ID: 356480
Sample Name: JMG Memo-Circular No 018-21.PDF.exe
Cookbook: default.jbs
Time: 08:39:03
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report JMG Memo-Circular No 018-21.PDF.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 6
Compliance: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 14
Public 14
Private 15
General Information 15
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 17
ASN 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 21
General 21

File Icon 21
Static PE Info 21
General 21
Entrypoint Preview 21
Data Directories 23
Sections 23
Resources 23
Imports 24
Version Infos 24
Network Behavior 24
Snort IDS Alerts 24
Network Port Distribution 24
TCP Packets 25
UDP Packets 26
DNS Queries 28
DNS Answers 28
Code Manipulations 29
Statistics 29
Behavior 29
System Behavior 29
Analysis Process: JMG Memo-Circular No 018-21.PDF.exe PID: 3540 Parent PID: 5740 29
General 29
File Activities 30
File Created 30
File Deleted 30
File Written 30
File Read 31
Analysis Process: schtasks.exe PID: 6568 Parent PID: 3540 32
General 32
File Activities 32
File Read 32
Analysis Process: conhost.exe PID: 6576 Parent PID: 6568 32
General 32
Analysis Process: JMG Memo-Circular No 018-21.PDF.exe PID: 6628 Parent PID: 3540 33
General 33
File Activities 34
File Created 34
File Deleted 35
File Written 35
File Read 37
Analysis Process: schtasks.exe PID: 6864 Parent PID: 6628 37
General 37
File Activities 37
File Read 37
Analysis Process: conhost.exe PID: 6888 Parent PID: 6864 37
General 37
Analysis Process: JMG Memo-Circular No 018-21.PDF.exe PID: 7000 Parent PID: 904 38
General 38
File Activities 38
File Created 38
File Deleted 38
File Written 38
File Read 39
Analysis Process: schtasks.exe PID: 5660 Parent PID: 7000 39
General 39
File Activities 40
File Read 40
Analysis Process: conhost.exe PID: 5716 Parent PID: 5660 40
General 40
Analysis Process: JMG Memo-Circular No 018-21.PDF.exe PID: 6376 Parent PID: 7000 40
General 40
File Activities 41
File Created 41
File Read 41
Disassembly 41
Code Analysis 41

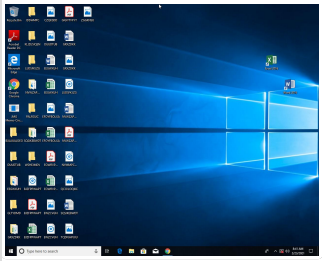
Analysis Report JMG Memo-Circular No 018-21.PDF.exe

Overview

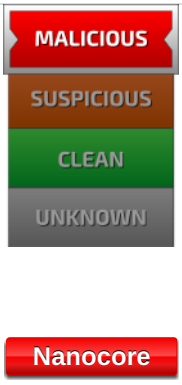
General Information

Sample Name:	JMG Memo-Circular No 018-21.PDF.exe
Analysis ID:	356480
MD5:	f12d78ae2ce77b1.
SHA1:	a4a09f0297221e8.
SHA256:	019dce879f64d1a.
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection



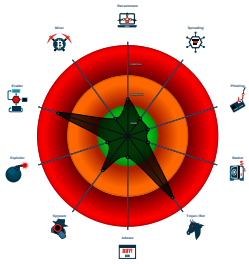
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- JMG Memo-Circular No 018-21.PDF.exe (PID: 3540 cmdline: 'C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe' MD5: F12D78AE2CE77B187E98B382BC400E6E)
  - schtasks.exe (PID: 6568 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GmaLrlDR' /XML 'C:\Users\user\AppData\Local\Temp\tmp1B75.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - JMG Memo-Circular No 018-21.PDF.exe (PID: 6628 cmdline: {path} MD5: F12D78AE2CE77B187E98B382BC400E6E)
    - schtasks.exe (PID: 6864 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpC90F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- JMG Memo-Circular No 018-21.PDF.exe (PID: 7000 cmdline: 'C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe' 0 MD5: F12D78AE2CE77B187E98B382BC400E6E)
  - schtasks.exe (PID: 5660 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GmaLrlDR' /XML 'C:\Users\user\AppData\Local\Temp\tmp8F7C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - JMG Memo-Circular No 018-21.PDF.exe (PID: 6376 cmdline: {path} MD5: F12D78AE2CE77B187E98B382BC400E6E)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c4cca249-81f6-4232-9f14-01569e09f5f0",
  "Group": "JANUARY",
  "Domain1": "shahzad73.casacam.net",
  "Domain2": "shahzad73.ddns.net",
  "Port": 9036,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.501005046.0000000006DD0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost
00000007.00000002.501005046.0000000006DD0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost
00000007.00000002.498456853.000000000538000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4bbb:$x1: NanoCore.ClientPluginHost • 0x4be5:$x2: IClientNetworkHost
00000007.00000002.498456853.000000000538000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x4bbb:$x2: NanoCore.ClientPluginHost • 0x6a6b:$s4: PipeCreated
00000007.00000002.501098807.0000000006E10000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost

Click to see the 55 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.JMG Memo-Circular No 018-21.PDF.exe.6de0000.31.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x39eb:$x1: NanoCore.ClientPluginHost • 0x3a24:$x2: IClientNetworkHost
7.2.JMG Memo-Circular No 018-21.PDF.exe.6de0000.31.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x39eb:$x2: NanoCore.ClientPluginHost • 0x3b36:$s4: PipeCreated • 0x3a05:$s5: IClientLoggingHost
7.2.JMG Memo-Circular No 018-21.PDF.exe.3ef4a1e.17.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
7.2.JMG Memo-Circular No 018-21.PDF.exe.3ef4a1e.17.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x170b:$x2: NanoCore.ClientPluginHost • 0x34b6:$s4: PipeCreated • 0x16f8:$s5: IClientLoggingHost
7.2.JMG Memo-Circular No 018-21.PDF.exe.6e60000.37.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x41ee:$x1: NanoCore.ClientPluginHost • 0x422b:$x2: IClientNetworkHost

Click to see the 157 entries

Sigma Overview

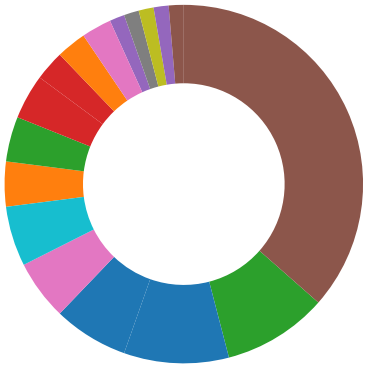
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Suspicious Double Extension

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

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)

Uses an obfuscated file name to hide its real file extension (double extension)

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

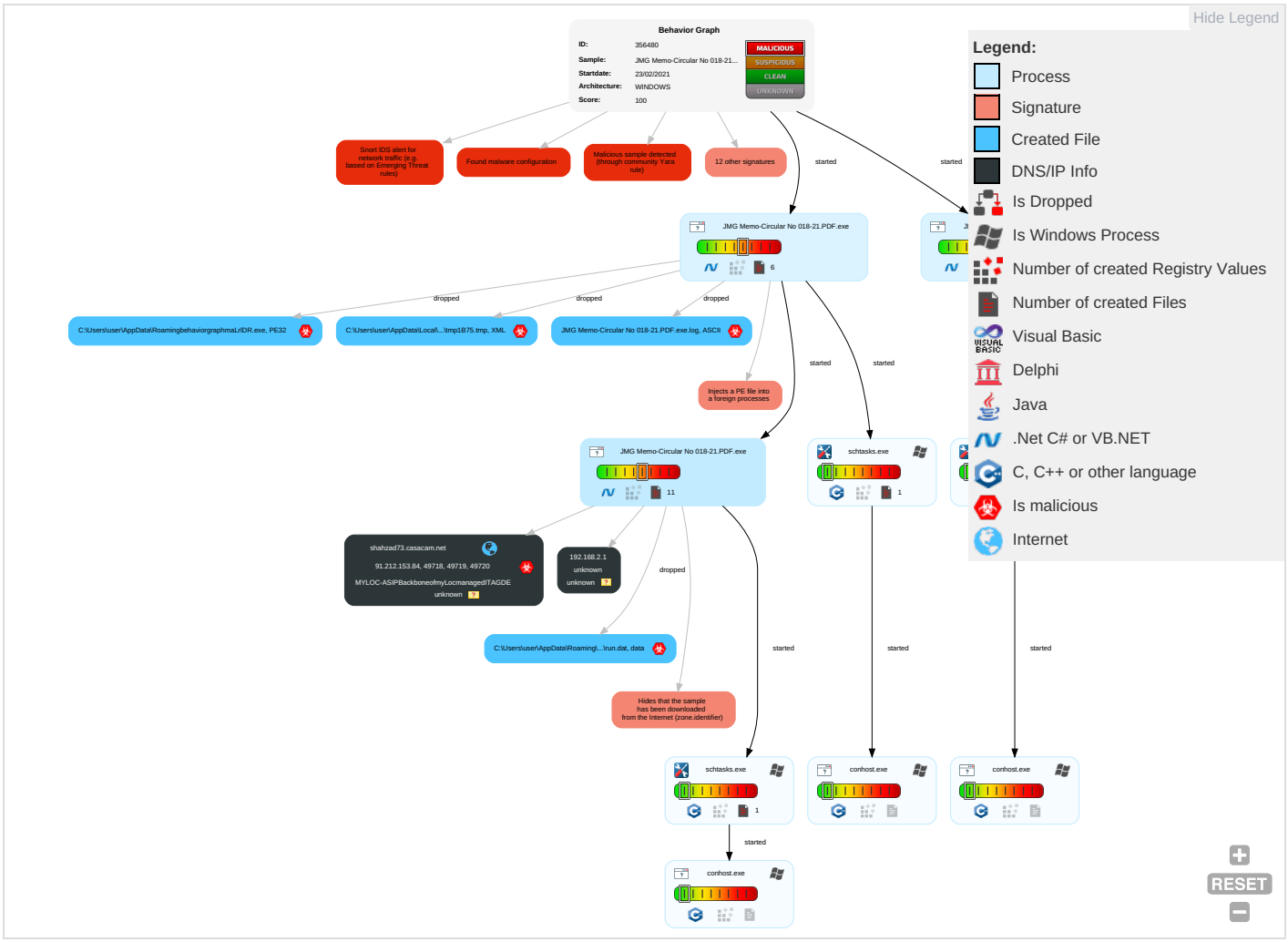
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Security Software Discovery 1 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 2	DCSync	File and Directory 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	Software Packing 1 2	Proc Filesystem	System Information Discovery 1 3	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
JMG Memo-Circular No 018-21.PDF.exe	12%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\GmaLrlDR.exe	12%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.JMG Memo-Circular No 018-21.PDF.exe.5230000.20.unpack	100%	Avira	TR/NanoCore.fadte		Download File
13.2.JMG Memo-Circular No 018-21.PDF.exe.43de1b8.2.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
7.2.JMG Memo-Circular No 018-21.PDF.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.2.JMG Memo-Circular No 018-21.PDF.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.JMG Memo-Circular No 018-21.PDF.exe.3bf9618.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File
0.2.JMG Memo-Circular No 018-21.PDF.exe.472e1b8.3.unpack	100%	Avira	HEUR/AGEN.1110362		Download File

Domains

Source	Detection	Scanner	Label	Link
shahzad73.casacam.net	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
shahzad73.ddns.net	1%	Virustotal		Browse
shahzad73.ddns.net	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.comq	0%	Avira URL Cloud	safe	
http://www.esvstudybible.org/search?q=	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.esvstudybible.org/search?q=Whttp://www.blueletterbible.org/Bible.cfm?b=	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://topicalmemorysystem.googlecode.com/files/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnB	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.carterandcone.comB	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.l	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.monotype.B	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.coma	0%	URL Reputation	safe	
http://www.sajatypeworks.coma	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.coma	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn(	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.coms-e	0%	Avira URL Cloud	safe	
shahzad73.casacam.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shahzad73.casacam.net	91.212.153.84	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
shahzad73.ddns.net	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
shahzad73.casacam.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

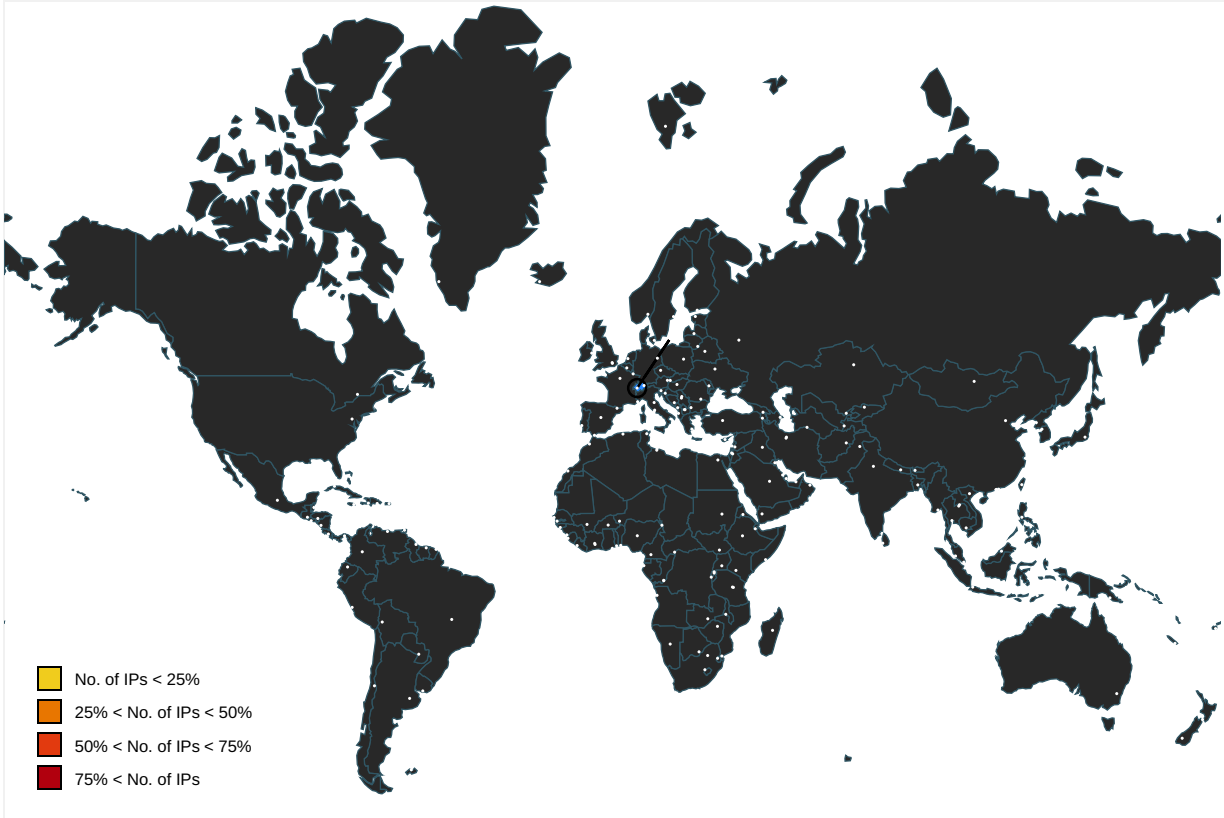
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000000007492000.00000004.00000001.sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002.357332280.0000000005DF0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000000007492000.00000004.00000001.sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002.357332280.0000000005DF0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000000007492000.00000004.00000001.sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002.357332280.0000000005DF0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000000007492000.00000004.00000001.sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002.357332280.0000000005DF0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000000007492000.00000004.00000001.sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002.357332280.0000000005DF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false		high
http://www.biblegateway.com/passage/?search=	JMG Memo-Circular No 018-21.PDF.exe	false		high
http://www.tiro.comq	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003.227665199.00000 00006288000.00000004.00000001. sdmp	false	• Avira URL Cloud: safe	unknown
http://www.esvstudybible.org/search?q=	JMG Memo-Circular No 018-21.PDF.exe	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002.357332280.00000 00005DF0000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.esvstudybible.org/search? q=Whttp://www.blueletterbible.org/Bible.cfm?b=	JMG Memo-Circular No 018-21.PDF.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002.357332280.00000 00005DF0000.00000002.00000001. sdmp	false		high
http://www.goodfont.co.kr	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003.232454691.00000 0000628D000.00000004.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://topicalmemorysystem.googlecode.com/files/	JMG Memo-Circular No 018-21.PDF.exe	false	• Avira URL Cloud: safe	unknown
http://www.biblija.net/biblija.cgi?m=	JMG Memo-Circular No 018-21.PDF.exe	false		high
http://www.founder.com.cn/cnB	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003.227574315.00000 00006288000.00000004.00000001. sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comB	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003.232454691.00000 0000628D000.00000004.00000001. sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003 .227574315.0000000006288000.00 000004.00000001.sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0 000000D.00000002.357332280.000 0000005DF0000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false		high
http://www.monotype.	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003.232848694.00000 0000628D000.00000004.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.monotype.l	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003.233327903.00000 0000628B000.00000004.00000001. sdmp	false	• Avira URL Cloud: safe	unknown
http://www.blueletterbible.org/Bible.cfm?b=	JMG Memo-Circular No 018-21.PDF.exe	false		high
http://www.jiyu-kobo.co.jp/	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false		high
http://www.fonts.com	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000 00007492000.00000004.00000001. sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002 .357332280.0000000005DF0000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.monotype.B	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003.232837315.00000 00006285000.00000004.00000001. sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.coma	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003.225859456.00000 0000629B000.00000004.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000000007492000.00000004.00000001.sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002.357332280.0000000005DF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000000007492000.00000004.00000001.sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002.357332280.0000000005DF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.278347739.00000000031C1000.00000004.00000001.sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002.349609477.0000000002E71000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.come	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003.225859456.00000000629B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000002.286703897.00000000007492000.00000004.00000001.sdmp, JMG Memo-Circular No 018-21.PDF.exe, 0000000D.00000002.357332280.0000000005DF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn(	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003.227574315.00000000006288000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.coms-e	JMG Memo-Circular No 018-21.PDF.exe, 00000000.00000003.225859456.00000000629B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.212.153.84	unknown	unknown	?	24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356480
Start date:	23.02.2021
Start time:	08:39:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JMG Memo-Circular No 018-21.PDF.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
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.evad.winEXE@15/10@15/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 100% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 131.253.33.200, 13.107.22.200, 13.64.90.137, 92.122.145.220, 40.88.32.150, 13.88.21.125, 52.255.188.83, 23.218.208.56, 51.103.5.159, 2.20.142.209, 2.20.142.210, 51.104.139.180, 92.122.213.194, 92.122.213.247, 51.11.168.160, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:39:59	API Interceptor	767x Sleep call for process: JMG Memo-Circular No 018-21.PDF.exe modified
08:40:20	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.212.153.84	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	Get hash	malicious	Browse	
	POEA ADVISORY ON DELISTED AGENCIES.PDF.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Swift copy_BILLING INVOICE.pdf.exe	Get hash	malicious	Browse	
	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	
	POEA ADVISORY NO 450 2021.pdf.exe	Get hash	malicious	Browse	
	POEA DELISTED AGENCIES (BATCH A).PDF.exe	Get hash	malicious	Browse	
	POEA MEMORANDUM N0 056.exe	Get hash	malicious	Browse	
	Protected.exe	Get hash	malicious	Browse	
	Protected.2.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shahzad73.casacam.net	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	Swift copy_BILLING INVOICE.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY NO 450 2021.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA DELISTED AGENCIES (BATCH A).PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA MEMORANDUM N0 056.exe	Get hash	malicious	Browse	• 91.212.153.84
	Protected.exe	Get hash	malicious	Browse	• 91.212.153.84
	Protected.2.exe	Get hash	malicious	Browse	• 91.212.153.84

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MYLOC-ASIPBackboneofmyLocmanagedITAGDE	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	Swift copy_BILLING INVOICE.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY NO 450 2021.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA DELISTED AGENCIES (BATCH A).PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA MEMORANDUM N0 056.exe	Get hash	malicious	Browse	• 91.212.153.84
	Swift_Payment_jpeg.exe	Get hash	malicious	Browse	• 62.141.37.17
	Protected.exe	Get hash	malicious	Browse	• 91.212.153.84
	Protected.2.exe	Get hash	malicious	Browse	• 91.212.153.84
	FickerStealer.exe	Get hash	malicious	Browse	• 89.163.225.172
	Documentaci#U00f3n.doc	Get hash	malicious	Browse	• 89.163.210.141
	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	• 89.163.140.102
	TaskAudio Driver.exe	Get hash	malicious	Browse	• 193.111.198.220
	Z8363664.doc	Get hash	malicious	Browse	• 89.163.210.141
	OhGodAnETHlargementPill2.exe	Get hash	malicious	Browse	• 193.111.198.220
	godflex-r2.exe	Get hash	malicious	Browse	• 193.111.198.220
	PolarisBiosEditor-master.exe	Get hash	malicious	Browse	• 193.111.198.220
	NKsplucdAu.exe	Get hash	malicious	Browse	• 85.114.134.88
	IZVNh1BPxm.exe	Get hash	malicious	Browse	• 85.114.134.88

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JMG Memo-Circular No 018-21.PDF.exe.log

Process:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JMG Memo-Circular No 018-21.PDF.exe.log	
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp1B75.tmp	
Process:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.16503394644957
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBqtn:cbhC7ZlNQF/rydbz9I3YODOLNdq32
MD5:	E8925C09B9BB23D063EE91146E77209B
SHA1:	1072F71BEF66C046ADCC8E9AA7E80660FCF666AA
SHA-256:	4D2ED0F58CA386198F355B70090AB55CB43F4C09FFAFC188A2CBB9B08B5D50AD
SHA-512:	BA1E7B1C9EEF7D2EBF63F797AB7217EE63C59B6C6A4B994A331546D291ACAEB05FA3AB277E901D15C76C41EC08800200C3B2D9838C532E805B284DAA4B74FF F4
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmp8F7C.tmp	
Process:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.16503394644957
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBqtn:cbhC7ZlNQF/rydbz9I3YODOLNdq32
MD5:	E8925C09B9BB23D063EE91146E77209B
SHA1:	1072F71BEF66C046ADCC8E9AA7E80660FCF666AA
SHA-256:	4D2ED0F58CA386198F355B70090AB55CB43F4C09FFAFC188A2CBB9B08B5D50AD
SHA-512:	BA1E7B1C9EEF7D2EBF63F797AB7217EE63C59B6C6A4B994A331546D291ACAEB05FA3AB277E901D15C76C41EC08800200C3B2D9838C532E805B284DAA4B74FF F4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmpC90F.tmp	
Process:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe

C:\Users\user\AppData\Local\Temp\tmpC90F.tmp

File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1322
Entropy (8bit):	5.130714996587634
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0PQxtn:cbk4oL600QydbQxIYODOLedq3SQj
MD5:	873118250D15609893AB07964F3B2366
SHA1:	87F00CD5D4F91128D2FE6ED69EFCABB87E6EDBAD
SHA-256:	43C45CFCBC19B8127ED719C7532FA1C677D2120C03755A04207E3ADE43F8BE88
SHA-512:	C9EE4356E5F62F4DFA0ABBD4BFEF76107073286E54312332BC19E92CAFC87F347DAC04D5C636C3CEDA1F315EC3D07BD291DC934259583A2686E1E786552DAF 8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <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\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhDjhL
MD5:	30D23CC577A89146961915B57F408623
SHA1:	9B5709D6081D8E0A570511E6E0AAE96FA041964F
SHA-256:	E2130A72E55193D402B5F43F7F3584ECF6B423F8EC4B1B1B69AD693C7E0E5A9E
SHA-512:	2D5C5747FD04F8326C2CC1FB313925070BC01D3352AFA6C36C167B72757A15F58B6263D96BD606338DA055812E69DDB628A6E18D64DD59697C2F42D1C58CC6
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:A9P:4
MD5:	3D84C57B91B521E65FDEE4541F112EC0
SHA1:	0D127DDC6EB4167551A63D3C27198E3FF1512618
SHA-256:	5EAE71E53B82FDBAC607F1E98BADC83B896C7615B72D1E47FA5A5518B5D2E760
SHA-512:	353A83E5354F540C99D379A015C0089B50E673869A8E395C291C21868F749AB1E1B9ED283B07500247B1DC054FD7DF0C87BA8AEF4E4AF37F77A7BA518BE71FF
Malicious:	**true**
Preview:	......H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin

Process:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wI8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3 A
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	59
Entropy (8bit):	4.846720753111607
Encrypted:	false
SSDEEP:	3:oNUWJRWv69XiKA16A:oNNJAupA0A
MD5:	255273167AB1F8F99E97AD1AD0A47F10
SHA1:	24C23E0E0627C103CA6FEF02EF506960494C4085
SHA-256:	7ED75483CB10B524E172E8DBE810B5F9871AF1DE0E1379076916E04367D9233C
SHA-512:	82817A6D63AE5247CB865723660381A9A63C05831E8EB564075134F19F0D3E2377D792A49A23C74CB18794B5305B137732E0D56E8FBD3F8834A7FE810BF6F389
Malicious:	false
Preview:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe

C:\Users\user\AppData\Roaming\GmaLrlDR.exe	
Process:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	714240
Entropy (8bit):	6.848207378321331
Encrypted:	false
SSDEEP:	12288:/GTEIGBl1jcqvSq5HGO9rHCrnaRsGFPY6:/4GJoGb586sGW
MD5:	F12D78AE2CE77B187E98B382BC400E6E
SHA1:	A4A09F0297221E8E3D8F510F139A10B30B9BB7E8
SHA-256:	019DCE879F64D1A5A23DE8AE1D0EAC08200954B26665232507187E7F524B4F24
SHA-512:	579431D0548682078764625D5557CA247371AD661483067A0A6F167DD2BBCC6597BF1EB38D1E6C1442FBA0C5FE4166B23EE088716669EE023ED40FD2D74D12FB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 12%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....n4`.....0..... .....@.. .....@..... ..@.....O..... ..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....[..t.....C.. .....}.....(.....{.....r...p~/...(....o.....{....o....&*..0.....r...p(....&.....o....&...*..... .....n..t.....o.....{....o....&*.....(.....*~..{....o.....{....o....(.....*.0..+.....,..{.....+.....,..{....o.....(...*..0.....s!...}.....("...s#.....s$...}.....s%...}.....s%...}.....{....s&...}.....s'... }.....s%...}.....s%...}.....s(...}.....{....o).....{....o)..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.848207378321331
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	JMG Memo-Circular No 018-21.PDF.exe
File size:	714240
MD5:	f12d78ae2ce77b187e98b382bc400e6e
SHA1:	a4a09f0297221e8e3d8f510f139a10b30b9bb7e8
SHA256:	019dce879f64d1a5a23de8ae1d0eac08200954b2666523 2507187e7f524b4f24
SHA512:	579431d0548682078764625d5557ca247371ad6614830 7a0a6f167dd2bbcc6597bf1eb38d1e6c1442fba0c5fe416 6b23ee088716669ee023ed40fd2d74d12fb
SSDEEP:	12288:/GTEIGBl1jcqvSq5HGO9rHCrnaRsGFPY6:/4GJ oGb586sGW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....n4`.....0..... ....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4afa12
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60346EDF [Tue Feb 23 02:56:31 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xaf9c0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb0000	0x5bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xada18	0xadc00	False	0.641475101169	data	6.85708013981	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb0000	0x5bc	0x600	False	0.427734375	data	4.17835569361	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb0090	0x32c	data		
RT_MANIFEST	0xb03cc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	5owG60.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Core.Numero
ProductVersion	1.0.0.0
FileDescription	Core.Numero
OriginalFilename	5owG60.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-08:40:22.477560	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	9036	192.168.2.5	91.212.153.84
02/23/21-08:40:31.001172	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	9036	192.168.2.5	91.212.153.84
02/23/21-08:40:38.101612	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	9036	192.168.2.5	91.212.153.84
02/23/21-08:40:44.976945	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	9036	192.168.2.5	91.212.153.84
02/23/21-08:40:52.211286	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	9036	192.168.2.5	91.212.153.84
02/23/21-08:40:59.018915	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	9036	192.168.2.5	91.212.153.84
02/23/21-08:41:06.599920	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	9036	192.168.2.5	91.212.153.84
02/23/21-08:41:15.848682	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	9036	192.168.2.5	91.212.153.84
02/23/21-08:41:22.701844	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	9036	192.168.2.5	91.212.153.84
02/23/21-08:41:29.724607	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	9036	192.168.2.5	91.212.153.84
02/23/21-08:41:34.259656	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	9036	192.168.2.5	91.212.153.84
02/23/21-08:41:40.252014	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	9036	192.168.2.5	91.212.153.84
02/23/21-08:41:45.641221	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	9036	192.168.2.5	91.212.153.84
02/23/21-08:41:53.912826	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	9036	192.168.2.5	91.212.153.84

Network Port Distribution

Total Packets: 64

- 53 (DNS)
- 9036 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:40:22.306313038 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:22.362927914 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:22.363090038 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:22.477560043 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:22.541064978 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:22.609545946 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:22.663753986 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:22.713645935 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:22.856252909 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:22.936887980 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.001763105 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.001796007 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.001812935 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.001830101 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.002203941 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.045665979 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.055763006 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.055793047 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.055939913 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.055958986 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.055980921 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.055999041 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.056015968 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.056032896 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.056036949 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.056075096 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.056081057 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.056086063 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.109719992 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109749079 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109766006 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109782934 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109798908 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109814882 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109831095 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109849930 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109869003 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109882116 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109899998 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109916925 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109920025 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.109930992 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109942913 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.109952927 CET	49718	9036	192.168.2.5	91.212.153.84

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:40:23.109956980 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109975100 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.109987020 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.109992027 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.113658905 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.113692045 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.163817883 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.163847923 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.163866043 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.163883924 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.163901091 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.163914919 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.163932085 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.163949966 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.163968086 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.163975000 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.163985968 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.164010048 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.164027929 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.164043903 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.164057016 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.164073944 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.164093971 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.164112091 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.164113045 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.164120913 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.164129019 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.164145947 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.164161921 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.164248943 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.164261103 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.164263964 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.166469097 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.166491985 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.166610003 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.166629076 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.166822910 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.166850090 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.167081118 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.167100906 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.167117119 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.167133093 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.167149067 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.167167902 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.167185068 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.167236090 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.167397976 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.167418957 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.167423010 CET	49718	9036	192.168.2.5	91.212.153.84
Feb 23, 2021 08:40:23.217665911 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.217693090 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.217711926 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.217730045 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.217746973 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.217761993 CET	9036	49718	91.212.153.84	192.168.2.5
Feb 23, 2021 08:40:23.217778921 CET	9036	49718	91.212.153.84	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:39:44.691495895 CET	64344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:44.730628014 CET	62060	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:44.740154028 CET	53	64344	8.8.8.8	192.168.2.5
Feb 23, 2021 08:39:44.779218912 CET	53	62060	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:39:45.486394882 CET	61805	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:45.543379068 CET	53	61805	8.8.8.8	192.168.2.5
Feb 23, 2021 08:39:46.681488037 CET	54795	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:46.730142117 CET	53	54795	8.8.8.8	192.168.2.5
Feb 23, 2021 08:39:47.484688997 CET	49557	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:47.541548967 CET	53	49557	8.8.8.8	192.168.2.5
Feb 23, 2021 08:39:48.200928926 CET	61733	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:48.258153915 CET	53	61733	8.8.8.8	192.168.2.5
Feb 23, 2021 08:39:48.261364937 CET	65447	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:48.312700987 CET	53	65447	8.8.8.8	192.168.2.5
Feb 23, 2021 08:39:49.133738041 CET	52441	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:49.216839075 CET	53	52441	8.8.8.8	192.168.2.5
Feb 23, 2021 08:39:50.872056007 CET	62176	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:50.921138048 CET	53	62176	8.8.8.8	192.168.2.5
Feb 23, 2021 08:39:51.670185089 CET	59596	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:51.721510887 CET	53	59596	8.8.8.8	192.168.2.5
Feb 23, 2021 08:39:52.497791052 CET	65296	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:52.549416065 CET	53	65296	8.8.8.8	192.168.2.5
Feb 23, 2021 08:39:53.853389978 CET	63183	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:53.910558939 CET	53	63183	8.8.8.8	192.168.2.5
Feb 23, 2021 08:39:55.442152023 CET	60151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:39:55.493588924 CET	53	60151	8.8.8.8	192.168.2.5
Feb 23, 2021 08:40:13.955656052 CET	56969	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:40:14.015691042 CET	53	56969	8.8.8.8	192.168.2.5
Feb 23, 2021 08:40:22.075712919 CET	55161	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:40:22.290473938 CET	53	55161	8.8.8.8	192.168.2.5
Feb 23, 2021 08:40:30.885245085 CET	54757	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:40:30.945283890 CET	53	54757	8.8.8.8	192.168.2.5
Feb 23, 2021 08:40:37.830142975 CET	49992	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:40:38.041395903 CET	53	49992	8.8.8.8	192.168.2.5
Feb 23, 2021 08:40:39.956291914 CET	60075	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:40:40.899060965 CET	53	60075	8.8.8.8	192.168.2.5
Feb 23, 2021 08:40:44.864003897 CET	55016	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:40:44.920957088 CET	53	55016	8.8.8.8	192.168.2.5
Feb 23, 2021 08:40:44.984555960 CET	64345	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:40:45.042771101 CET	53	64345	8.8.8.8	192.168.2.5
Feb 23, 2021 08:40:45.509427071 CET	57128	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:40:45.558054924 CET	53	57128	8.8.8.8	192.168.2.5
Feb 23, 2021 08:40:52.009077072 CET	54791	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:40:52.060513973 CET	53	54791	8.8.8.8	192.168.2.5
Feb 23, 2021 08:40:58.732026100 CET	50463	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:40:58.947155952 CET	53	50463	8.8.8.8	192.168.2.5
Feb 23, 2021 08:41:03.406004906 CET	50394	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:41:03.465306997 CET	53	50394	8.8.8.8	192.168.2.5
Feb 23, 2021 08:41:06.286660910 CET	58530	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:41:06.343776941 CET	53	58530	8.8.8.8	192.168.2.5
Feb 23, 2021 08:41:13.806901932 CET	53813	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:41:14.826397896 CET	53813	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:41:15.792766094 CET	53	53813	8.8.8.8	192.168.2.5
Feb 23, 2021 08:41:22.557945013 CET	63732	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:41:22.615175962 CET	53	63732	8.8.8.8	192.168.2.5
Feb 23, 2021 08:41:29.611041069 CET	57344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:41:29.668272972 CET	53	57344	8.8.8.8	192.168.2.5
Feb 23, 2021 08:41:33.882359982 CET	54450	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:41:33.936230898 CET	53	54450	8.8.8.8	192.168.2.5
Feb 23, 2021 08:41:34.144674063 CET	59261	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:41:34.203854084 CET	53	59261	8.8.8.8	192.168.2.5
Feb 23, 2021 08:41:40.148147106 CET	57151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:41:40.196775913 CET	53	57151	8.8.8.8	192.168.2.5
Feb 23, 2021 08:41:45.525274992 CET	59413	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:41:45.585443974 CET	53	59413	8.8.8.8	192.168.2.5
Feb 23, 2021 08:41:53.790009022 CET	60516	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:41:53.838754892 CET	53	60516	8.8.8.8	192.168.2.5
Feb 23, 2021 08:41:55.965818882 CET	51649	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:41:56.041786909 CET	53	51649	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:40:22.075712919 CET	192.168.2.5	8.8.8.8	0xa521	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:40:30.885245085 CET	192.168.2.5	8.8.8.8	0x43aa	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:40:37.830142975 CET	192.168.2.5	8.8.8.8	0x85c	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:40:44.864003897 CET	192.168.2.5	8.8.8.8	0xe3de	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:40:52.009077072 CET	192.168.2.5	8.8.8.8	0xe92	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:40:58.732026100 CET	192.168.2.5	8.8.8.8	0x681b	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:06.286660910 CET	192.168.2.5	8.8.8.8	0x3f0d	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:13.806901932 CET	192.168.2.5	8.8.8.8	0xe5e7	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:14.826397896 CET	192.168.2.5	8.8.8.8	0xe5e7	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:22.557945013 CET	192.168.2.5	8.8.8.8	0x924e	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:29.611041069 CET	192.168.2.5	8.8.8.8	0xfa33	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:34.144674063 CET	192.168.2.5	8.8.8.8	0x99c8	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:40.148147106 CET	192.168.2.5	8.8.8.8	0x1f1a	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:45.525274992 CET	192.168.2.5	8.8.8.8	0x31da	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:53.790009022 CET	192.168.2.5	8.8.8.8	0x4858	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)

DNS Answers

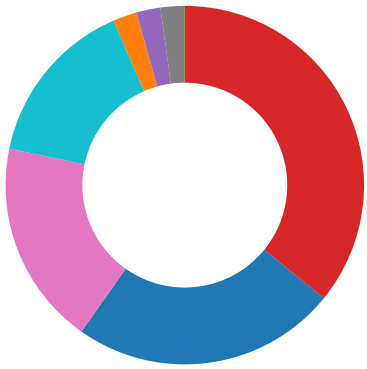
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:40:22.290473938 CET	8.8.8.8	192.168.2.5	0xa521	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:40:30.945283890 CET	8.8.8.8	192.168.2.5	0x43aa	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:40:38.041395903 CET	8.8.8.8	192.168.2.5	0x85c	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:40:44.920957088 CET	8.8.8.8	192.168.2.5	0xe3de	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:40:52.060513973 CET	8.8.8.8	192.168.2.5	0xe92	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:40:58.947155952 CET	8.8.8.8	192.168.2.5	0x681b	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:06.343776941 CET	8.8.8.8	192.168.2.5	0x3f0d	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:15.792766094 CET	8.8.8.8	192.168.2.5	0xe5e7	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:22.615175962 CET	8.8.8.8	192.168.2.5	0x924e	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:29.668272972 CET	8.8.8.8	192.168.2.5	0xfa33	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:34.203854084 CET	8.8.8.8	192.168.2.5	0x99c8	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:40.196775913 CET	8.8.8.8	192.168.2.5	0x1f1a	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:41:45.585443974 CET	8.8.8.8	192.168.2.5	0x31da	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 23, 2021 08:41:53.838754892 CET	8.8.8.8	192.168.2.5	0x4858	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



- JMG Memo-Circular No 018-21.PDF.
- schtasks.exe
- conhost.exe
- JMG Memo-Circular No 018-21.PDF.
- schtasks.exe
- conhost.exe
- JMG Memo-Circular No 018-21.PDF.
- schtasks.exe
- conhost.exe
- JMG Memo-Circular No 018-21.PDF.

Click to jump to process

System Behavior

Analysis Process: JMG Memo-Circular No 018-21.PDF.exe PID: 3540 Parent PID: 5740

General

Start time:	08:39:52
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe'
Imagebase:	0xe50000
File size:	714240 bytes
MD5 hash:	F12D78AE2CE77B187E98B382BC400E6E
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: 00000000.00000002.280456931.00000000041C9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.280456931.00000000041C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.280456931.00000000041C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DABCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DABCF06	unknown
C:\Users\user\AppData\Roaming\GmaLrlDR.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C901E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp1B75.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C907038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JMG Memo-Circular No 018-21.PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDCC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1B75.tmp	success or wait	1	6C906A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GmaLrlDR.exe	unknown	714240	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 df 6e 34 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 dc 0a 00 00 08 00 00 00 00 00 00 12 fa 0a 00 00 20 00 00 00 00 0b 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 40 0b 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....n4`.......... ....0................. ....@.. ....@ ....@................	success or wait	1	6C901B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1B75.tmp	unknown	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	6C901B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JMG Memo-Circular No 018-21.PDF.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DDCC907	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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile
C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe	unknown	714240	success or wait	1	6C901B4F	ReadFile

Analysis Process: schtasks.exe PID: 6568 Parent PID: 3540

General

Start time:	08:40:15
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GmaLrlDR' /XML 'C:\Users \user\AppData\Local\Temp\tmp1B75.tmp'
Imagebase:	0x9a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1B75.tmp	unknown	2	success or wait	1	9AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1B75.tmp	unknown	1646	success or wait	1	9AABD9	ReadFile

Analysis Process: conhost.exe PID: 6576 Parent PID: 6568

General

Start time:	08:40:16
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: JMG Memo-Circular No 018-21.PDF.exe PID: 6628 Parent PID: 3540

General

Start time:	08:40:16
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x710000
File size:	714240 bytes
MD5 hash:	F12D78AE2CE77B187E98B382BC400E6E
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: 00000007.00000002.501005046.0000000006DD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.501005046.0000000006DD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.498456853.0000000005380000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.498456853.0000000005380000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.501098807.0000000006E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.501098807.0000000006E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.492270047.0000000002BFD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.496807047.0000000003E81000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.500985326.0000000006DC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.500985326.0000000006DC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.501114313.0000000006E20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.501114313.0000000006E20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.500970500.0000000006DB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.500970500.0000000006DB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.500950111.0000000006DA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.500950111.0000000006DA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.500819703.0000000006BF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.500819703.0000000006BF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.501154629.0000000006E60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.501154629.0000000006E60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.496443867.0000000003BE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.501030742.0000000006DE0000.00000004.00000001.sdmp, Author: Florian Roth

	• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.501030742.0000000006DE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.500935667.0000000006D90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.500935667.0000000006D90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.498042432.0000000005230000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.498042432.0000000005230000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.498042432.0000000005230000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.496714685.0000000003DA4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.496714685.0000000003DA4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.488093735.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.488093735.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.488093735.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.492154123.0000000002B91000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.501047468.0000000006DF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.501047468.0000000006DF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.497599353.0000000005170000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.497599353.0000000005170000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DABCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DABCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C90BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C901E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpC90F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C907038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C901E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C90BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C90BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	9	6C901E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C901E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C901E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC90F.tmp	success or wait	1	6C906A95	DeleteFileW
C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe:Zone.Identifier	success or wait	1	5167E96	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	e3 01 e4 b4 19 d8 d8 48	.....H	success or wait	1	6C901B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpC90F.tmp	unknown	1322	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	6C901B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	59	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 4a 4d 47 20 4d 65 6d 6f 2d 43 69 72 63 75 6c 61 72 20 4e 6f 20 30 31 38 2d 32 31 2e 50 44 46 2e 65 78 65	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe	success or wait	1	6C901B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^....;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	8	6C901B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327768	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_...Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6C901B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6C901B4F	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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile
C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe	unknown	4096	success or wait	1	6DA7D72F	unknown
C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe	unknown	512	success or wait	1	6DA7D72F	unknown

Analysis Process: schtasks.exe PID: 6864 Parent PID: 6628

General

Start time:	08:40:19
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpC90F.tmp'
Imagebase:	0x9a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC90F.tmp	unknown	2	success or wait	1	9AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC90F.tmp	unknown	1323	success or wait	1	9AABD9	ReadFile

Analysis Process: conhost.exe PID: 6888 Parent PID: 6864

General

Start time:	08:40:19
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: JMG Memo-Circular No 018-21.PDF.exe PID: 7000 Parent PID: 904

General

Start time:	08:40:20
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe' 0
Imagebase:	0x870000
File size:	714240 bytes
MD5 hash:	F12D78AE2CE77B187E98B382BC400E6E
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: 0000000D.00000002.352208720.0000000003E79000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.352208720.0000000003E79000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.352208720.0000000003E79000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DABCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DABCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp8F7C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C907038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8F7C.tmp	success or wait	1	6C906A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8F7C.tmp	unknown	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	6C901B4F	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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile

Analysis Process: schtasks.exe PID: 5660 Parent PID: 7000

General

Start time:	08:40:46
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GmaLrlDR' /XML 'C:\Users\user\AppData\Local\Temp\tmp8F7C.tmp'
Imagebase:	0xd80000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04

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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8F7C.tmp	unknown	2	success or wait	1	D8AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8F7C.tmp	unknown	1646	success or wait	1	D8ABD9	ReadFile

Analysis Process: conhost.exe PID: 5716 Parent PID: 5660

General

Start time:	08:40:46
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: JMG Memo-Circular No 018-21.PDF.exe PID: 6376 Parent PID: 7000

General

Start time:	08:40:47
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\JMG Memo-Circular No 018-21.PDF.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd60000
File size:	714240 bytes
MD5 hash:	F12D78AE2CE77B187E98B382BC400E6E
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: 00000013.00000002.366475568.0000000003151000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.366475568.0000000003151000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.366560257.0000000004159000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.366560257.0000000004159000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.365338773.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.365338773.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.365338773.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DABCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DABCF06	unknown

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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile

Disassembly

Code Analysis