderoffer.exe	Get hash	malicious	Browse	• 194.5.98.66
	neue bestellung.PDF.exe	Get hash	malicious	Browse	• 194.5.97.48
	OrderSuppliesQuote0817916.exe	Get hash	malicious	Browse	• 194.5.97.248
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 194.5.97.244
	QuotationInvoices.exe	Get hash	malicious	Browse	• 194.5.97.248
	PAYMENT_.EXE	Get hash	malicious	Browse	• 194.5.98.211
	payment.exe	Get hash	malicious	Browse	• 194.5.98.66
	RFQ_1101983736366355 1101938377388.exe	Get hash	malicious	Browse	• 194.5.98.21
	Slip copy .xls.exe	Get hash	malicious	Browse	• 194.5.97.116
	Scan0059.pdf.exe	Get hash	malicious	Browse	• 194.5.97.34
	DHL AWB # 6008824216.png.exe	Get hash	malicious	Browse	• 194.5.97.48
	Scan0019.exe	Get hash	malicious	Browse	• 194.5.97.34
	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• 194.5.97.248
	Invoice467972.jar	Get hash	malicious	Browse	• 194.5.97.18
	Invoice467972.jar	Get hash	malicious	Browse	• 194.5.97.18
	Hk6Im7DPON.exe	Get hash	malicious	Browse	• 194.5.98.107
	Zfpmspqv.exe	Get hash	malicious	Browse	• 194.5.97.21
	Notification of payment.exe	Get hash	malicious	Browse	• 194.5.97.92
GOOGLE-PRIVATE-CLOUDUS	PO55004.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	RFQ Document.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 67.199.248.10
	Order.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTE.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 67.199.248.10
	swift payment.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_61061_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• 67.199.248.11
	_a6590.docx	Get hash	malicious	Browse	• 67.199.248.11
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	• 67.199.248.10
	Statement-ID21488878391791.vbs	Get hash	malicious	Browse	• 67.199.248.11
	Statement-ID72347595684775.vbs	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	• 67.199.248.10

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	
	RFQ # TSI2202708.doc	Get hash	malicious	Browse	
	rfq_20712557-20200308 Order.doc	Get hash	malicious	Browse	
	31RFQ 49177 PO-DM-11-2018-109159.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	69shipment Details...exe	Get hash	malicious	Browse	
	64RFQ#4500052988_AHBGroup_01734221347210 3_20181024.exe	Get hash	malicious	Browse	
	22RFQ#4500052988_AHBGroup_01734221347210 3_20181024.exe	Get hash	malicious	Browse	
	41COSCO TBN FULLY SIGNED CPFN.exe	Get hash	malicious	Browse	
	19Request for Quote_Goedeker_6397_3 01-2_12137018.exe	Get hash	malicious	Browse	
	72Payment....exe	Get hash	malicious	Browse	
	832238740303837363.exe	Get hash	malicious	Browse	
	35Request for Quote_SOSi_6397_3 01-2_12137018.exe	Get hash	malicious	Browse	
	61Request for Quote_SOSi_6397_3 01-2_12137018.exe	Get hash	malicious	Browse	
	17Request for Quote_SOSi_6397_3 01-2_12137018.exe	Get hash	malicious	Browse	
	59Doc_RFQ Roccia s.r.l. 180001899918 & 500037221 (1).exe	Get hash	malicious	Browse	
	71RFQ Ganix Global-180001899918 & 500037221.exe	Get hash	malicious	Browse	
	81PAYMENT.exe	Get hash	malicious	Browse	
	59Doc_RFQ Roccia s.r.l. 180001899918 & 500037221.exe	Get hash	malicious	Browse	
	2810010518.exe	Get hash	malicious	Browse	
	66Doc_BONATTI 18000229 IQ1201 WO 210000102767.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	53248
Entropy (8bit):	4.48905382202799
Encrypted:	false
SSDEEP:	768:GP2Bbv+VazyoD2z9TU//1mz1+M9GnLEu+2hhFRJS8AW:tJv46yoD2BTNz1+M9GLfvw8AW
MD5:	246BB0F8D68A463FD17C235DEB5491C0
SHA1:	63F237F94EAB14CB4DCA7ACB5817644D4428873A
SHA-256:	32B60D7BBA22CC1682F4BA651D86C9FB357BDC82E9A284AB9668E5446BD24BB3
SHA-512:	187D08DF6563739A3A537439F313D9F4D53001FA8A9CD146986DAB3C1168E25E210771AFC2A7D6C2A88EB44F0EEF2E91DDCEA8ABD86742AD0E6D78F07BDF796
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc, Detection: malicious, Browse • Filename: RFQ # TSI2202708.doc, Detection: malicious, Browse • Filename: rfq_20712557-20200308 Order.doc, Detection: malicious, Browse • Filename: 31RFQ 49177 PO-DM-11-2018-109159.exe, Detection: malicious, Browse • Filename: 69shipment Details...exe, Detection: malicious, Browse • Filename: 64RFQ#4500052988_AHBGroup_017342213472103_20181024.exe, Detection: malicious, Browse • Filename: 22RFQ#4500052988_AHBGroup_017342213472103_20181024.exe, Detection: malicious, Browse • Filename: 41COSCO TBN FULLY SIGNED CPFN.exe, Detection: malicious, Browse • Filename: 19Request for Quote_Goedeker_6397_3 01-2_12137018.exe, Detection: malicious, Browse • Filename: 72Payment....exe, Detection: malicious, Browse • Filename: 832238740303837363.exe, Detection: malicious, Browse • Filename: 35Request for Quote_SOSi_6397_3 01-2_12137018.exe, Detection: malicious, Browse • Filename: 61Request for Quote_SOSi_6397_3 01-2_12137018.exe, Detection: malicious, Browse • Filename: 17Request for Quote_SOSi_6397_3 01-2_12137018.exe, Detection: malicious, Browse • Filename: 59Doc_RFQ Roccia s.r.l. 180001899918 & 500037221 (1).exe, Detection: malicious, Browse • Filename: 71RFQ Ganix Global-180001899918 & 500037221.exe, Detection: malicious, Browse • Filename: 81PAYMENT.exe, Detection: malicious, Browse • Filename: 59Doc_RFQ Roccia s.r.l. 180001899918 & 500037221.exe, Detection: malicious, Browse • Filename: 2810010518.exe, Detection: malicious, Browse • Filename: 66Doc_BONATTI 18000229 IQ1201 WO 210000102767.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....S..... ....@.. ..... .@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..Ir.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep....xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....].....B0@0...U.....0....0...U.....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pI.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.090852246460565
Encrypted:	false
SSDEEP:	6:kKShbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:93kPlE99SNxAhUeo+aKt
MD5:	BA8C46428A6FA596F901B63BD2866482
SHA1:	406BE55AAF0AF8BCB55E66978678128FF5D936B4
SHA-256:	CFF4081C8033E6D3DF207C1DEC83503A4C7C3619E2780062918DB54E3B407E49
SHA-512:	AD2651B0A73F69FE842082E70978EE982C494A4AF9030D0B369F659DC9D65D01A7B639DA787696096E265A69DD0DA5D0E66581572F9A791A6846696F388AF83D
Malicious:	false
Preview:	p..... .....MI.....(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.018531379206123
Encrypted:	false
SSDEEP:	3:kkFkl8fllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKXliBAIdQZV7eAYLit
MD5:	F5024D7097D7BD054FB0E8F112AE0878
SHA1:	DB442D7323A0F13A7B9B146F56A9D17F98DA48F1
SHA-256:	3530EE9892B047529057DAAE8618C3BF7479A2946AC256CDD452CE24D788B015

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
SHA-512:	1BC6C2F0474F4AD130C9CE37D20AC7367E33D7709251D9A4A7AE148977CD9B2B600DE866839D0B610CF750EB3290B702E28685EA8A0EC962CDA9D2E16479FF4C
Malicious:	false
Preview:	p..... ....`....e.....(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\TFppy[1].txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	131072
Entropy (8bit):	4.85840802848053
Encrypted:	false
SSDEEP:	3072:FwVUPYLV4+aQTxxs+7Qx+2OGeoyrARHNlyCI2jnyIa3MAB+f/FwGIt1KFzOn1k4H:FwVUPYLV4+aQTxxs+7Qx+2OGeoyrARHs
MD5:	ACFCBD916FA04787E4388B339592DD78
SHA1:	F2A572347C81B71C3A59F00A37F68DB698715460
SHA-256:	EDE5C7B0267F4801A7BEBB22A18035923E71A476CEB3B9D94F582AA199DEB3F0
SHA-512:	23B895AD239AC48726A1446299E4534E496BB891530CB11E3764FB871F5F5097B12CCE346FDBCFE4A1C31D46F31A25CE407B17D6AB1A141BEEF9613E92DA817
Malicious:	**true**
IE Cache URL:	http://https://u.teknik.io/TFppy.txt
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~..0.....0...Rich1.....PE..L....$T.....P.....`....@.....TY..(....p.....(.. .....text....M.....P.....`.data.....`.....`.....@....rsrc.....p.....p.....@..@...I.....MSVBVM60.DLL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\3pNzHgj[1].htm	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.534813815767662
Encrypted:	false
SSDEEP:	3:qVvzLURODccZ/vXbvx9nDyZHL+EVMIkFSXbKFvNGb:qFzLIeco3XLx92ZHqEmIMSLWQb
MD5:	83612AE2434582AC7D267DC358EE3AFE
SHA1:	56A7C0DD21B81E84C12388E1F24B9CABB03FBB49
SHA-256:	6B721A8C98F8629EFCD006197C7BB38109F5783C10E2056916A5BF8A3CB4C63F
SHA-512:	53D0B67458C589F4B612EBAD26839934FF617D7E2AE23C624416CA9D2C12C888B4B9A3DA6F0E110F400CAD70F23D1FF7A1C039A8719D66B16A1509F4FF334BF
Malicious:	false
Preview:	<html>.<head><title>Bitly</title></head>.<body>moved here</body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A5A0-0BCBA7498F21}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2496870
Entropy (8bit):	4.120148428675921
Encrypted:	false
SSDEEP:	12288:fDaFDrFDeFDIFDWFDrFDsFDoFDrFDrWDkFDrFD0jDrFDrFwdFDrFDruDwFDrFDAK:fad+cmdw8de4d+ddCdmEdEdo3Ee
MD5:	5CB2CE6B1963218437AE4593429E3AAD
SHA1:	E7A7BDD84E63B9F56559D4ECA4DB7E4CAC071FD8
SHA-256:	6ADBC21E243E3974B278EFAA85452760E0A00179263646E1597A44DDE263A367
SHA-512:	A6C9C8B3160C8489A4089EAE2430F1D40190A625E826FAE53C953B1F6A5C87C616F2D0B60D1649FDE53909DD2A7568936D7190BC75ACE82ADDE912504118DEE
Malicious:	false
Preview:	..@.A.p.J.n.b.S.m.E.I.k.B.Y.w.P.B.r.@.-.D.y.s.i.v.y.j.z.Z.m.o.I.e.C.P.i.F.<.e.h.&.&.0._.M.-.C._.g.-.-._.-.d.,.6.4.>.3.2.9.9.7.$.C.v.>.y.t.=.n.5.|.:.%._.>.j.n.8.%.b.m.;.=.u...2.8.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{784442AB-DE8E-4300-98F0-AE5841A8170E}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{784442AB-DE8E-4300-98F0-AE5841A8170E}.tmp	
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A867ADF-3614-4635-BF44-6C9AC8D8FC42}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3568273340340578
Encrypted:	false
SSDEEP:	3:liiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlb7:liiiiiiiifdLloZQc8++lsJe1MzQ
MD5:	8BBA101DD4CCBB491B159086265AA203
SHA1:	B05248909106B80A56350FD5334B139A2C4E7B94
SHA-256:	1469FCBD040B763444AF4931D1D3499FFB3E168DAE994EEACB1367376B9260C8
SHA-512:	8C388DCE0A6BF9DC4559088A2F3C2B37E65A6CEA49816F9F2B5D001AF820D04000331B151EF1B2E02286F4B6F254AA9B5F905515F880F55C9883A2A1791E1C3F
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ..... ."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Temp\Cab9B56.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..Ir.....I.l6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\Local\Temp\Tar9B57.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false

C:\Users\user\AppData\Local\Temp\Tar9B57.tmp	
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..210115004237Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\tmp1A35.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1319
Entropy (8bit):	5.133606110275315
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mne5xtn:cbk4oL600QydbQxIYODOLedq3Ze5j
MD5:	C6F0625BF4C1CDFB699980C9243D3B22
SHA1:	43DE1FE5805769355163 27F17B5DA0C656C72851
SHA-256:	8DFC4E937F0B2374E3CED25FCE344B0731CF44B8854625B318D50ECE2DA8F576
SHA-512:	9EF2DBD4142AD0E1E6006929376ECB8011E7FFC801EE2101E906787D70325AD82752DF65839DE9972391FA52E1E5974EC1A5C7465A88AA56257633EBB7D70969
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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp678.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.1063907901076036
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Rl4xtn:cbk4oL600QydbQxIYODOLedq3Sl4j
MD5:	CFAE5A3B7D8AA9653FE2512578A0D23A
SHA1:	A91A2F8DAEF114F89038925ADA6784646A0A5B12
SHA-256:	2AB741415F193A2A9134EAC48A2310899D18EFB5E61C3E81C35140A7EFEA30FA
SHA-512:	9DFD7ECA6924AE2785CE826A447B6CE6D043C552FBD3B8A804CE6722B07A74900E703DC56CD4443CAE9AB9601F21A6068E29771E48497A9AE434096A11814E8
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	1160
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	24:IQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtd:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/a
MD5:	786E4F1138F3E30FB67C690E55AC5A4F
SHA1:	828C2B627BCB54053173B54C3A4C289EF3476641
SHA-256:	D953043AE0955AA739AF97A60DAC7541048D83FC7601365A861A527E59DBFA38
SHA-512:	5FA075AB5626579DFE5A96E5B6DABF60DC3DDBA8A6E5ADEF0538032E8FB000772C7DCB73D315B208A04125F014ACCB92FAA194108D4C76443B9FB7B97719FF6
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:sft:Mt
MD5:	88A7CB28E1F9D160FFED7B6A32D1C419
SHA1:	0B88822CD1B4F5A97BE75F69312FCD856571F36B
SHA-256:	153FAD0BD2B8BC7346F2C92D8A723E578A62628C92E9D3EF882BF8AA12D27E2E
SHA-512:	57258E5199BB71D7B2A85673279FA60125FB442B9C46F9C80EC68CDBF1F10DD7DB6FD240D531CADB448BEA931B54D4A884823074195E9C2F192BBB073FFF0F1
Malicious:	**true**
Preview:	.....H

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO AAN2102002-V020.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Wed Feb 24 14:57:31 2021, length=1297796, window=hide
Category:	dropped
Size (bytes):	2108
Entropy (8bit):	4.53782979475892
Encrypted:	false
SSDEEP:	48:81h/XT0jkwt3vr//Qh21h/XT0jkwt3vr//Q/:8j/Xojk+L/Qh2j/Xojk+L/Q/
MD5:	2D31E0A5E3CE2FB05B3249A2E7A50391
SHA1:	D65033284A86BEE643FCF6B4A910B05510958C79
SHA-256:	C1134693165539B4931F830E108B2DEFAFD1B2B22A78B9AF29B1D7520672F120
SHA-512:	18E6786A75490E4EDEB790989A2033502C140582ED0C14FC7CFCE9F5258DB8796FBF208EC883F8ADF528175F317DE5666AED6E819CED49C3E0C624A4B078F8A
Malicious:	false
Preview:	L.....F.... .....{.....{.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9....v.2.....XR0. .POAAN2~1.DOC..Z.....Q.y.Q.y*...8.....P.O. .A.A.N.2.1.0.2.0.0.2.-.V.0.2.0...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\888683\Users.user\Desktop\PO AAN2102002-V020.doc.-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.O. .A.A.N.2.1.0.2.0.0.2.-.V.0.2.0...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....888683.....D_....3N...W..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	92
Entropy (8bit):	4.025019499385517
Encrypted:	false
SSDEEP:	3:M1geiWY5v6ltOWY5v6lmX1geiWY5v6lv:Mivdc/Odc1vdc1
MD5:	7BDDD1418843BBC290F1CC2B2111829D
SHA1:	6AC41238F0E8FF7E578CAD5393E01A74A48294A8
SHA-256:	09050AF358201FC6E0A9C00D67108621E4F631F77903C2A16FEB35136467A9A6
SHA-512:	98656A2CBFED289E758467D8828648FA4DA8135E69C49669886B1A51A130CD37D5B1CBF6889196F25718A156C9528A427EE4C4712369A2A7700C2DEB4262D0EF
Malicious:	false
Preview:	[doc]..PO AAN2102002-V020.LNK=0..PO AAN2102002-V020.LNK=0..[doc]..PO AAN2102002-V020.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\YJQ5VHCG.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	64
Entropy (8bit):	4.038298827786958
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2R4VaUvuRRXv:vEMWXR4N23Xv
MD5:	3364137558A8998E179AC8C49945D25B
SHA1:	B7017E68567C6F7FE4A9F3C73BF79608E301A169
SHA-256:	0C7E288147364D8ED85060BB4B5C9D3DF6E53D31EC20A6A1E20F62B5CB02217D
SHA-512:	EBFA04F00C4FD683034E9423C1F736DBB9EC6E5BAC3860B9474B6C9A18D97EC53FB28304AE98322DA63B51DE9664E949D342612CF74B92C799B8A6C7D582155
Malicious:	false
IE Cache URL:	live.com/
Preview:	wla42..live.com/.1536.3303040384.30871546.2904902535.30870214.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\ZEL5A6R0.txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	88
Entropy (8bit):	4.258726971363556
Encrypted:	false
SSDEEP:	3:jvl3LSUyVV2HWci2nOJgrELWhRXv:p7SHVSWci2nIgrQoXv
MD5:	6AA36785C40C2F47334E368D31E7EAF0
SHA1:	CC27C6201F13F7AE5BF0894A2FE1A6A77825B232
SHA-256:	0A256EFDCE25140BC8F809617DE87BDA6C86BC7E40F6EA113F878C1C3C4909DE
SHA-512:	C984D57DEFC775D264A2B7A3D95266CEF8920767A0AB6454D881A5A873622BBAB86B9A15A35C4325A0A1BBE85CFA32F0F08717B079BF6B41B5465C043372C08
Malicious:	false
IE Cache URL:	bit.ly/
Preview:	_bit.l1o6W3-c81e1a3d057d34d143-001.bit.ly/.1536.931204992.30906348.184848914.30870214.*.

C:\Users\user\Desktop\~$ AAN2102002-V020.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A

C:\Users\user\Desktop\~$ AAN2102002-V020.doc	
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\subfolder1\filename1.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	4.85840802848053
Encrypted:	false
SSDEEP:	3072:FwVUPYLV4+aQTxxs+7Qx+2OGeoyrARHNlyCI2jnyIa3MAB+f/FwGIt1KFzOn1k4H:FwVUPYLV4+aQTxxs+7Qx+2OGeoyrARHs
MD5:	ACFCBD916FA04787E4388B339592DD78
SHA1:	F2A572347C81B71C3A59F00A37F68DB698715460
SHA-256:	EDE5C7B0267F4801A7BEBB22A18035923E71A476CEB3B9D94F582AA199DEB3F0
SHA-512:	23B895AD239AC48726A1446299E4534E496BB891530CB11E3764FB871F5F5097B12CCE346FDBCFE4A1C31D46F31A25CE407B17D6AB1A141BEEF9613E92DA817
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~..0.....0...Rich1.....PE..L....$T.....P.....`....@.....TY..(....p.....(.. .....text....M.....P.....`.data.....`.....`.....@....rsrc.....p.....p.....@..@...I.....MSVBVM60.DLL.....

C:\Users\Public\69577.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	131072
Entropy (8bit):	4.85840802848053
Encrypted:	false
SSDEEP:	3072:FwVUPYLV4+aQTxxs+7Qx+2OGeoyrARHNlyCI2jnyIa3MAB+f/FwGIt1KFzOn1k4H:FwVUPYLV4+aQTxxs+7Qx+2OGeoyrARHs
MD5:	ACFCBD916FA04787E4388B339592DD78
SHA1:	F2A572347C81B71C3A59F00A37F68DB698715460
SHA-256:	EDE5C7B0267F4801A7BEBB22A18035923E71A476CEB3B9D94F582AA199DEB3F0
SHA-512:	23B895AD239AC48726A1446299E4534E496BB891530CB11E3764FB871F5F5097B12CCE346FDBCFE4A1C31D46F31A25CE407B17D6AB1A141BEEF9613E92DA817
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~..0.....0...Rich1.....PE..L....$T.....P.....`....@.....TY..(....p.....(.. .....text....M.....P.....`.data.....`.....`.....@....rsrc.....p.....p.....@..@...I.....MSVBVM60.DLL.....

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	6.255341250007536
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	PO AAN2102002-V020.doc
File size:	1297796
MD5:	71e541e756ee25fb690431d271d26e47
SHA1:	f7f6c91b2673d889035e3d542aa47c95130d9273
SHA256:	b3104dab0a4fd156fd26e66c494970ba11bc2e954b62d7b b23a618ae7519d1b9
SHA512:	5db56f9dc9a6c2dd0daf0086a64b47750e46672e7b723b0 8525ead86e5d9d69d7ad3e0a55f44c79fbac15008770895 09c8ca9298a0df84a6853fb1e6f68b9c0e
SSDEEP:	6144:Zy+By+By+By+By+By+By+By+By+By+By+By+By+By +By+By+By+By+By+By+By+o:ZBBBBBBBBBBBBB BBBBBBBBBBW+Uh53

General

File Content Preview:	{\rtf51437\page11419927264400464@ApJnbSmElkBYw PBr@-DysivyjzZmoIeCPiF<eh&&0_M-C_g--_-d,64>329 97$Cv>yt=n5|:%_>jn8%bm\mklP;=u\m3699.28.... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

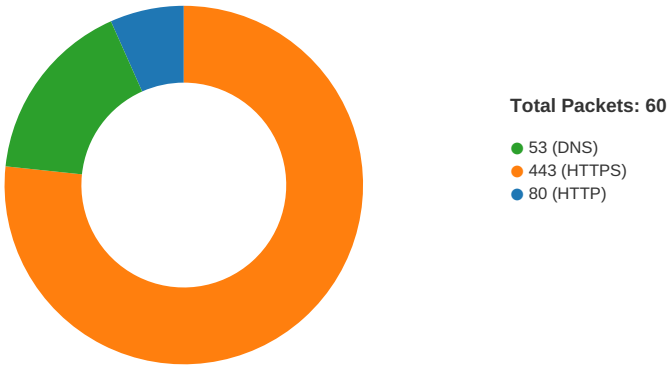
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0012A664h								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/24/21-07:59:39.832037	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49171	3765	192.168.2.22	194.5.98.182
02/24/21-07:59:46.029027	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49172	3765	192.168.2.22	194.5.98.182
02/24/21-07:59:52.264398	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49173	3765	192.168.2.22	194.5.98.182
02/24/21-07:59:58.400400	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49174	3765	192.168.2.22	194.5.98.182
02/24/21-08:00:04.540398	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49175	3765	192.168.2.22	194.5.98.182
02/24/21-08:00:10.762650	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49176	3765	192.168.2.22	194.5.98.182

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 07:58:03.525432110 CET	49165	80	192.168.2.22	67.199.248.10
Feb 24, 2021 07:58:03.580601931 CET	80	49165	67.199.248.10	192.168.2.22
Feb 24, 2021 07:58:03.580698967 CET	49165	80	192.168.2.22	67.199.248.10

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 07:58:03.581068039 CET	49165	80	192.168.2.22	67.199.248.10
Feb 24, 2021 07:58:03.634711027 CET	80	49165	67.199.248.10	192.168.2.22
Feb 24, 2021 07:58:03.725155115 CET	80	49165	67.199.248.10	192.168.2.22
Feb 24, 2021 07:58:03.725308895 CET	49165	80	192.168.2.22	67.199.248.10
Feb 24, 2021 07:58:03.922012091 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:03.976551056 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:03.976748943 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:03.988882065 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:04.044708014 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:04.044763088 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:04.044866085 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:04.044929981 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:04.062096119 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:04.118747950 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:04.118971109 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:05.707983017 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:05.785584927 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.175651073 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.175712109 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.175753117 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.175815105 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.175858974 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.175929070 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.175972939 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.176023960 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.176069021 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.176107883 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.176137924 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.176176071 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.176213026 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.176356077 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.176409960 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.176414967 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.176419020 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.176423073 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.176426888 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.176430941 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.176433086 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.176434994 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.176438093 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.176440001 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.176441908 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.182267904 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.228215933 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228244066 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228257895 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228319883 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228435040 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.228481054 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228528976 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.228557110 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228563070 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.228589058 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228616953 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.228620052 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228650093 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.228687048 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.228687048 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228708982 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228774071 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.228801012 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228842974 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.228851080 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228857994 CET	49166	443	192.168.2.22	5.79.72.163

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 07:58:06.228869915 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228888988 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228910923 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.228956938 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228956938 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.228988886 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.228990078 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.229007959 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.229037046 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.229083061 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.229137897 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.229161024 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.229177952 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.229214907 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.229239941 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.229269028 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.229305029 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.229310989 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.229321003 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.229345083 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.229370117 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.229398012 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.230669975 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.280603886 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.280636072 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.280723095 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.280862093 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.280915022 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.280957937 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.281013012 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.281100035 CET	443	49166	5.79.72.163	192.168.2.22
Feb 24, 2021 07:58:06.281150103 CET	49166	443	192.168.2.22	5.79.72.163
Feb 24, 2021 07:58:06.281160116 CET	443	49166	5.79.72.163	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 07:58:03.413405895 CET	52197	53	192.168.2.22	8.8.8.8
Feb 24, 2021 07:58:03.462511063 CET	53	52197	8.8.8.8	192.168.2.22
Feb 24, 2021 07:58:03.462815046 CET	52197	53	192.168.2.22	8.8.8.8
Feb 24, 2021 07:58:03.511917114 CET	53	52197	8.8.8.8	192.168.2.22
Feb 24, 2021 07:58:03.784756899 CET	53099	53	192.168.2.22	8.8.8.8
Feb 24, 2021 07:58:03.849397898 CET	53	53099	8.8.8.8	192.168.2.22
Feb 24, 2021 07:58:03.849713087 CET	53099	53	192.168.2.22	8.8.8.8
Feb 24, 2021 07:58:03.920074940 CET	53	53099	8.8.8.8	192.168.2.22
Feb 24, 2021 07:58:04.387250900 CET	52838	53	192.168.2.22	8.8.8.8
Feb 24, 2021 07:58:04.437798023 CET	53	52838	8.8.8.8	192.168.2.22
Feb 24, 2021 07:58:04.440893888 CET	61200	53	192.168.2.22	8.8.8.8
Feb 24, 2021 07:58:04.494389057 CET	53	61200	8.8.8.8	192.168.2.22
Feb 24, 2021 07:58:05.008219957 CET	49548	53	192.168.2.22	8.8.8.8
Feb 24, 2021 07:58:05.071787119 CET	53	49548	8.8.8.8	192.168.2.22
Feb 24, 2021 07:58:05.074932098 CET	55627	53	192.168.2.22	8.8.8.8
Feb 24, 2021 07:58:05.132577896 CET	53	55627	8.8.8.8	192.168.2.22
Feb 24, 2021 07:59:34.796936989 CET	56009	53	192.168.2.22	8.8.8.8
Feb 24, 2021 07:59:34.848627090 CET	53	56009	8.8.8.8	192.168.2.22
Feb 24, 2021 07:59:36.092518091 CET	61865	53	192.168.2.22	8.8.8.8
Feb 24, 2021 07:59:36.188860893 CET	53	61865	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 07:58:03.413405895 CET	192.168.2.22	8.8.8.8	0xd372	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Feb 24, 2021 07:58:03.462815046 CET	192.168.2.22	8.8.8.8	0xd372	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 07:58:03.784756899 CET	192.168.2.22	8.8.8.8	0x7032	Standard query (0)	u.teknik.io	A (IP address)	IN (0x0001)
Feb 24, 2021 07:58:03.849713087 CET	192.168.2.22	8.8.8.8	0x7032	Standard query (0)	u.teknik.io	A (IP address)	IN (0x0001)
Feb 24, 2021 07:59:34.796936989 CET	192.168.2.22	8.8.8.8	0xfad2	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Feb 24, 2021 07:59:36.092518091 CET	192.168.2.22	8.8.8.8	0x8eb3	Standard query (0)	cbavwq.bl.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 07:58:03.462511063 CET	8.8.8.8	192.168.2.22	0xd372	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Feb 24, 2021 07:58:03.462511063 CET	8.8.8.8	192.168.2.22	0xd372	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Feb 24, 2021 07:58:03.511917114 CET	8.8.8.8	192.168.2.22	0xd372	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Feb 24, 2021 07:58:03.511917114 CET	8.8.8.8	192.168.2.22	0xd372	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Feb 24, 2021 07:58:03.849397898 CET	8.8.8.8	192.168.2.22	0x7032	No error (0)	u.teknik.io	teknik.io		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 07:58:03.849397898 CET	8.8.8.8	192.168.2.22	0x7032	No error (0)	teknik.io		5.79.72.163	A (IP address)	IN (0x0001)
Feb 24, 2021 07:58:03.920074940 CET	8.8.8.8	192.168.2.22	0x7032	No error (0)	u.teknik.io	teknik.io		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 07:58:03.920074940 CET	8.8.8.8	192.168.2.22	0x7032	No error (0)	teknik.io		5.79.72.163	A (IP address)	IN (0x0001)
Feb 24, 2021 07:59:34.848627090 CET	8.8.8.8	192.168.2.22	0xfad2	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 07:59:36.188860893 CET	8.8.8.8	192.168.2.22	0x8eb3	No error (0)	cbavwq.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 07:59:36.188860893 CET	8.8.8.8	192.168.2.22	0x8eb3	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- bit.ly

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	67.199.248.10	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

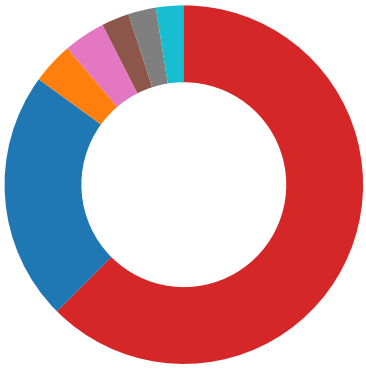
Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 07:58:03.581068039 CET	0	OUT	GET /3pNzHgj HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: bit.ly Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 07:58:03.725155115 CET	1	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 24 Feb 2021 06:58:03 GMT Content-Type: text/html; charset=utf-8 Content-Length: 116 Cache-Control: private, max-age=90 Location: https://u.teknik.io/TFppy.txt Set-Cookie: _bit=l1o6W3-c81e1a3d057d34d143-001; Domain=bit.ly; Expires=Mon, 23 Aug 2021 06:58:03 GMT Via: 1.1 google Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 42 69 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 75 2e 74 65 6b 6e 69 6b 2e 69 6f 2f 54 46 70 70 79 2e 74 78 74 22 3e 6d 6f 76 65 64 20 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Bitly</title></head><body>moved here</body></html>

Code Manipulations

Statistics

Behavior



- WINWORD.EXE
- EQNEDT32.EXE
- 69577.exe
- RegAsm.exe
- schtasks.exe
- schtasks.exe
- taskeng.exe
- smtpsvc.exe
- filename1.exe
- smtpsvc.exe
- filename1.exe

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 252 Parent PID: 584

General

Start time:	07:57:31
Start date:	24/02/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f0b0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8FE26B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$ AAN2102002-V020.doc	success or wait	1	7FEE8F09AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A5A0-0BCBA7498F21}.tmp	unknown	512	success or wait	173	7FEE8E40172	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A5A0-0BCBA7498F21}.tmp	unknown	512	success or wait	4819	7FEE8F09AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A5A0-0BCBA7498F21}.tmp	unknown	512	success or wait	1	7FEE8F09AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A5A0-0BCBA7498F21}.tmp	unknown	512	success or wait	15	7FEE8F09AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A5A0-0BCBA7498F21}.tmp	unknown	512	success or wait	28	7FEE8F09AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE8F1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE8F1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE8F1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F9FF7	success or wait	1	7FEE8F09AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F9FF7	F9FF7	binary	04 00 00 00 FC 00 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 CD C6 2E E6 C5 0A D7 01 F7 9F 0F 00 F7 9F 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE8F09AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381498926	1381498927	success or wait	1	7FEE8F09AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381498927	1381498928	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F9FF7	F9FF7	binary	04 00 00 00 FC 00 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 CD C6 2E E6 C5 0A D7 01 F7 9F 0F 00 F7 9F 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 FC 00 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F7 9F 0F 00 F7 9F 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE8F09AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: 1204 Parent PID: 584

General

Start time:	07:57:32
Start date:	24/02/2021
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	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: 69577.exe PID: 896 Parent PID: 1204

General

Start time:	07:57:36
Start date:	24/02/2021
Path:	C:\Users\Public\69577.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	ACFCBD916FA04787E4388B339592DD78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 2428 Parent PID: 896

General

Start time:	07:58:56
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0x370000
File size:	53248 bytes
MD5 hash:	246BB0F8D68A463FD17C235DEB5491C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000005.00000002.2342821040.0000000000562000.00000040.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2342294404.0000000000080000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2342294404.0000000000080000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2342304047.0000000000090000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2342304047.0000000000090000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2342304047.0000000000090000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\subfolder1	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	56196C	SHCreateDirectoryExW
C:\Users\user\subfolder1\filename1.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	567766	CreateFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564519	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564519	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564519	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564519	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564519	InternetOpenUrlA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564519	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564519	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564519	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564519	InternetOpenUrlA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\YJQ5VHCG.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	564519	InternetOpenUrlA
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	718BAE4B	unknown
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	718EB05E	unknown
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	718BAE4B	unknown
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	7189920B	unknown
C:\Users\user\AppData\Local\Temp\tmp1A35.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	71869869	unknown
C:\Users\user\AppData\Local\Temp\tmp678.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	71869869	unknown
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	718BAE4B	unknown
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	718BAE4B	unknown
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	718EB05E	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1A35.tmp	success or wait	1	39BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp678.tmp	success or wait	1	39BF0E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\subfolder1\filename1.exe	unknown	131072	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 b8 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 75 9f f9 db 31 fe 97 88 31 fe 97 88 31 fe 97 88 b2 e2 99 88 30 fe 97 88 7e dc 9e 88 30 fe 97 88 07 d8 9a 88 30 fe 97 88 52 69 63 68 31 fe 97 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 d4 ae 24 54 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 50 01 00 00 a0 00 00 00 00 00 00 dc 13 00 00 00 10 00 00 00 60 01 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......u...1...1...1.......0. ..~...0.......0...Rich1....... ....PE..L.....$T............. ...P...................`....@.	success or wait	1	561C6F	WriteFile
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	unknown	8	a1 cf 80 d0 dd d8 d8 48	.......H	success or wait	1	718EAE97	unknown
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0	53248	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 2c 00 0f 53 00 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 a0 00 00 00 20 00 00 00 00 00 00 de b7 00 00 00 20 00 00 00 c0 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 01 00 00 10 00 00 9f e8 00 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 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.......... ....@.. ....@.................	success or wait	1	7189920B	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1A35.tmp	unknown	1319	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 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	718EAE97	unknown
C:\Users\user\AppData\Local\Temp\tmp678.tmp	unknown	1310	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 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	718EAE97	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	1	718EAE97	unknown
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	4	718EAE97	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\69577.exe	unknown	131072	success or wait	1	567766	ReadFile
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\regasm.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.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\RegAsm.exe	unknown	4096	success or wait	1	74034496	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	unknown	512	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.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	718EBEF7	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	718EBEF7	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	success or wait	1	718EBEF7	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	end of file	1	718EBEF7	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	Startup key	unicode	C:\Users\user\subfolder1\filename1.exe	success or wait	1	5617E4	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	SMTP Service	unicode	C:\Program Files (x86)\SMTP Service\smtpsvc.exe	success or wait	1	718DC5C3	unknown

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

Analysis Process: schtasks.exe PID: 2988 Parent PID: 2428

General

Start time:	07:59:07
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp1A35.tmp'
Imagebase:	0xf0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 2980 Parent PID: 2428

General

Start time:	07:59:08
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp678.tmp'
Imagebase:	0xf0000
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\tmp678.tmp	unknown	2	success or wait	1	F8F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp678.tmp	unknown	1311	success or wait	1	F900C	ReadFile

Analysis Process: taskeng.exe PID: 1688 Parent PID: 860

General

Start time:	07:59:09
Start date:	24/02/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {DA6299CA-95CA-4E9D-8945-2CC05321254C} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1]
Imagebase:	0xff3b0000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\Tasks\SMTP Service Task	unknown	2	success or wait	1	FF3B433D	ReadFile
C:\Windows\System32\Tasks\SMTP Service Task	unknown	2700	success or wait	1	FF3B43A4	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{DA6299CA-95CA-4E9D-8945-2CC05321254C}	data	binary	4D 45 4F 57 01 00 00 00 E4 B7 BD 92 8B F2 A0 46 B5 51 45 A5 2B DD 51 25 00 00 00 00 00 00 00 00 7D DC E1 06 C1 2A 42 E2 2E 42 B3 1F FE A4 90 BC 01 44 00 00 98 06 00 00 7F 63 86 8E 98 1A 20 79 00 00 00 00	success or wait	1	FF3C2CB8	RegSetValueExW

Analysis Process: smtpsvc.exe PID: 2380 Parent PID: 1688

General

Start time:	07:59:09
Start date:	24/02/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0
Imagebase:	0x1280000
File size:	53248 bytes
MD5 hash:	246BB0F8D68A463FD17C235DEB5491C0
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Virustotal, Browse • 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

Analysis Process: filename1.exe PID: 2152 Parent PID: 1388

General

Start time:	07:59:15
Start date:	24/02/2021
Path:	C:\Users\user\subfolder1\filename1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	ACFCBD916FA04787E4388B339592DD78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: smtpsvc.exe PID: 2500 Parent PID: 1388

General

Start time:	07:59:23
Start date:	24/02/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe'
Imagebase:	0x270000
File size:	53248 bytes
MD5 hash:	246BB0F8D68A463FD17C235DEB5491C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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

Analysis Process: filename1.exe PID: 1480 Parent PID: 1388

General

Start time:	07:59:32
Start date:	24/02/2021
Path:	C:\Users\user\subfolder1\filename1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	ACFCBD916FA04787E4388B339592DD78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis