
**ID:** 553030
**Sample Name:**
PO#0065026.doc.exe
**Cookbook:** default.jbs
**Time:** 06:17:19
**Date:** 14/01/2022
**Version:** 34.0.0 Boulder Opal

# Table of Contents

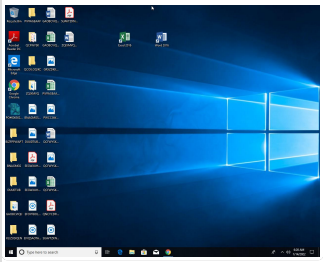
# Windows Analysis Report PO#0065026.doc.exe

## Overview

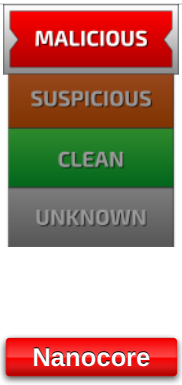
### General Information

| | |
|---|---|
| Sample Name: | PO#0065026.doc.exe |
| Analysis ID: | 553030 |
| MD5: | 23306452598466.. |
| SHA1: | 91bec44a6ff58c2.. |
| SHA256: | 30e1ba61a63a27.. |
| Tags: | exe NanoCore RAT |
| Infos: | |

Most interesting Screenshot:



### Detection

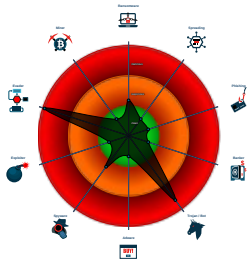



| | |
|---|---|
| Score: | 100 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Detected unpacking (overwrites its o…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…

### Classification



## Process Tree

- **System is w10x64**
- PO#0065026.doc.exe (PID: 7096 cmdline: "C:\Users\user\Desktop\PO#0065026.doc.exe" MD5: 233064525984666FE973125F4E60C903)
  - PO#0065026.doc.exe (PID: 5348 cmdline: C:\Users\user\Desktop\PO#0065026.doc.exe MD5: 233064525984666FE973125F4E60C903)
    - schtasks.exe (PID: 6524 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp71C5.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6664 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6724 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp7E78.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- PO#0065026.doc.exe (PID: 6712 cmdline: C:\Users\user\Desktop\PO#0065026.doc.exe 0 MD5: 233064525984666FE973125F4E60C903)
  - PO#0065026.doc.exe (PID: 7160 cmdline: C:\Users\user\Desktop\PO#0065026.doc.exe MD5: 233064525984666FE973125F4E60C903)
- dhcpmon.exe (PID: 7112 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 233064525984666FE973125F4E60C903)
- dhcpmon.exe (PID: 1312 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 233064525984666FE973125F4E60C903)
  - dhcpmon.exe (PID: 6616 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 233064525984666FE973125F4E60C903)
  - dhcpmon.exe (PID: 6592 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 233064525984666FE973125F4E60C903)
  - BackgroundTransferHost.exe (PID: 6616 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
- **cleanup**

## Malware Configuration

### Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "1122355e-5fe3-470d-a458-8c4cf035",
  "Group": "Default",
  "Domain1": "185.140.53.132",
  "Domain2": "127.0.0.1",
  "Port": 1604,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000016.00000000.366825626.000000000402000.00000040.00000001.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xff8d:$x1: NanoCore.ClientPluginHost<br>• 0xffca:$x2: IClientNetworkHost<br>• 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| 00000016.00000000.366825626.000000000402000.00000040.00000001.sdmp | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| 00000016.00000000.366825626.000000000402000.00000040.00000001.sdmp | NanoCore | unknown | Kevin Breen <kevin@techanarchy.net> | • 0xfcf5:$a: NanoCore<br>• 0xfd05:$a: NanoCore<br>• 0xff39:$a: NanoCore<br>• 0xff4d:$a: NanoCore<br>• 0xff8d:$a: NanoCore<br>• 0xfd54:$b: ClientPlugin<br>• 0xff56:$b: ClientPlugin<br>• 0xff96:$b: ClientPlugin<br>• 0xfe7b:$c: ProjectData<br>• 0x10882:$d: DESCrypto<br>• 0x1824e:$e: KeepAlive<br>• 0x1623c:$g: LogClientMessage<br>• 0x12437:$i: get_Connected<br>• 0x10bb8:$j: #=q<br>• 0x10be8:$j: #=q<br>• 0x10c04:$j: #=q<br>• 0x10c34:$j: #=q<br>• 0x10c50:$j: #=q<br>• 0x10c6c:$j: #=q<br>• 0x10c9c:$j: #=q<br>• 0x10cb8:$j: #=q |
| 00000013.00000000.333627100.000000000402000.00000040.00000001.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xff8d:$x1: NanoCore.ClientPluginHost<br>• 0xffca:$x2: IClientNetworkHost<br>• 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| 00000013.00000000.333627100.000000000402000.00000040.00000001.sdmp | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |

Click to see the 80 entries

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 1.2.PO#0065026.doc.exe.5131b38.5.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xe38d:$x1: NanoCore.ClientPluginHost<br>• 0xe3ca:$x2: IClientNetworkHost<br>• 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| 1.2.PO#0065026.doc.exe.5131b38.5.unpack | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0xe105:$x1: NanoCore Client.exe<br>• 0xe38d:$x2: NanoCore.ClientPluginHost<br>• 0xf9c6:$s1: PluginCommand<br>• 0xf9ba:$s2: FileCommand<br>• 0x1086b:$s3: PipeExists<br>• 0x16622:$s4: PipeCreated<br>• 0xe3b7:$s5: IClientLoggingHost |
| 1.2.PO#0065026.doc.exe.5131b38.5.unpack | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| 1.2.PO#0065026.doc.exe.5131b38.5.unpack | NanoCore | unknown | Kevin Breen <kevin@techanarchy.net> | • 0xe0f5:$a: NanoCore<br>• 0xe105:$a: NanoCore<br>• 0xe339:$a: NanoCore<br>• 0xe34d:$a: NanoCore<br>• 0xe38d:$a: NanoCore<br>• 0xe154:$b: ClientPlugin<br>• 0xe356:$b: ClientPlugin<br>• 0xe396:$b: ClientPlugin<br>• 0xe27b:$c: ProjectData<br>• 0xec82:$d: DESCrypto<br>• 0x1664e:$e: KeepAlive<br>• 0x1463c:$g: LogClientMessage<br>• 0x10837:$i: get_Connected<br>• 0xefb8:$j: #=q<br>• 0xefe8:$j: #=q<br>• 0xf004:$j: #=q<br>• 0xf034:$j: #=q<br>• 0xf050:$j: #=q<br>• 0xf06c:$j: #=q<br>• 0xf09c:$j: #=q<br>• 0xf0b8:$j: #=q |
| 19.0.PO#0065026.doc.exe.400000.8.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x1018d:$x1: NanoCore.ClientPluginHost<br>• 0x101ca:$x2: IClientNetworkHost<br>• 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| Click to see the 142 entries | | | | |

# Sigma Overview

**AV Detection:**

**Sigma detected: NanoCore**

**E-Banking Fraud:**

**Sigma detected: NanoCore**

**System Summary:**

**Sigma detected: Suspicious Double Extension**

**Sigma detected: Suspicius Add Task From User AppData Temp**

**Stealing of Sensitive Information:**

**Sigma detected: NanoCore**

**Remote Access Functionality:**

**Sigma detected: NanoCore**

# Jbx Signature Overview

Click to jump to signature section

## AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for dropped file
- Yara detected Nanocore RAT
- Machine Learning detection for sample
- Machine Learning detection for dropped file

## Compliance:

- Detected unpacking (overwrites its own PE header)

## 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:

- Detected unpacking (overwrites its own PE header)
- Detected unpacking (changes PE section rights)
- .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)

## Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

## HIPS / PFW / Operating System Protection Evasion:

- Injects a PE file into a foreign processes

## Stealing of Sensitive Information:

Yara detected Nanocore RAT

## Remote Access Functionality:

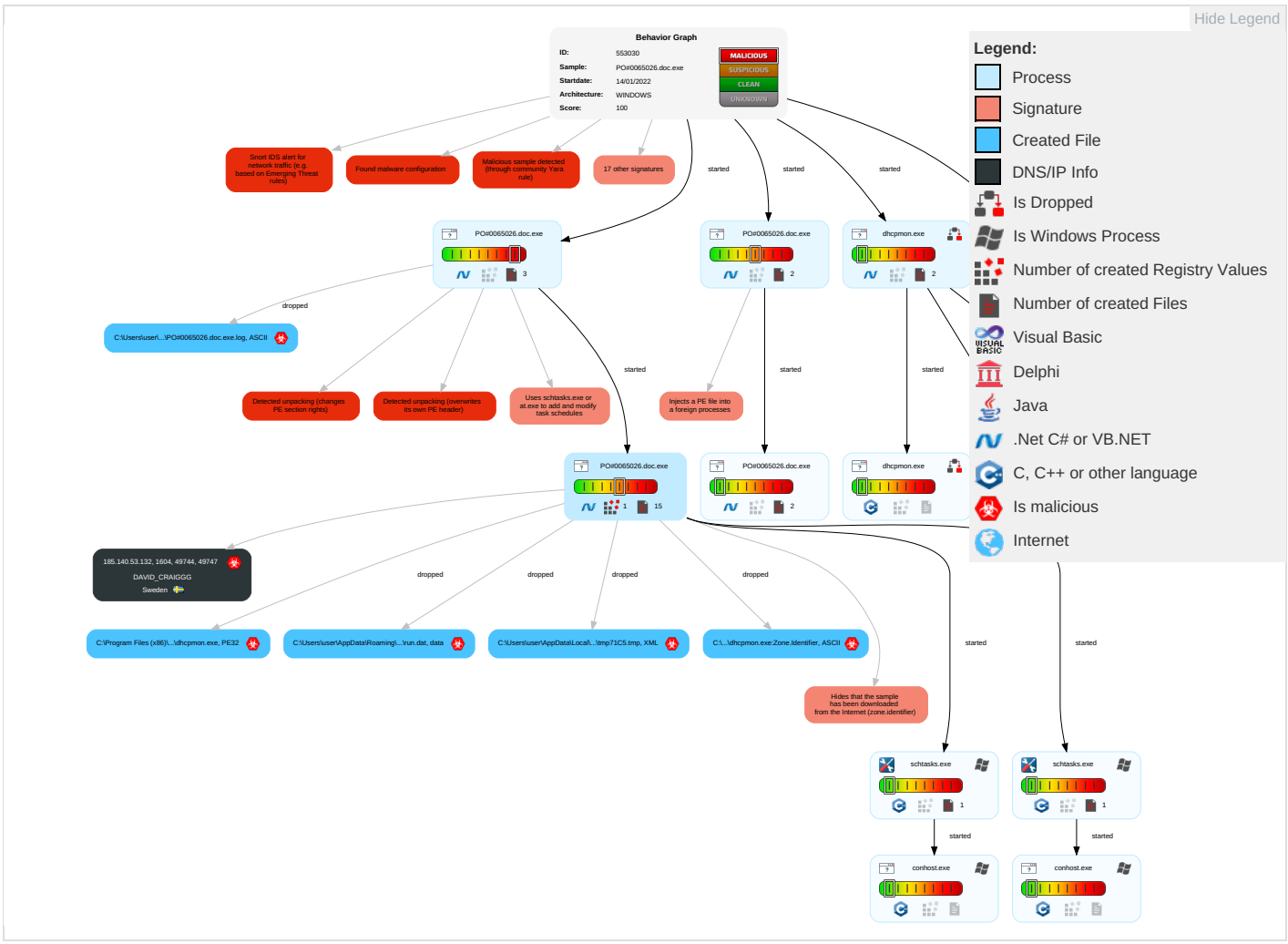
Detected Nanocore Rat

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 1 | Masquerading 1 2 | Input Capture 1 1 | Security Software Discovery 2 1 1 | Remote Services | Input Capture 1 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 |
| Default Accounts | Scheduled Task/Job 1 | Boot or Logon Initialization Scripts | Scheduled Task/Job 1 | Disable or Modify Tools 1 | LSASS Memory | Process Discovery 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) | Virtualization/Sandbox Evasion 2 1 | Security Account Manager | Virtualization/Sandbox Evasion 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 1 | NTDS | Application Window Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 1 |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Deobfuscate/Decode Files or Information 1 | LSA Secrets | System Information Discovery 1 2 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Hidden Files and Directories 1 | Cached Domain Credentials | System Owner/User Discovery | 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 | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Software Packing 3 2 | Proc Filesystem | Network Service Scanning | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol |

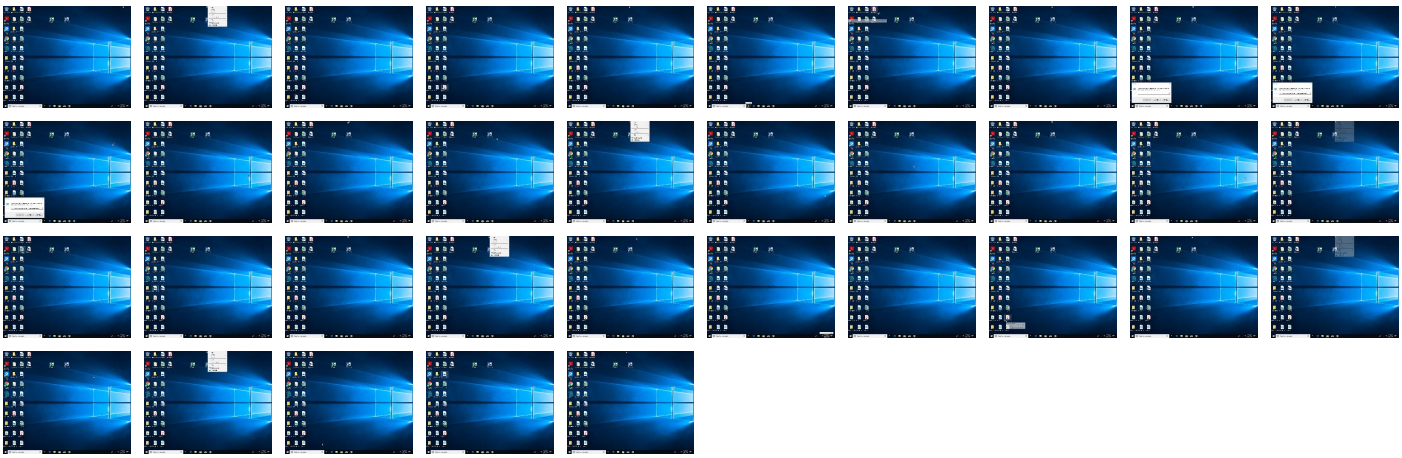
# Behavior Graph




## Screenshots

### Thumbnails

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




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| PO#0065026.doc.exe | 23% | ReversingLabs | ByteCode-MSIL.Trojan.NanoBot | |
| PO#0065026.doc.exe | 100% | Joe Sandbox ML | | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe | 100% | Joe Sandbox ML | | |
| C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe | 23% | ReversingLabs | ByteCode-MSIL.Trojan.NanoBot | |

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 17.2.dhcpmon.exe.d0000.0.unpack | 100% | Avira | HEUR/AGEN.1109526 | | Download File |
| 19.0.PO#0065026.doc.exe.400000.10.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 22.0.dhcpmon.exe.400000.10.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 19.0.PO#0065026.doc.exe.400000.12.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 10.0.PO#0065026.doc.exe.400000.4.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 19.0.PO#0065026.doc.exe.400000.8.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 10.0.PO#0065026.doc.exe.400000.10.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 19.0.PO#0065026.doc.exe.400000.6.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 19.0.PO#0065026.doc.exe.400000.4.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 10.0.PO#0065026.doc.exe.400000.12.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 22.0.dhcpmon.exe.400000.12.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 10.0.PO#0065026.doc.exe.400000.6.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 1.2.PO#0065026.doc.exe.ee0000.0.unpack | 100% | Avira | HEUR/AGEN.1109526 | | Download File |
| 20.2.dhcpmon.exe.ba0000.0.unpack | 100% | Avira | HEUR/AGEN.1109526 | | Download File |
| 22.0.dhcpmon.exe.400000.8.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 13.2.PO#0065026.doc.exe.f10000.0.unpack | 100% | Avira | HEUR/AGEN.1109526 | | Download File |
| 22.0.dhcpmon.exe.400000.4.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 10.0.PO#0065026.doc.exe.400000.8.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 22.0.dhcpmon.exe.400000.6.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 22.2.dhcpmon.exe.400000.0.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 19.2.PO#0065026.doc.exe.400000.0.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |

## Domains

**No Antivirus matches**

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.jiyu-kobo.co.jp/uro | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.comn-u | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/-hu | 0% | Avira URL Cloud | safe | |
| http://www.zhongyicts.com.cnaU | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comttod | 0% | Avira URL Cloud | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/Y0/O | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comTTF | 0% | URL Reputation | safe | |
| http://www.goodfont.co.kr | 0% | URL Reputation | safe | |
| http://www.carterandcone.com | 0% | URL Reputation | safe | |
| http://www.fontbureau.comitu/D | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comionaY | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comalsF | 0% | URL Reputation | safe | |
| http://www.carterandcone.compef6K | 0% | Avira URL Cloud | safe | |
| http://www.sajatypeworks.com | 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.galapagosdesign.com/staff/dennis.htm | 0% | URL Reputation | safe | |
| http://fontfabrik.com | 0% | URL Reputation | safe | |
| http://www.carterandcone.comaU | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/jp/c | 0% | URL Reputation | safe | |
| http://www.fontbureau.comcom | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cnt | 0% | URL Reputation | safe | |
| http://www.galapagosdesign.com/DPlease | 0% | URL Reputation | safe | |
| http://www.fontbureau.comcomFc | 0% | Avira URL Cloud | safe | |
| http://www.sandoll.co.kr | 0% | URL Reputation | safe | |
| http://www.urwpp.deDPlease | 0% | URL Reputation | safe | |
| http://www.zhongyicts.com.cn | 0% | URL Reputation | safe | |
| http://www.galapagosdesign.com/CD | 0% | Avira URL Cloud | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| 127.0.0.1 | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comalsd | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/hi | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/Y | 0% | URL Reputation | safe | |
| http://www.galapagosdesign.com/ | 0% | URL Reputation | safe | |
| http://www.fontbureau.comue | 0% | URL Reputation | safe | |
| http://www.fontbureau.comF | 0% | URL Reputation | safe | |
| http://www.fontbureau.comaO | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/V | 0% | URL Reputation | safe | |
| http://www.carterandcone.comuesDK | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/O | 0% | URL Reputation | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.galapagosdesign.com/V | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comaV | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comY | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comdc | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comda | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comzana | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/D | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/jp/ | 0% | URL Reputation | safe | |
| http://www.fontbureau.coma | 0% | URL Reputation | safe | |
| http://www.fontbureau.come.com | 0% | URL Reputation | safe | |
| http://www.carterandcone.coml | 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.jiyu-kobo.co.jp/ite | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.compe | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/Y0-f | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/ | 0% | URL Reputation | safe | |
| http://www.fontbureau.como | 0% | URL Reputation | safe | |
| http://www.fontbureau.comFc | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/c | 0% | URL Reputation | safe | |
| 185.140.53.132 | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.commcom | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| 127.0.0.1 | true | • Avira URL Cloud: safe | unknown |
| 185.140.53.132 | true | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 185.140.53.132 | unknown | Sweden | | 209623 | DAVID_CRAIGGG | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 553030 |
| Start date: | 14.01.2022 |
| Start time: | 06:17:19 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 13m 7s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | PO#0065026.doc.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: | 34 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.evad.winEXE@19/11@0/1 |
| EGA Information: | • Successful, ratio: 71.4% |
| HDC Information: | • Successful, ratio: 3.1% (good quality ratio 1.6%)<br>• Quality average: 30.1%<br>• Quality standard deviation: 33.9% |
| HCA Information: | • Successful, ratio: 97%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 06:18:18 | API Interceptor | 895x Sleep call for process: PO#0065026.doc.exe modified |
| 06:18:28 | Task Scheduler | Run new task: DHCP Monitor path: "C:\Users\user\Desktop\PO#0065026.doc.exe" s>$(Arg0) |
| 06:18:29 | Autostart | Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| 06:18:31 | Task Scheduler | Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0) |
| 06:18:37 | API Interceptor | 3x Sleep call for process: dhcpmon.exe modified |

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

**No context**

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

## Created / dropped Files

| C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 1605632 |
| Entropy (8bit): | 6.867701113625518 |
| Encrypted: | false |
| SSDEEP: | 24576:n4qAtkN+Nvs0rQp5bafs2OrHbja8+GefT1:nQkUNlrEbafcrHbja8+GefT |
| MD5: | 233064525984666FE973125F4E60C903 |
| SHA1: | 91BEC44A6FF58C22CC58122B2DAAB04FD54DCF8E |
| SHA-256: | 30E1BA61A63A27B668EEE09F960A83D944E878C33B46F85EA86BACDF1427F4DD |
| SHA-512: | 9122F40F10F25B63362FF216E01A2E82271ED6CC9E81F8CB8D77FBD016FD50E11874E7D24A70C97004949E450589C015213DCA68ED7BB1FD7472B7CF24CE79E |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100%<br>• Antivirus: ReversingLabs, Detection: 23% |
| Reputation: | unknown |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..... .....@.. ..... ..@.....x...S..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....~.....@..B.....H.....C.....$...H2...v.....1o..s++./....5..30..+F..7P.#...d?...../)..V.B....-..v..A..FQ3..0...O.f.iw.....7....dE.Q.[..... .s.Y...^.].>.`...{x.....7...:l._(.F@.UE.s.\h.]...V.E..q....\.E'...+...,..R..A.....,...[sAo.+...0.C....\..G.....;e..{..sD.....<Ju.....g`8>$)...i..Dqa/.....^.....6.....,_.....jy.=.F....D?. .k.....].w....aF...D..h.l.>...C.....BX`.d."t..;.2.b...7g.[..y.+.....#...L |

| C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier | |
|---|---|
| Process: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 26 |
| Entropy (8bit): | 3.95006375643621 |
| Encrypted: | false |
| SSDEEP: | 3:ggPYV:rPYV |
| MD5: | 187F488E27DB4AF347237FE461A079AD |
| SHA1: | 6693BA299EC1881249D59262276A0D2CB21F8E64 |
| SHA-256: | 255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309 |
| SHA-512: | 89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 |
| Malicious: | **true** |
| Reputation: | unknown |
| Preview: | [ZoneTransfer]....ZoneId=0 |

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#0065026.doc.exe.log | |
|---|---|
| Process: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1302 |
| Entropy (8bit): | 5.3499841584777394 |
| Encrypted: | false |
| SSDEEP: | 24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x84j:MIHK5HKXE1qHbHK5AHKzvRYHKhQnoPtW |
| MD5: | E2C3A19FF3EBB1649BF9F41DFE3B7E8F |
| SHA1: | 5DA8AB9561D3C096BB9103413F64EE6E50D5AD88 |
| SHA-256: | 18E921771341555EF6167DEBBD7C83727518897E9B4B3545B7CCDB48E2043B74 |
| SHA-512: | 6B62A68EC358699D55E4CCD0BBDD4ADDC0F38641D82A019697893CEB503E853A5F087FAF9F4408425AD6631C9CBA31C3354FD98B45F051F2F59A0ECC3CA2FA 6 |
| Malicious: | **true** |
| Reputation: | unknown |
| 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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",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\assem |

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log | |
|---|---|
| Process: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1302 |
| Entropy (8bit): | 5.3499841584777394 |
| Encrypted: | false |
| SSDEEP: | 24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x84j:MIHK5HKXE1qHbHK5AHKzvRYHKhQnoPtW |
| MD5: | E2C3A19FF3EBB1649BF9F41DFE3B7E8F |
| SHA1: | 5DA8AB9561D3C096BB9103413F64EE6E50D5AD88 |
| SHA-256: | 18E921771341555EF6167DEBBD7C83727518897E9B4B3545B7CCDB48E2043B74 |
| SHA-512: | 6B62A68EC358699D55E4CCD0BBDD4ADDC0F38641D82A019697893CEB503E853A5F087FAF9F4408425AD6631C9CBA31C3354FD98B45F051F2F59A0ECC3CA2FA6 |
| Malicious: | false |
| Reputation: | unknown |
| 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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",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\assem |

| C:\Users\user\AppData\Local\Temp\tmp71C5.tmp | |
|---|---|
| Process: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1304 |
| Entropy (8bit): | 5.125174265894056 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Dzxtn:cbk4oL600QydbQxIYODOLedq3Ezj |
| MD5: | D7630CB1A0DA72CB2D665DCB21B85C5C |
| SHA1: | 62C73470FF8F388E106F6F06AE389987DC6E423F |
| SHA-256: | BDAB7EE10F2EC71260AC278E04869D1F9DF157CDC2BC6C6E76A01DCCE9685C0F |
| SHA-512: | EF37DEFF646A3F6DFFC33436706C9C084F59B6B4219FBD608E5B31DF32FC453D4FCD31A61C0F8F663E3E1DF9742A1FA59EAC766E457BDA6A5F62A3274C689E5 |
| Malicious: | **true** |
| Reputation: | unknown |
| Preview: | <?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak |

| C:\Users\user\AppData\Local\Temp\tmp7E78.tmp | |
|---|---|
| Process: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1310 |
| Entropy (8bit): | 5.109425792877704 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j |
| MD5: | 5C2F41CFC6F988C859DA7D727AC2B62A |
| SHA1: | 68999C85FC7E37BAB9216E0099836D40D4545C1C |
| SHA-256: | 98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B |
| SHA-512: | B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733 |
| Malicious: | false |
| Reputation: | unknown |
| 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\PO#0065026.doc.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 232 |
| Entropy (8bit): | 7.024371743172393 |
| Encrypted: | false |
| SSDEEP: | 6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9 |
| MD5: | 32D0AAE13696FF7F8AF33B2D22451028 |
| SHA1: | EF80C4E0DB2AE8EF288027C9D3518E6950B583A4 |
| SHA-256: | 5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29 |
| SHA-512: | 1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&. |

| C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat | |
|---|---|
| Process: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 8 |
| Entropy (8bit): | 3.0 |
| Encrypted: | false |
| SSDEEP: | 3:Iz:Iz |
| MD5: | 94CA9341866AED685B952D4AAA9879D0 |
| SHA1: | 80A1DFEED24F70C5DA45A82CC5FE6650A467B903 |
| SHA-256: | 6A1E2163FCEC87FE3D826AFC6F3791C90348D22C23332ABB4A82E50C38398113 |
| SHA-512: | 585EA033946428E92A89BDF3E4FED242ED0B86D93F46597667D6969AEFCAE8FE5EDA29F03B6F731489170DF3B0E6E52C1E6A57404AD525BCB105CBD86F2E5652 |
| Malicious: | **true** |
| Reputation: | unknown |
| Preview: | ..h..H |

| C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin | |
|---|---|
| Process: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| File Type: | data |
| Category: | modified |
| Size (bytes): | 40 |
| Entropy (8bit): | 5.153055907333276 |
| Encrypted: | false |
| SSDEEP: | 3:9bzY6oRDT6P2bfVn1:RzWDT621 |
| MD5: | 4E5E92E2369688041CC82EF9650EDED2 |
| SHA1: | 15E44F2F3194EE232B44E9684163B6F66472C862 |
| SHA-256: | F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48 |
| SHA-512: | 1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB |
| Malicious: | false |
| Reputation: | unknown |
| 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\PO#0065026.doc.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 327432 |
| Entropy (8bit): | **7.99938831605763** |
| Encrypted: | **true** |
| SSDEEP: | 6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm |
| MD5: | 7E8F4A764B981D5B82D1CC49D341E9C6 |
| SHA1: | D9F0685A028FB219E1A6286AEFB7D6FCFC778B85 |
| SHA-256: | 0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480 |
| SHA-512: | 880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92 |

| C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat | |
|---|---|
| Malicious: | false |
| Reputation: | unknown |
| 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\PO#0065026.doc.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 41 |
| Entropy (8bit): | 4.491459931341817 |
| Encrypted: | false |
| SSDEEP: | 3:oNWXp5v1qbXhTn:oNWXpFgdT |
| MD5: | E155CE7B2273DFE68ACA42D13A0BCDD3 |
| SHA1: | 63D30E43FE6A829CE3AFF6F173C919A0090E49AB |
| SHA-256: | 474F89C669509186781A2CAA73F699FE498A43E420A5484421AA7706ACB572CA |
| SHA-512: | 4C884C6E632E6072087174692102A215DF27B67BD2A97566DFDA14EC15ED05A13C53085F100A600A45B44BDBBCB56BE79B04B542BAF355301F0A1A5AF2E0701 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | C:\Users\user\Desktop\PO#0065026.doc.exe |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 6.867701113625518 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.83%<br>• Win32 Executable (generic) a (10002005/4) 49.78%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Generic Win/DOS Executable (2004/3) 0.01%<br>• DOS Executable Generic (2002/1) 0.01% |
| File name: | PO#0065026.doc.exe |
| File size: | 1605632 |
| MD5: | 233064525984666fe973125f4e60c903 |
| SHA1: | 91bec44a6ff58c22cc58122b2daab04fd54dcf8e |
| SHA256: | 30e1ba61a63a27b668eee09f960a83d944e878c33b46f85 ea86bacdf1427f4dd |
| SHA512: | 9122f40f10f25b63362ff216e01a2e82271ed6cc9e81f8cb 8d77fbd016fd50e11874e7d24a70c97004949e450589c01 5213dca68ed7bb1fd7472b7cf24ce79ed |
| SSDEEP: | 24576:n4qAtkN+Nvs0rQp5bafs2OrHbja8+GefT1:nQkU NlrEbafcrHbja8+GefT |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... .a.....0..... ..... .....@.. ..... @..... |

## File Icon

| | |
|---|---|
| Icon Hash: | d8993890949c64a4 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x52ecce |

### General

| | |
|---|---|
| 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: | 0x61E0F8C7 [Fri Jan 14 04:15:03 2022 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

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x2000 | 0x12ccd4 | 0x12ce00 | False | 0.624642968425 | data | 7.06155313656 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x130000 | 0x5ad08 | 0x5ae00 | False | 0.280215676582 | data | 5.3185705094 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x18c000 | 0xc | 0x200 | False | 0.044921875 | data | 0.101910425663 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 01/14/22-06:18:31.903919 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49744 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:18:38.386653 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49747 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:18:45.673562 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49748 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:18:51.870370 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49749 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:18:57.991593 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49750 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:19:03.949221 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49752 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:19:10.637670 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49769 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:19:16.757844 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49788 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:19:22.767026 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49794 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:19:28.811657 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49796 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:19:35.076661 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49811 | 1604 | 192.168.2.3 | 185.140.53.132 |

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 01/14/22-06:19:42.006820 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49820 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:19:48.060858 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49822 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:19:53.986644 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49823 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:20:00.581076 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49824 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:20:07.178570 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49825 | 1604 | 192.168.2.3 | 185.140.53.132 |
| 01/14/22-06:20:13.191702 | TCP | 2025019 | ET TROJAN Possible NanoCore C2 60B | 49826 | 1604 | 192.168.2.3 | 185.140.53.132 |

### Network Port Distribution

### TCP Packets

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: PO#0065026.doc.exe PID: 7096 Parent PID: 2228

#### General

| | |
|---|---|
| Start time: | 06:18:09 |
| Start date: | 14/01/2022 |
| Path: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\PO#0065026.doc.exe" |
| Imagebase: | 0xee0000 |
| File size: | 1605632 bytes |
| MD5 hash: | 233064525984666FE973125F4E60C903 |
| 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: 00000001.00000002.312409953.0000000004FF0000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.312409953.0000000004FF0000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000001.00000002.312409953.0000000004FF0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.306051032.0000000003510000.00000004.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Written

#### File Read

## Analysis Process: PO#0065026.doc.exe PID: 5348 Parent PID: 7096

### General

| | |
|---|---|
| Start time: | 06:18:19 |
| Start date: | 14/01/2022 |
| Path: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| Imagebase: | 0x950000 |
| File size: | 1605632 bytes |
| MD5 hash: | 233064525984666FE973125F4E60C903 |
| 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: 0000000A.00000000.300740890.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.300740890.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.300740890.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.302917559.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.302917559.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.302917559.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.300022383.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.300022383.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.300022383.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.301457212.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.301457212.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.301457212.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Reputation: | low |

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

## Analysis Process: schtasks.exe PID: 6524 Parent PID: 5348

### General

| | |
|---|---|
| Start time: | 06:18:25 |
| Start date: | 14/01/2022 |
| 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\tmp71C5.tmp |
| Imagebase: | 0xef0000 |
| 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 — Show Windows behavior

File Read

## Analysis Process: conhost.exe PID: 6664 Parent PID: 6524

### General

| | |
|---|---|
| Start time: | 06:18:27 |
| Start date: | 14/01/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| 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: PO#0065026.doc.exe PID: 6712 Parent PID: 664

### General

| | |
|---|---|
| Start time: | 06:18:28 |
| Start date: | 14/01/2022 |
| Path: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\PO#0065026.doc.exe 0 |
| Imagebase: | 0xf10000 |
| File size: | 1605632 bytes |
| MD5 hash: | 233064525984666FE973125F4E60C903 |
| 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.00000002.352052455.0000000004E90000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.352052455.0000000004E90000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.352052455.0000000004E90000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000D.00000002.342454786.00000000033B0000.00000004.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Read

## Analysis Process: schtasks.exe PID: 6724 Parent PID: 5348

### General

| | |
|---|---|
| Start time: | 06:18:29 |
| Start date: | 14/01/2022 |
| Path: | C:\Windows\SysWOW64\schtasks.exe |
| Wow64 process (32bit): | true |
| Commandline: | schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp7E78.tmp |
| Imagebase: | 0xef0000 |
| 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

Show Windows behavior

#### File Read

## Analysis Process: conhost.exe PID: 6604 Parent PID: 6724

### General

| | |
|---|---|
| Start time: | 06:18:29 |
| Start date: | 14/01/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |

| | |
|---|---|
| Imagebase: | 0x7ff7f20f0000 |
| 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: dhcpmon.exe PID: 7112 Parent PID: 664

### General

| | |
|---|---|
| Start time: | 06:18:31 |
| Start date: | 14/01/2022 |
| Path: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 |
| Imagebase: | 0xd0000 |
| File size: | 1605632 bytes |
| MD5 hash: | 233064525984666FE973125F4E60C903 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000011.00000002.340545804.0000000002610000.00000004.00000001.sdmp, Author: Joe Security |
| Antivirus matches: | • Detection: 100%, Joe Sandbox ML<br>• Detection: 23%, ReversingLabs |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Written

#### File Read

## Analysis Process: PO#0065026.doc.exe PID: 7160 Parent PID: 6712

### General

| | |
|---|---|
| Start time: | 06:18:33 |
| Start date: | 14/01/2022 |
| Path: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\PO#0065026.doc.exe |
| Imagebase: | 0x6c0000 |
| File size: | 1605632 bytes |
| MD5 hash: | 233064525984666FE973125F4E60C903 |
| 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: 00000013.00000000.333627100.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.333627100.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000013.00000000.333627100.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.337826803.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.337826803.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000013.00000000.337826803.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.335589407.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.335589407.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000013.00000000.335589407.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.366690953.0000000002C41000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000013.00000002.366690953.0000000002C41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.336831952.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.336831952.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000013.00000000.336831952.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.363668804.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.363668804.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000013.00000002.363668804.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.366795171.0000000003C49000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000013.00000002.366795171.0000000003C49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Reputation: | low |

## File Activities

Show Windows behavior

### File Created

### File Read

## Analysis Process: dhcpmon.exe PID: 1312 Parent PID: 3352

### General

| | |
|---|---|
| Start time: | 06:18:37 |
| Start date: | 14/01/2022 |
| Path: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" |
| Imagebase: | 0xba0000 |
| File size: | 1605632 bytes |
| MD5 hash: | 233064525984666FE973125F4E60C903 |

| | |
|---|---|
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.373248632.00000000030B0000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.375404860.0000000004B90000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.375404860.0000000004B90000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000014.00000002.375404860.0000000004B90000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Read

## Analysis Process: dhcpmon.exe PID: 6616 Parent PID: 1312

### General

| | |
|---|---|
| Start time: | 06:18:47 |
| Start date: | 14/01/2022 |
| Path: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| Imagebase: | 0x210000 |
| File size: | 1605632 bytes |
| MD5 hash: | 233064525984666FE973125F4E60C903 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

## Analysis Process: dhcpmon.exe PID: 6592 Parent PID: 1312

### General

| | |
|---|---|
| Start time: | 06:18:48 |
| Start date: | 14/01/2022 |
| Path: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| Imagebase: | 0x530000 |
| File size: | 1605632 bytes |
| MD5 hash: | 233064525984666FE973125F4E60C903 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | .Net C# or VB.NET |

| | |
|---|---|
| Yara matches: | • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000000.366825626.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000000.366825626.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000016.00000000.366825626.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.391042000.0000000002B51000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000016.00000002.391042000.0000000002B51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.389921703.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.389921703.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000016.00000002.389921703.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000000.367777233.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000000.367777233.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000016.00000000.367777233.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000000.369712840.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000000.369712840.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000016.00000000.369712840.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000000.365733325.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000000.365733325.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000016.00000000.365733325.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.391135988.0000000003B59000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000016.00000002.391135988.0000000003B59000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Reputation: | low |

## Analysis Process: BackgroundTransferHost.exe PID: 6616 Parent PID: 744

### General

| | |
|---|---|
| Start time: | 06:19:27 |
| Start date: | 14/01/2022 |
| Path: | C:\Windows\System32\BackgroundTransferHost.exe |
| Wow64 process (32bit): | false |
| Commandline: | "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 |
| Imagebase: | 0x7ff62a980000 |
| File size: | 36864 bytes |
| MD5 hash: | 02BA81746B929ECC9DB6665589B68335 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

# Disassembly

## Code Analysis