


**ID:** 527347
**Sample Name:**
NGBCB21034772.exe
**Cookbook:** default.jbs
**Time:** 16:58:26
**Date:** 23/11/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

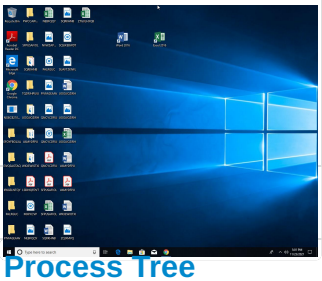
# Windows Analysis Report NGBCB21034772.exe

## Overview

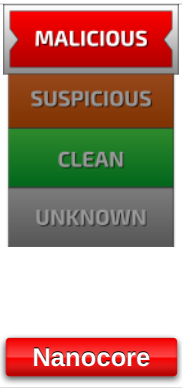
### General Information

| | |
|---|---|
| Sample Name: | NGBCB21034772.exe |
| Analysis ID: | 527347 |
| MD5: | b8c4a67ffad19ae.. |
| SHA1: | 06633fe82d0dd37. |
| SHA256: | dd50acbecbb2c7… |
| Tags: | exe |
| Infos: | |

Most interesting Screenshot:



### Detection

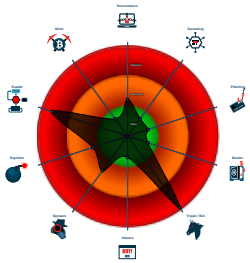



| | |
|---|---|
| Score: | 100 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Writes to foreign memory regions
- Connects to many ports of the same…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…

### Classification



## Process Tree

- **System is w10x64**
- NGBCB21034772.exe (PID: 6352 cmdline: "C:\Users\user\Desktop\NGBCB21034772.exe" MD5: B8C4A67FFAD19AE3C9F3C9770798E751)
  - schtasks.exe (PID: 2928 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\aZWHJb" /XML "C:\Users\user\AppData\Local\Temp\tmp2BE9.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6712 cmdline: {path} MD5: 71369277D09DA0830C8C59F9E22BB23A)
    - schtasks.exe (PID: 5840 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp45AF.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5780 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp5CC2.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 5564 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 5592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6912 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6956 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

## Malware Configuration

### Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "ce7fbdd9-3c95-435d-8876-f6695519",
  "Group": "0SPEED",
  "Domain1": "strongodss.ddns.net",
  "Domain2": "185.19.85.175",
  "Port": 50421,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8009,
  "BufferSize": "02000100",
  "MaxPacketSize": "",
  "GCThreshold": "",
  "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 |
|---|---|---|---|---|
| 00000004.00000000.691846174.000000000402000.00000040.00000001.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xff8d:$x1: NanoCore.ClientPluginHost<br>• 0xffca:$x2: IClientNetworkHost<br>• 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| 00000004.00000000.691846174.000000000402000.00000040.00000001.sdmp | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| 00000004.00000000.691846174.000000000402000.00000040.00000001.sdmp | NanoCore | unknown | Kevin Breen <kevin@techanarchy.net> | • 0xfcf5:$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 |
| 00000000.00000002.694978767.00000000028EF000.00000004.00000001.sdmp | JoeSecurity_AntiVM_3 | Yara detected AntiVM_3 | Joe Security | |
| 00000004.00000000.692150121.000000000402000.00000040.00000001.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xff8d:$x1: NanoCore.ClientPluginHost<br>• 0xffca:$x2: IClientNetworkHost<br>• 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| Click to see the 30 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 4.2.RegSvcs.exe.36216fc.2.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x40c2:$x1: NanoCore.ClientPluginHost |
| 4.2.RegSvcs.exe.36216fc.2.unpack | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0x40c2:$x2: NanoCore.ClientPluginHost<br>• 0x41a0:$s4: PipeCreated<br>• 0x40dc:$s5: IClientLoggingHost |
| 4.2.RegSvcs.exe.465ec9e.5.raw.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xe75:$x1: NanoCore.ClientPluginHost<br>• 0x6483:$x1: NanoCore.ClientPluginHost<br>• 0x1a020:$x1: NanoCore.ClientPluginHost<br>• 0x32fbf:$x1: NanoCore.ClientPluginHost<br>• 0xe8f:$x2: IClientNetworkHost<br>• 0x1a04d:$x2: IClientNetworkHost<br>• 0x32fec:$x2: IClientNetworkHost |
| 4.2.RegSvcs.exe.465ec9e.5.raw.unpack | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0xe75:$x2: NanoCore.ClientPluginHost<br>• 0x6483:$x2: NanoCore.ClientPluginHost<br>• 0x1a020:$x2: NanoCore.ClientPluginHost<br>• 0x32fbf:$x2: NanoCore.ClientPluginHost<br>• 0x1261:$s3: PipeExists<br>• 0x1136:$s4: PipeCreated<br>• 0x6561:$s4: PipeCreated<br>• 0x1b0fb:$s4: PipeCreated<br>• 0x3409a:$s4: PipeCreated<br>• 0xeb0:$s5: IClientLoggingHost<br>• 0x649d:$s5: IClientLoggingHost<br>• 0x1a03a:$s5: IClientLoggingHost<br>• 0x32fd9:$s5: IClientLoggingHost |
| 4.2.RegSvcs.exe.465ec9e.5.raw.unpack | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| Click to see the 67 entries | | | | |

# Sigma Overview

## AV Detection:

**Sigma detected: NanoCore**

## E-Banking Fraud:

**Sigma detected: NanoCore**

## System Summary:

**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**

## Networking:

Connects to many ports of the same IP (likely port scanning)

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

## E-Banking Fraud:

Yara detected Nanocore RAT

## System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

## Data Obfuscation:

.NET source code contains potential unpacker

## Boot Survival:

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

## Hooking and other Techniques for Hiding and Protection:

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

## Malware Analysis System Evasion:

Yara detected AntiVM3

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

## HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Injects a PE file into a foreign processes

## Stealing of Sensitive Information:

Yara detected Nanocore RAT

## Remote Access Functionality:

Detected Nanocore Rat

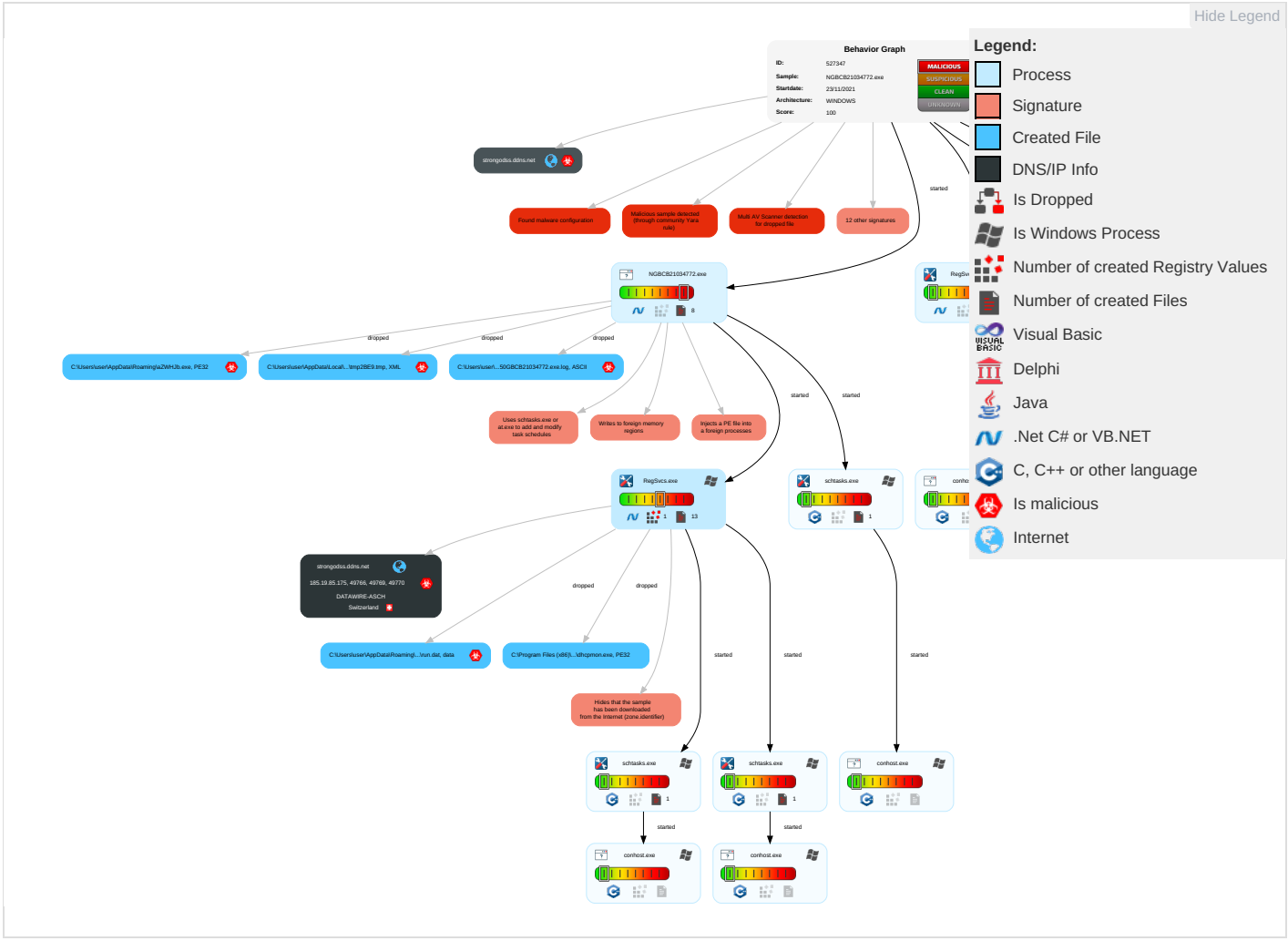
Yara detected Nanocore RAT

# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Comman and Cont |
|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Scheduled Task/Job 1 | Scheduled Task/Job 1 | Access Token Manipulation 1 | Masquerading 2 | Input Capture 2 1 | Security Software Discovery 2 1 | Remote Services | Input Capture 2 1 | Exfiltration Over Other Network Medium | Encrypted Channel |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Comman and Cont |
|---|---|---|---|---|---|---|---|---|---|---|
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Process Injection 2 1 2 | Disable or Modify Tools 1 | LSASS Memory | Process Discovery 1 | Remote Desktop Protocol | Archive Collected Data 1 1 | Exfiltration Over Bluetooth | Non-Stan Port 1 |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Scheduled Task/Job 1 | 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 A Software |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Access Token Manipulation 1 | NTDS | Application Window Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Non-Applicatio Layer Protocol |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Process Injection 2 1 2 | LSA Secrets | Remote System Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Applicatio Layer Protocol |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Deobfuscate/Decode Files or Information 1 | Cached Domain Credentials | File and Directory Discovery 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communi |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Hidden Files and Directories 1 | DCSync | System Information Discovery 1 3 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonl Used Port |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Obfuscated Files or Information 3 | Proc Filesystem | Network Service Scanning | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Applicatio Layer Pro |
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | Software Packing 1 3 | /etc/passwd and /etc/shadow | System Network Connections Discovery | Software Deployment Tools | Data Staged | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web Prot |
| Supply Chain Compromise | AppleScript | At (Windows) | At (Windows) | Timestomp 1 | Network Sniffing | Process Discovery | Taint Shared Content | Local Data Staging | Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | File Trans Protocols |

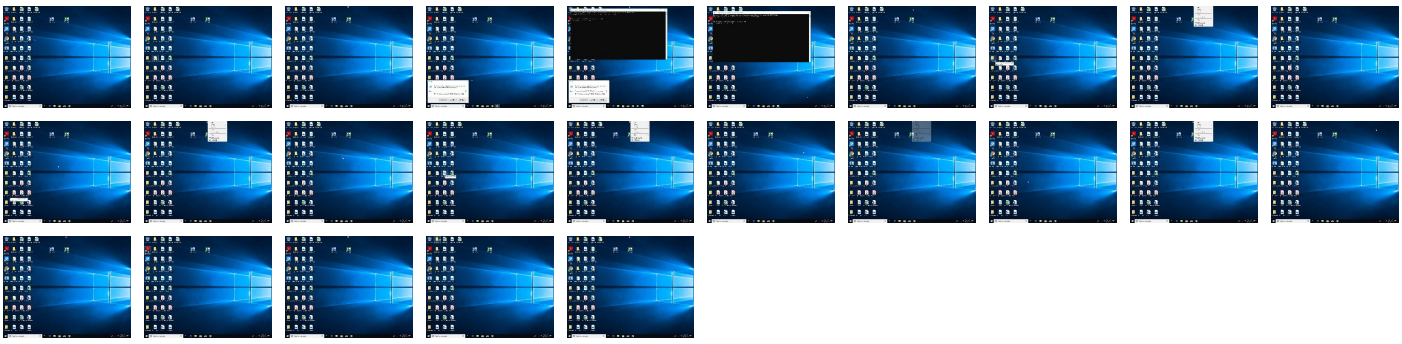
## Behavior Graph




## Screenshots

### Thumbnails

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




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| NGBCB21034772.exe | 54% | ReversingLabs | ByteCode-MSIL.Backdoor.NanoCore | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe | 0% | Metadefender | | Browse |
| C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Roaming\aZWHJb.exe | 40% | ReversingLabs | ByteCode-MSIL.Backdoor.NanoCore | |

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 4.0.RegSvcs.exe.400000.2.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 4.2.RegSvcs.exe.400000.0.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 4.0.RegSvcs.exe.400000.1.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 4.0.RegSvcs.exe.400000.4.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 4.2.RegSvcs.exe.61a0000.9.unpack | 100% | Avira | TR/NanoCore.fadte | | Download File |
| 4.0.RegSvcs.exe.400000.0.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 4.0.RegSvcs.exe.400000.3.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |

## Domains

No Antivirus matches

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.sandoll.co.krent | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/xi | 0% | Avira URL Cloud | safe | |
| http://www.goodfont.co.kry/ | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.comcin | 0% | Avira URL Cloud | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://www.carterandcone.comantAg | 0% | Avira URL Cloud | safe | |
| http://www.goodfont.co.kr | 0% | URL Reputation | safe | |
| http://www.carterandcone.com | 0% | URL Reputation | 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.carterandcone.comTlH | 0% | Avira URL Cloud | safe | |
| http://www.galapagosdesign.com/staff/dennis.htm | 0% | URL Reputation | safe | |
| http://fontfabrik.com | 0% | URL Reputation | safe | |
| http://www.carterandcone.comC | 0% | URL Reputation | safe | |
| http://www.galapagosdesign.com/DPlease | 0% | URL Reputation | safe | |
| http://www.sandoll.co.krati | 0% | Avira URL Cloud | safe | |
| http://www.sandoll.co.kr | 0% | URL Reputation | safe | |
| http://www.urwpp.deDPlease | 0% | URL Reputation | safe | |
| http://www.urwpp.de | 0% | URL Reputation | safe | |
| http://www.zhongyicts.com.cn | 0% | URL Reputation | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://www.fonts.comy | 0% | Avira URL Cloud | safe | |
| 185.19.85.175 | 0% | Avira URL Cloud | safe | |
| http://www.goodfont.co.kry/font | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.comech | 0% | Avira URL Cloud | safe | |
| http://www.tiro.comely_ | 0% | Avira URL Cloud | safe | |
| http://www.urwpp.dePx | 0% | Avira URL Cloud | safe | |
| http://www.galapagosdesign.com/lo | 0% | Avira URL Cloud | safe | |
| strongodss.ddns.net | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.coml | 0% | URL Reputation | safe | |
| http://www.galapagosdesign.com/boZ | 0% | Avira URL Cloud | safe | |
| http://www.sandoll.co.krimry | 0% | Avira URL Cloud | safe | |
| http://www.urwpp.deC | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cn | 0% | URL Reputation | safe | |
| http://www.monotype. | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/ | 0% | URL Reputation | safe | |
| http://www.urwpp.de&x | 0% | Avira URL Cloud | safe | |
| http://https://ocram-codes.net | 0% | Avira URL Cloud | safe | |
| http://www.fonts.com1 | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.comangKg | 0% | Avira URL Cloud | safe | |
| http://www.ascendercorp.com/typedesigners.htmld | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| strongodss.ddns.net | 185.19.85.175 | true | true | | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| 185.19.85.175 | true | • Avira URL Cloud: safe | unknown |

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| strongodss.ddns.net | true | • Avira URL Cloud: safe | unknown |

### URLs from Memory and Binaries

### Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 185.19.85.175 | strongodss.ddns.net | Switzerland | | 48971 | DATAWIRE-ASCH | true |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 527347 |
| Start date: | 23.11.2021 |
| Start time: | 16:58:26 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 10m 15s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | NGBCB21034772.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: | 25 |
| 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@18/13@10/1 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 12.8% (good quality ratio 9%)<br>• Quality average: 43.6%<br>• Quality standard deviation: 35.8% |
| HCA Information: | • Successful, ratio: 99%<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 |
|---|---|---|
| 16:59:29 | API Interceptor | 1x Sleep call for process: NGBCB21034772.exe modified |
| 16:59:38 | Autostart | Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| 16:59:43 | Task Scheduler | Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0) |

| Time | Type | Description |
|---|---|---|
| 16:59:45 | API Interceptor | 849x Sleep call for process: RegSvcs.exe modified |
| 16:59:46 | Task Scheduler | Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0) |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 185.19.85.175 | z.exe | Get hash | malicious | Browse | |
| | qaNcOX8rVf.exe | Get hash | malicious | Browse | |
| | Doc09768735093053.jpg.exe | Get hash | malicious | Browse | |
| | 36bc08479d28021f3931aee14512442e.scr.exe | Get hash | malicious | Browse | |
| | Ps3uhyF5Kw.exe | Get hash | malicious | Browse | |
| | mE5zWhfclN.exe | Get hash | malicious | Browse | |
| | XRKUHg8GO5.exe | Get hash | malicious | Browse | |
| | GOv2C9p0Jy.exe | Get hash | malicious | Browse | |
| | ameHrrFwNp.exe | Get hash | malicious | Browse | |
| | gNFfZ1w8E6.exe | Get hash | malicious | Browse | |
| | KRSEL0000056286.JPG.exe | Get hash | malicious | Browse | |
| | dAkJsQr7A9.exe | Get hash | malicious | Browse | |
| | dUzAkYsvl8.exe | Get hash | malicious | Browse | |
| | voo7b2BBq6.exe | Get hash | malicious | Browse | |
| | xmsGPH324z.exe | Get hash | malicious | Browse | |
| | dVWsghK4Aj.exe | Get hash | malicious | Browse | |
| | 2E9xpfvD2O.exe | Get hash | malicious | Browse | |
| | uF74GlbXPc.exe | Get hash | malicious | Browse | |
| | jFjTeUfek3.exe | Get hash | malicious | Browse | |
| | Q7DYDgQhKp.exe | Get hash | malicious | Browse | |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| strongodss.ddns.net | z.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | qaNcOX8rVf.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | Doc09768735093053.jpg.exe | Get hash | malicious | Browse | • 105.112.108.177 |
| | 36bc08479d28021f3931aee14512442e.scr.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | Ps3uhyF5Kw.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | mE5zWhfclN.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | XRKUHg8GO5.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | GOv2C9p0Jy.exe | Get hash | malicious | Browse | • 105.112.100.16 |
| | ameHrrFwNp.exe | Get hash | malicious | Browse | • 197.210.54.24 |
| | gNFfZ1w8E6.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | KRSEL0000056286.JPG.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | dAkJsQr7A9.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | dUzAkYsvl8.exe | Get hash | malicious | Browse | • 197.210.84.227 |
| | voo7b2BBq6.exe | Get hash | malicious | Browse | • 105.112.32.231 |
| | xmsGPH324z.exe | Get hash | malicious | Browse | • 105.112.32.231 |
| | dVWsghK4Aj.exe | Get hash | malicious | Browse | • 105.112.32.231 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| DATAWIRE-ASCH | TenderCopy16112021.exe | Get hash | malicious | Browse | • 185.19.85.166 |
| | uJHNawbgfZ.exe | Get hash | malicious | Browse | • 185.19.85.155 |
| | z.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | nlM5RNaNku.exe | Get hash | malicious | Browse | • 185.19.85.155 |
| | qaNcOX8rVf.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | Doc09768735093053.jpg.exe | Get hash | malicious | Browse | • 185.19.85.175 |
| | 36bc08479d28021f3931aee14512442e.scr.exe | Get hash | malicious | Browse | • 185.19.85.175 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | rAxnQsZKZt.exe | Get hash | malicious | Browse | • 185.19.85.152 |
| | TNT_Shipment_Advice2021011.exe | Get hash | malicious | Browse | • 185.19.85.166 |
| | XgKuBg8h23.exe | Get hash | malicious | Browse | • 185.19.85.155 |
| | o51ysudijF.exe | Get hash | malicious | Browse | • 185.19.85.155 |
| | Oqf4rUp3TA.exe | Get hash | malicious | Browse | • 185.19.85.155 |
| | Part Details.vbs | Get hash | malicious | Browse | • 185.19.85.171 |
| | Details.vbs | Get hash | malicious | Browse | • 185.19.85.171 |
| | Routing Details.vbs | Get hash | malicious | Browse | • 185.19.85.171 |
| | DHL_Shipment_notificationpdf.exe | Get hash | malicious | Browse | • 185.19.85.166 |
| | MkyxPXGeTq | Get hash | malicious | Browse | • 185.19.84.144 |
| | Order291021PDF.exe | Get hash | malicious | Browse | • 185.19.85.166 |
| | 1ZKA7xDrFG.exe | Get hash | malicious | Browse | • 185.19.85.155 |
| | K6uMMU9Ni5.exe | Get hash | malicious | Browse | • 185.19.85.155 |

## JA3 Fingerprints

**No context**

## Dropped Files

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe | z.exe | Get hash | malicious | Browse | |
| | 83Vbz4Ws7e.exe | Get hash | malicious | Browse | |
| | qF1xeOlWMA.exe | Get hash | malicious | Browse | |
| | 3EhG7plOed.exe | Get hash | malicious | Browse | |
| | GHhMZFFEmf.exe | Get hash | malicious | Browse | |
| | DRAFT BL-DOCS-20211510-VP-KMC022021.exe | Get hash | malicious | Browse | |
| | b2ZeLApyX2.exe | Get hash | malicious | Browse | |
| | YKr3m9a7C3.exe | Get hash | malicious | Browse | |
| | tEdxwnE4lw.exe | Get hash | malicious | Browse | |
| | 87R65JT93I.exe | Get hash | malicious | Browse | |
| | invo.exe | Get hash | malicious | Browse | |
| | U5s97oQj9A.exe | Get hash | malicious | Browse | |
| | hAmgDpjdg5.exe | Get hash | malicious | Browse | |
| | PO00174Quotations.exe | Get hash | malicious | Browse | |
| | mNgTZMYBA8.exe | Get hash | malicious | Browse | |
| | xvE67cxGKh.exe | Get hash | malicious | Browse | |
| | C9UKyFaVBg.exe | Get hash | malicious | Browse | |
| | lzopQnj0od.exe | Get hash | malicious | Browse | |
| | khmU580OCp.exe | Get hash | malicious | Browse | |
| | eKLFu9iX5X.exe | Get hash | malicious | Browse | |

# Created / dropped Files

**C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe**

| | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe |
| File Type: | PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 32768 |
| Entropy (8bit): | 3.7515815714465193 |
| Encrypted: | false |
| SSDEEP: | 384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u |
| MD5: | 71369277D09DA0830C8C59F9E22BB23A |
| SHA1: | 37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F |
| SHA-256: | D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698 |
| SHA-512: | 2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB7 |
| Malicious: | false |
| Antivirus: | • Antivirus: Metadefender, Detection: 0%, Browse<br>• Antivirus: ReversingLabs, Detection: 0% |

| C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe | |
|---|---|
| Joe Sandbox View: | • Filename: z.exe, Detection: malicious, Browse<br>• Filename: 83Vbz4Ws7e.exe, Detection: malicious, Browse<br>• Filename: qF1xeOlWMA.exe, Detection: malicious, Browse<br>• Filename: 3EhG7plOed.exe, Detection: malicious, Browse<br>• Filename: GHhMZFFEmf.exe, Detection: malicious, Browse<br>• Filename: DRAFT BL-DOCS-20211510-VP-KMC022021.exe, Detection: malicious, Browse<br>• Filename: b2ZeLApyX2.exe, Detection: malicious, Browse<br>• Filename: YKr3m9a7C3.exe, Detection: malicious, Browse<br>• Filename: tEdxwnE4lw.exe, Detection: malicious, Browse<br>• Filename: 87R65JT93I.exe, Detection: malicious, Browse<br>• Filename: invo.exe, Detection: malicious, Browse<br>• Filename: U5s97oQj9A.exe, Detection: malicious, Browse<br>• Filename: hAmgDpjdg5.exe, Detection: malicious, Browse<br>• Filename: PO00174Quotations.exe, Detection: malicious, Browse<br>• Filename: mNgTZMYBA8.exe, Detection: malicious, Browse<br>• Filename: xvE67cxGKh.exe, Detection: malicious, Browse<br>• Filename: C9UKyFaVBg.exe, Detection: malicious, Browse<br>• Filename: IzopQnj0od.exe, Detection: malicious, Browse<br>• Filename: khmU580OCp.exe, Detection: malicious, Browse<br>• Filename: eKLFu9iX5X.exe, Detection: malicious, Browse |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....P... .....k... .....@.. .....[.. ..@.....k..K..... k..... .....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... ..... ..... ..... |

| C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\NGBCB21034772.exe.log | |
|---|---|
| Process: | C:\Users\user\Desktop\NGBCB21034772.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 916 |
| Entropy (8bit): | 5.282390836641403 |
| Encrypted: | false |
| SSDEEP: | 24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+ |
| MD5: | 5AD8E7ABEADADAC4CE06FF693476581A |
| SHA1: | 81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E |
| SHA-256: | BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD |
| SHA-512: | 7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EE FF |
| Malicious: | **true** |
| Preview: | 1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a909923 7864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System .Xml.ni.dll",0.. |

| C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 120 |
| Entropy (8bit): | 5.016405576253028 |
| Encrypted: | false |
| SSDEEP: | 3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs |
| MD5: | 50DEC1858E13F033E6DCA3CBFAD5E8DE |
| SHA1: | 79AE1E9131B0FAF215B499D2F7B4C595AA120925 |
| SHA-256: | 14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4 |
| SHA-512: | 1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF |
| Malicious: | false |
| Preview: | 1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0.. |

| C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log | |
|---|---|
| Process: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 120 |
| Entropy (8bit): | 5.016405576253028 |
| Encrypted: | false |

| C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log | |
|---|---|
| SSDEEP: | 3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs |
| MD5: | 50DEC1858E13F033E6DCA3CBFAD5E8DE |
| SHA1: | 79AE1E9131B0FAF215B499D2F7B4C595AA120925 |
| SHA-256: | 14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4 |
| SHA-512: | 1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF |
| Malicious: | false |
| Preview: | 1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0.. |

| C:\Users\user\AppData\Local\Temp\tmp2BE9.tmp | |
|---|---|
| Process: | C:\Users\user\Desktop\NGBCB21034772.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1639 |
| Entropy (8bit): | 5.1815004977170664 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGdOtn:cbhK79lNQR/rydbz9l3YODOLNdq3+o |
| MD5: | 0753135815A870EE2CB87BAD2DB645BE |
| SHA1: | 523C2B870674551DAC3E2C7074FF76716106F6AF |
| SHA-256: | 962569F8F74909A7957902545C0D497E7EAA7FBFDCBCCEF6BC1081150530C6A6 |
| SHA-512: | E5AFFBAA859E32D343A24FF7CC433722816BF85594E7CA6CAA6F62CF092D237743988CE4A136D9B79CAA8F04F1AC3CEC6C831DE746745F69E8E483F41A192E1F |
| Malicious: | **true** |
| Preview: | <?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>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>true |

| C:\Users\user\AppData\Local\Temp\tmp45AF.tmp | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1320 |
| Entropy (8bit): | 5.135021273392143 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mn4xtn:cbk4oL600QydbQxIYODOLedq3Z4j |
| MD5: | 40B11EF601FB28F9B2E69D36857BF2EC |
| SHA1: | B6454020AD2CEED193F4792B77001D0BD741B370 |
| SHA-256: | C51E12D18CC664425F6711D8AE2507068884C7057092CFA11884100E1E9D49E1 |
| SHA-512: | E3C5BCC714CBFCA4B8058DDCDDF231DCEFA69C15881CE3F8123E59ED45CFB5DA052B56E1945DCF8DC7F800D62F9A4EECB82BCA69A66A1530787AEFFEB15E2BD5 |
| Malicious: | false |
| Preview: | <?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak |

| C:\Users\user\AppData\Local\Temp\tmp5CC2.tmp | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1310 |
| Entropy (8bit): | 5.109425792877704 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j |
| MD5: | 5C2F41CFC6F988C859DA7D727AC2B62A |
| SHA1: | 68999C85FC7E37BAB9216E0099836D40D4545C1C |
| SHA-256: | 98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B |
| SHA-512: | B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733 |
| Malicious: | false |

| C:\Users\user\AppData\Local\Temp\tmp5CC2.tmp | |
|---|---|
| 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\run.dat | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 8 |
| Entropy (8bit): | 3.0 |
| Encrypted: | false |
| SSDEEP: | 3:Iu8t:Iu8 |
| MD5: | F49BE19076602ED9C5DBD91A3CDC0058 |
| SHA1: | E410ED5FB26B57B3F2341F79ED8326E03DCB7A5B |
| SHA-256: | 896F2CD9B40213E6A20AD71ECF42242F1A23E86310259BD6D736B5A7B48A3CF8 |
| SHA-512: | C883CD4891FA6DB63204F3DAC2B164862D2766F651932BFEE6B72D23E24664AA19F4F961868DA64B810112F59DBF50FE404A8A1F4EAEF46413938DDFA337350E |
| Malicious: | **true** |
| Preview: | .&.?...H |

| C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 57 |
| Entropy (8bit): | 4.795707286467131 |
| Encrypted: | false |
| SSDEEP: | 3:oMty8WbSX/MNn:oMLWus |
| MD5: | D685103573539B7E9FDBF5F1D7DD96CE |
| SHA1: | 4B2FE6B5C0B37954B314FCAEE1F12237A9B02D07 |
| SHA-256: | D78BC23B0CA3EDDF52D56AB85CDC30A71B3756569CB32AA2F6C28DBC23C76E8E |
| SHA-512: | 17769A5944E8929323A34269ABEEF0861D5C6799B0A27F5545FBFADC80E5AB684A471AD6F6A7FC623002385154EA89DE94013051E09120AB94362E542AB0F1DD |
| Malicious: | false |
| Preview: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe |

| C:\Users\user\AppData\Roaming\aZWHJb.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\NGBCB21034772.exe |
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 516608 |
| Entropy (8bit): | 7.697368319306422 |
| Encrypted: | false |
| SSDEEP: | 12288:vcN79R2TvnX5u8HWEzB92DdPfCSO46n2DfHVEYT:kN79UTA8HWErw8662TT |
| MD5: | B8C4A67FFAD19AE3C9F3C9770798E751 |
| SHA1: | 06633FE82D0DD379D78A03A6014A0C49124BF126 |
| SHA-256: | DD50ACBECBB2C744DC18AF4769A1BC3196D59E8014E4F1AD87CF0214218AE129 |
| SHA-512: | 4B97FF911E8E7F299B71CD526E769293150127138DD99271BA950978BB14F8FF3ED18BDB15A19B2747CD22BC6A2C907554659A8E6FFA4A2885388252E1DEFB31 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: ReversingLabs, Detection: 40% |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...<.....P..... .....@.. .....@..... ..@.....K...O..... .....8..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....$..... 7.....0.....(....(.....(.....o ....*.....(!.....("....(#.....($.....(%....*N..(....o....(&....*&.. ('....*.s(.....s).....s*.....s+.....s,.....*....0.....~....o-....+..*.0.....~....o....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0..<.....~.....(2.....!r. ..p.....(3...o4...s5.....~.....+..*.0..... |

| \Device\ConDrv | |
|---|---|
| Process: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1145 |
| Entropy (8bit): | 4.462201512373672 |

| \Device\ConDrv | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC |
| MD5: | 46EBEB88876A00A52CC37B1F8E0D0438 |
| SHA1: | 5E5DB352F964E5F398301662FF558BD905798A65 |
| SHA-256: | D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B |
| SHA-512: | E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071BE |
| Malicious: | false |
| Preview: | Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:... /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo Suppress logo output... /quiet Suppress logo output and success output... |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 7.697368319306422 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.80%<br>• Win32 Executable (generic) a (10002005/4) 49.75%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Windows Screen Saver (13104/52) 0.07%<br>• Generic Win/DOS Executable (2004/3) 0.01% |
| File name: | NGBCB21034772.exe |
| File size: | 516608 |
| MD5: | b8c4a67ffad19ae3c9f3c9770798e751 |
| SHA1: | 06633fe82d0dd379d78a03a6014a0c49124bf126 |
| SHA256: | dd50acbecbb2c744dc18af4769a1bc3196d59e8014e4f1ad87cf0214218ae129 |
| SHA512: | 4b97ff911e8e7f299b71cd526e7692931501271380d99271ba950978bb14f8ff3ed18bdb15a19b2747cd22bc6a2c907554659a8e6ffa4a2885388252e1defb31 |
| SSDEEP: | 12288:vcN79R2TvnX5u8HWEzB92DdPfCSO46n2DfHVEYT:kN79UTA8HWErw8662TT |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...<.....P..... .....@.. .....@.....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 00828e8e8686b000 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x47ea9e |
| 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: | 0xC1B8B23C [Tue Dec 27 23:29:00 2072 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | v2.0.50727 |
| OS Version Major: | 4 |
| OS Version Minor: | 0 |

### General

| | |
|---|---|
| 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 | 0x7caa4 | 0x7cc00 | False | 0.868132749875 | data | 7.71013078572 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x80000 | 0x1114 | 0x1200 | False | 0.379774305556 | data | 4.91737888095 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x82000 | 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 |
|---|---|---|---|---|---|---|---|
| 11/23/21-16:59:47.041370 | UDP | 254 | DNS SPOOF query response with TTL of 1 min. and no authority | 53 | 49714 | 8.8.8.8 | 192.168.2.4 |
| 11/23/21-16:59:52.364874 | UDP | 254 | DNS SPOOF query response with TTL of 1 min. and no authority | 53 | 53097 | 8.8.8.8 | 192.168.2.4 |
| 11/23/21-17:01:03.643249 | UDP | 254 | DNS SPOOF query response with TTL of 1 min. and no authority | 53 | 63116 | 8.8.8.8 | 192.168.2.4 |
| 11/23/21-17:01:14.539138 | UDP | 254 | DNS SPOOF query response with TTL of 1 min. and no authority | 53 | 64801 | 8.8.8.8 | 192.168.2.4 |
| 11/23/21-17:01:36.075841 | UDP | 254 | DNS SPOOF query response with TTL of 1 min. and no authority | 53 | 61522 | 8.8.8.8 | 192.168.2.4 |

## Network Port Distribution

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Nov 23, 2021 16:59:47.021945000 CET | 192.168.2.4 | 8.8.8.8 | 0x8d54 | Standard query (0) | strongodss.ddns.net | A (IP address) | IN (0x0001) |
| Nov 23, 2021 16:59:52.343342066 CET | 192.168.2.4 | 8.8.8.8 | 0x95fa | Standard query (0) | strongodss.ddns.net | A (IP address) | IN (0x0001) |
| Nov 23, 2021 16:59:57.888725042 CET | 192.168.2.4 | 8.8.8.8 | 0xe329 | Standard query (0) | strongodss.ddns.net | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:00:31.400423050 CET | 192.168.2.4 | 8.8.8.8 | 0x34b | Standard query (0) | strongodss.ddns.net | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Nov 23, 2021 17:00:36.942168951 CET | 192.168.2.4 | 8.8.8.8 | 0x5f10 | Standard query (0) | strongodss .ddns.net | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:00:42.580620050 CET | 192.168.2.4 | 8.8.8.8 | 0x8e1c | Standard query (0) | strongodss .ddns.net | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:01:03.619900942 CET | 192.168.2.4 | 8.8.8.8 | 0x8b16 | Standard query (0) | strongodss .ddns.net | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:01:09.054589033 CET | 192.168.2.4 | 8.8.8.8 | 0xc88c | Standard query (0) | strongodss .ddns.net | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:01:14.517723083 CET | 192.168.2.4 | 8.8.8.8 | 0xf47f | Standard query (0) | strongodss .ddns.net | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:01:36.054240942 CET | 192.168.2.4 | 8.8.8.8 | 0xe1af | Standard query (0) | strongodss .ddns.net | A (IP address) | IN (0x0001) |

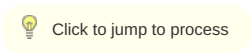
### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Nov 23, 2021 16:59:39.683557987 CET | 8.8.8.8 | 192.168.2.4 | 0x52b2 | No error (0) | a-0019.a.dns.azurefd.net | a-0019.standard.a-msedge.net | | CNAME (Canonical name) | IN (0x0001) |
| Nov 23, 2021 16:59:47.041369915 CET | 8.8.8.8 | 192.168.2.4 | 0x8d54 | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Nov 23, 2021 16:59:52.364873886 CET | 8.8.8.8 | 192.168.2.4 | 0x95fa | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Nov 23, 2021 16:59:57.908610106 CET | 8.8.8.8 | 192.168.2.4 | 0xe329 | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:00:31.419972897 CET | 8.8.8.8 | 192.168.2.4 | 0x34b | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:00:36.960076094 CET | 8.8.8.8 | 192.168.2.4 | 0x5f10 | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:00:42.600270987 CET | 8.8.8.8 | 192.168.2.4 | 0x8e1c | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:01:03.643249035 CET | 8.8.8.8 | 192.168.2.4 | 0x8b16 | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:01:09.074542046 CET | 8.8.8.8 | 192.168.2.4 | 0xc88c | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:01:14.539138079 CET | 8.8.8.8 | 192.168.2.4 | 0xf47f | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Nov 23, 2021 17:01:36.075840950 CET | 8.8.8.8 | 192.168.2.4 | 0xe1af | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |

## Code Manipulations

## Statistics

### Behavior




## System Behavior

### Analysis Process: NGBCB21034772.exe PID: 6352 Parent PID: 5172

### General

| | |
|---|---|
| Start time: | 16:59:23 |
| Start date: | 23/11/2021 |
| Path: | C:\Users\user\Desktop\NGBCB21034772.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\NGBCB21034772.exe" |
| Imagebase: | 0x230000 |
| File size: | 516608 bytes |
| MD5 hash: | B8C4A67FFAD19AE3C9F3C9770798E751 |
| 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: 00000000.00000002.694978767.00000000028EF000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.695908255.00000000038A1000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.695908255.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000000.00000002.695908255.00000000038A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

## Analysis Process: schtasks.exe PID: 2928 Parent PID: 6352

### General

| | |
|---|---|
| Start time: | 16:59:32 |
| Start date: | 23/11/2021 |
| Path: | C:\Windows\SysWOW64\schtasks.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\System32\schtasks.exe" /Create /TN "Updates\aZWHJb" /XML "C:\Users\user\AppData\Local\Temp\tmp2BE9.tmp |
| Imagebase: | 0xfb0000 |
| 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: 5140 Parent PID: 2928

### General

| | |
|---|---|
| Start time: | 16:59:33 |
| Start date: | 23/11/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff724c50000 |
| 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: RegSvcs.exe PID: 6712 Parent PID: 6352

### General

| | |
|---|---|
| Start time: | 16:59:34 |
| Start date: | 23/11/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe |
| Wow64 process (32bit): | true |
| Commandline: | {path} |
| Imagebase: | 0xed0000 |
| File size: | 32768 bytes |
| MD5 hash: | 71369277D09DA0830C8C59F9E22BB23A |
| 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: 00000004.00000000.691846174.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.691846174.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000000.691846174.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.692150121.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.692150121.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000000.692150121.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.692457604.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.692457604.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000000.692457604.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.933774763.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.933774763.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000002.933774763.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.935996896.0000000005A10000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.935996896.0000000005A10000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.936154958.0000000006190000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.936154958.0000000006190000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.936165853.00000000061A0000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.936165853.00000000061A0000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.936165853.00000000061A0000.00000004.00020000.sdmp, Author: Joe Security<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.692795570.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.692795570.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000000.692795570.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.935569052.0000000004657000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000002.935569052.0000000004657000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Reputation: | moderate |

## File Activities

Show Windows behavior

### File Created

### File Deleted

### File Written

### File Read

### Registry Activities

Show Windows behavior

#### Key Value Created

## Analysis Process: schtasks.exe PID: 5840 Parent PID: 6712

### General

| | |
|---|---|
| Start time: | 16:59:37 |
| Start date: | 23/11/2021 |
| 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\tmp45AF.tmp |
| Imagebase: | 0xfb0000 |
| 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: 6616 Parent PID: 5840

### General

| | |
|---|---|
| Start time: | 16:59:41 |
| Start date: | 23/11/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff724c50000 |
| 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: schtasks.exe PID: 5780 Parent PID: 6712

### General

| | |
|---|---|
| Start time: | 16:59:43 |
| Start date: | 23/11/2021 |
| 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\tmp5CC2.tmp |
| Imagebase: | 0xfb0000 |
| 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: RegSvcs.exe PID: 5564 Parent PID: 968

### General

| | |
|---|---|
| Start time: | 16:59:43 |
| Start date: | 23/11/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 |
| Imagebase: | 0x910000 |
| File size: | 32768 bytes |
| MD5 hash: | 71369277D09DA0830C8C59F9E22BB23A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | moderate |

**File Activities** Show Windows behavior

**File Created**

**File Written**

**File Read**

## Analysis Process: conhost.exe PID: 5592 Parent PID: 5564

### General

| | |
|---|---|
| Start time: | 16:59:44 |
| Start date: | 23/11/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff724c50000 |
| 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: conhost.exe PID: 5672 Parent PID: 5780

### General

| | |
|---|---|
| Start time: | 16:59:44 |
| Start date: | 23/11/2021 |
| Path: | C:\Windows\System32\conhost.exe |

| | |
|---|---|
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff724c50000 |
| 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: 6912 Parent PID: 968

### General

| | |
|---|---|
| Start time: | 16:59:46 |
| Start date: | 23/11/2021 |
| Path: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 |
| Imagebase: | 0xb00000 |
| File size: | 32768 bytes |
| MD5 hash: | 71369277D09DA0830C8C59F9E22BB23A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Antivirus matches: | • Detection: 0%, Metadefender, Browse<br>• Detection: 0%, ReversingLabs |

### File Activities

Show Windows behavior

#### File Created

#### File Written

#### File Read

## Analysis Process: conhost.exe PID: 6924 Parent PID: 6912

### General

| | |
|---|---|
| Start time: | 16:59:46 |
| Start date: | 23/11/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff724c50000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: dhcpmon.exe PID: 6956 Parent PID: 3424

### General

| | |
|---|---|
| Start time: | 16:59:46 |
| Start date: | 23/11/2021 |
| Path: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" |
| Imagebase: | 0xdc0000 |
| File size: | 32768 bytes |
| MD5 hash: | 71369277D09DA0830C8C59F9E22BB23A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |

### File Activities

Show Windows behavior

#### File Created

#### File Written

#### File Read

## Analysis Process: conhost.exe PID: 6764 Parent PID: 6956

### General

| | |
|---|---|
| Start time: | 16:59:47 |
| Start date: | 23/11/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff724c50000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

# Disassembly

## Code Analysis