
**ID:** 499571
**Sample Name:**
Eral_order_8499248_pdf.exe
**Cookbook:** default.jbs
**Time:** 16:11:08
**Date:** 08/10/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

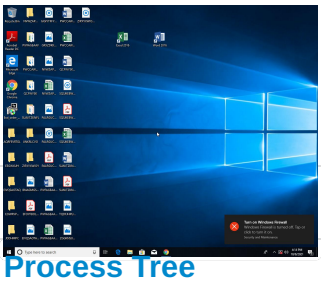
# Windows Analysis Report Eral_order_8499248_pdf.exe

## Overview

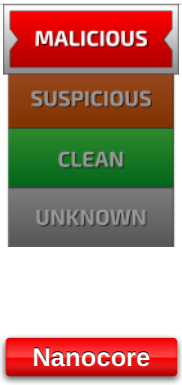
### General Information

| | |
|---|---|
| Sample Name: | Eral_order_8499248_pdf.exe |
| Analysis ID: | 499571 |
| MD5: | c87a4d4a3d7055.. |
| SHA1: | fcaea92aebebd7e. |
| SHA256: | 5925ea17cc4efd2.. |
| Tags: | exe |
| Infos: | |

Most interesting Screenshot:



### Detection

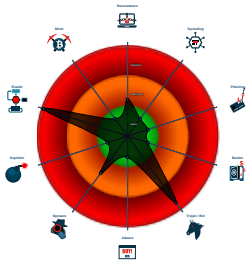



| | |
|---|---|
| Score: | 100 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Detected unpacking (overwrites its o…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Yara detected Nanocore RAT
- Detected unpacking (creates a PE fi…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- .NET source code contains potentia…

### Classification



## Process Tree

- **System is w10x64**
- Eral_order_8499248_pdf.exe (PID: 6636 cmdline: 'C:\Users\user\Desktop\Eral_order_8499248_pdf.exe' MD5: C87A4D4A3D7055D3FB628E9F5034200A)
  - Eral_order_8499248_pdf.exe (PID: 2932 cmdline: 'C:\Users\user\Desktop\Eral_order_8499248_pdf.exe' MD5: C87A4D4A3D7055D3FB628E9F5034200A)
    - schtasks.exe (PID: 4556 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8379.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Eral_order_8499248_pdf.exe (PID: 5284 cmdline: C:\Users\user\Desktop\Eral_order_8499248_pdf.exe 0 MD5: C87A4D4A3D7055D3FB628E9F5034200A)
  - Eral_order_8499248_pdf.exe (PID: 6592 cmdline: C:\Users\user\Desktop\Eral_order_8499248_pdf.exe 0 MD5: C87A4D4A3D7055D3FB628E9F5034200A)
- **cleanup**

## Malware Configuration

### Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "8eff5e85-5667-437d-b37d-ffe758cd",
  "Group": "NETH",
  "Domain1": "185.157.162.92",
  "Domain2": "",
  "Port": 2036,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000001.00000002.556639770.00000000038ED000.00000004.00000001.sdmp | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| 00000001.00000002.556639770.00000000038ED000.00000004.00000001.sdmp | NanoCore | unknown | Kevin Breen <kevin@techanarchy.net> | • 0x1068d:$a: NanoCore<br>• 0x106e6:$a: NanoCore<br>• 0x10723:$a: NanoCore<br>• 0x1079c:$a: NanoCore<br>• 0x23e47:$a: NanoCore<br>• 0x23e5c:$a: NanoCore<br>• 0x23e91:$a: NanoCore<br>• 0x3ce1b:$a: NanoCore<br>• 0x3ce30:$a: NanoCore<br>• 0x3ce65:$a: NanoCore<br>• 0x106ef:$b: ClientPlugin<br>• 0x1072c:$b: ClientPlugin<br>• 0x1102a:$b: ClientPlugin<br>• 0x11037:$b: ClientPlugin<br>• 0x23c03:$b: ClientPlugin<br>• 0x23c1e:$b: ClientPlugin<br>• 0x23c4e:$b: ClientPlugin<br>• 0x23e65:$b: ClientPlugin<br>• 0x23e9a:$b: ClientPlugin<br>• 0x3cbd7:$b: ClientPlugin<br>• 0x3cbf2:$b: ClientPlugin |
| 00000001.00000002.557530361.000000000522 0000.00000004.00020000.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xf7ad:$x1: NanoCore.ClientPluginHost<br>• 0xf7da:$x2: IClientNetworkHost |
| 00000001.00000002.557530361.000000000522 0000.00000004.00020000.sdmp | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0xf7ad:$x2: NanoCore.ClientPluginHost<br>• 0x10888:$s4: PipeCreated<br>• 0xf7c7:$s5: IClientLoggingHost |
| 00000001.00000002.557530361.000000000522 0000.00000004.00020000.sdmp | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| Click to see the 60 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 8.2.Eral_order_8499248_pdf.exe.415058.0.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xe38d:$x1: NanoCore.ClientPluginHost<br>• 0xe3ca:$x2: IClientNetworkHost<br>• 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| 8.2.Eral_order_8499248_pdf.exe.415058.0.unpack | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0xe105:$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 |
| 8.2.Eral_order_8499248_pdf.exe.415058.0.unpack | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| 8.2.Eral_order_8499248_pdf.exe.415058.0.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:$j: #=q |
| 7.2.Eral_order_8499248_pdf.exe.e801458.3.raw.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x1018d:$x1: NanoCore.ClientPluginHost<br>• 0x101ca:$x2: IClientNetworkHost<br>• 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| Click to see the 172 entries | | | | |

# Sigma Overview

## AV Detection:

**Sigma detected: NanoCore**

## E-Banking Fraud:

**Sigma detected: NanoCore**

## 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**

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

## Compliance:

Detected unpacking (overwrites its own PE header)

Detected unpacking (creates a PE file in dynamic memory)

## Networking:

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)

Detected unpacking (creates a PE file in dynamic memory)

.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)

## 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:

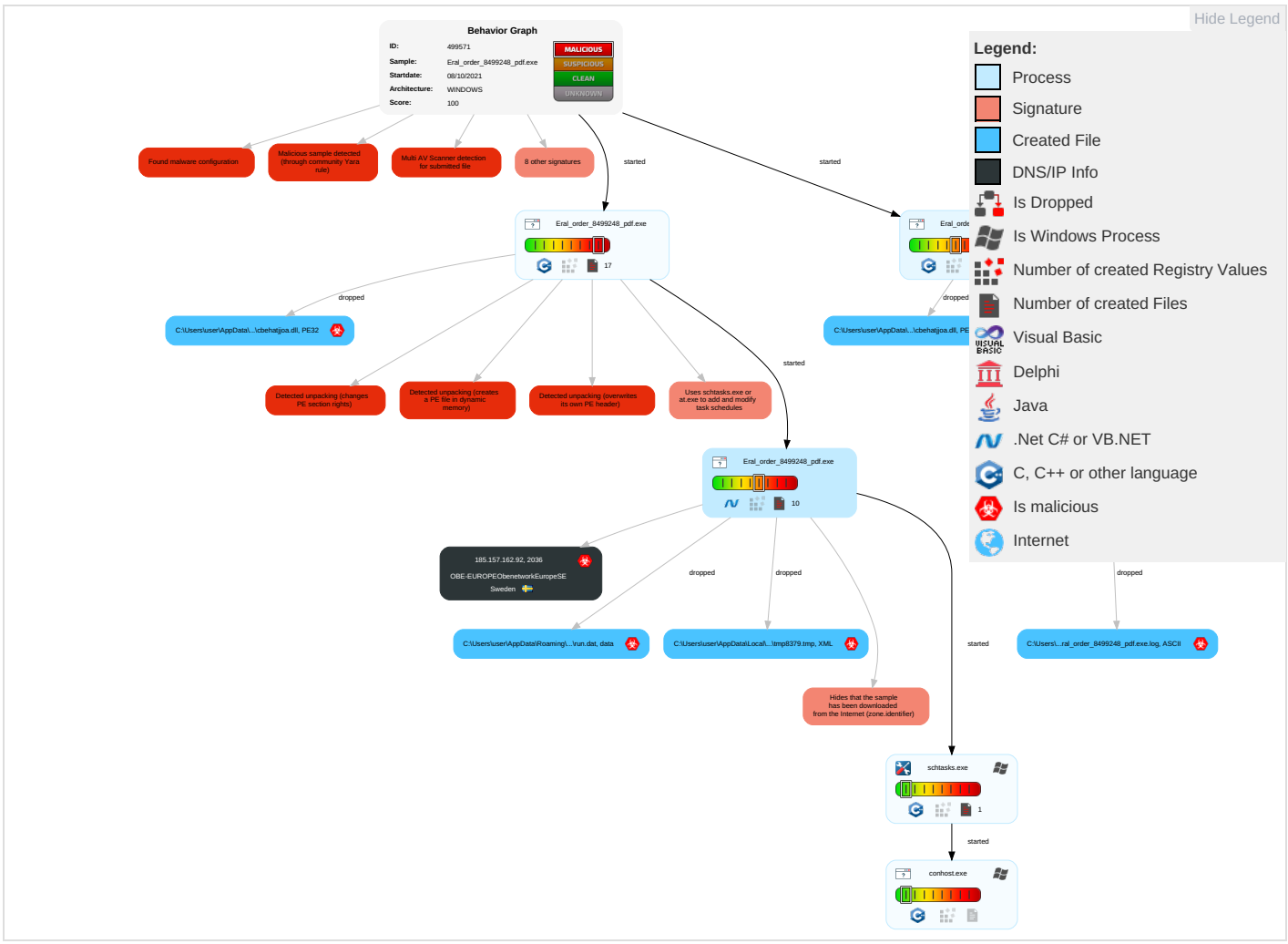
Detected Nanocore Rat

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 | Netwo Effect |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Scheduled Task/Job 1 | Scheduled Task/Job 1 | Access Token Manipulation 1 | Disable or Modify Tools 1 | Input Capture 2 1 | System Time Discovery 1 | Remote Services | Archive Collected Data 1 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eaves Insecu Netwo Comm |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Process Injection 1 1 2 | Deobfuscate/Decode Files or Information 1 1 | LSASS Memory | Account Discovery 1 | Remote Desktop Protocol | Input Capture 2 1 | Exfiltration Over Bluetooth | Non-Standard Port 1 | Exploi Redire Calls/S |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Scheduled Task/Job 1 | Obfuscated Files or Information 3 | Security Account Manager | File and Directory Discovery 2 | SMB/Windows Admin Shares | Clipboard Data 1 | Automated Exfiltration | Remote Access Software 1 | Exploi Track Locati |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Software Packing 4 2 | NTDS | System Information Discovery 1 6 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 1 | SIM C Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Masquerading 1 | LSA Secrets | Security Software Discovery 2 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manip Device Comm |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Virtualization/Sandbox Evasion 2 1 | Cached Domain Credentials | Process Discovery 2 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamm Denial Servic |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Access Token Manipulation 1 | DCSync | Virtualization/Sandbox Evasion 2 1 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Acces |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Process Injection 1 1 2 | Proc Filesystem | Application Window Discovery 1 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downg Insecu Protoc |
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | Hidden Files and Directories 1 | /etc/passwd and /etc/shadow | System Owner/User Discovery 1 | Software Deployment Tools | Data Staged | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web Protocols | Rogue Base S |

## 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 |
|---|---|---|---|---|
| Eral_order_8499248_pdf.exe | 39% | Virustotal | | Browse |
| Eral_order_8499248_pdf.exe | 100% | Joe Sandbox ML | | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\nsd3EE2.tmp\cbehatjjoa.dll | 100% | Joe Sandbox ML | | |
| C:\Users\user\AppData\Local\Temp\nsp5C2E.tmp\cbehatjjoa.dll | 100% | Joe Sandbox ML | | |

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 1.1.Eral_order_8499248_pdf.exe.400000.0.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 8.2.Eral_order_8499248_pdf.exe.4840000.8.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 1.0.Eral_order_8499248_pdf.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1130366 | | Download File |
| 7.2.Eral_order_8499248_pdf.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1130366 | | Download File |
| 7.0.Eral_order_8499248_pdf.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1130366 | | Download File |
| 0.2.Eral_order_8499248_pdf.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1130366 | | Download File |
| 1.2.Eral_order_8499248_pdf.exe.4980000.8.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 0.0.Eral_order_8499248_pdf.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1130366 | | Download File |
| 1.2.Eral_order_8499248_pdf.exe.400000.0.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 8.0.Eral_order_8499248_pdf.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1130366 | | Download File |
| 1.2.Eral_order_8499248_pdf.exe.5220000.10.unpack | 100% | Avira | TR/NanoCore.fadte | | Download File |
| 8.2.Eral_order_8499248_pdf.exe.400000.1.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 8.1.Eral_order_8499248_pdf.exe.400000.0.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |

### Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| windowsupdate.s.llnwi.net | 0% | Virustotal | | Browse |

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| | 0% | Avira URL Cloud | safe | |
| 185.157.162.92 | 0% | Avira URL Cloud | safe | |

## Domains and IPs

### Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| windowsupdate.s.llnwi.net | 178.79.242.128 | true | false | • 0%, Virustotal, Browse | unknown |

### Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| | true | • Avira URL Cloud: safe | low |
| 185.157.162.92 | true | • Avira URL Cloud: safe | unknown |

### URLs from Memory and Binaries

### Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 185.157.162.92 | unknown | Sweden | | 197595 | OBE-EUROPEObenetworkEuropeSE | true |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 499571 |
| Start date: | 08.10.2021 |
| Start time: | 16:11:08 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 9m 13s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | Eral_order_8499248_pdf.exe |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 24 |
| 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@9/8@0/1 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 62.9% (good quality ratio 57.2%)<br>• Quality average: 75.5%<br>• Quality standard deviation: 32.6% |
| HCA Information: | • Successful, ratio: 86%<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 |
|---|---|---|
| 16:12:11 | API Interceptor | 928x Sleep call for process: Eral_order_8499248_pdf.exe modified |
| 16:12:12 | Task Scheduler | Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Eral_order_8499248_pdf.exe" s>$(Arg0) |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 185.157.162.92 | Tartak Olczyk  Sp. z o.o,pdf.exe | Get hash | malicious | Browse | |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| windowsupdate.s.llnwi.net | zytMOhqzK6.exe | Get hash | malicious | Browse | • 178.79.242.0 |
| | 5e1UFhYpWX.dll | Get hash | malicious | Browse | • 178.79.242.0 |
| | PTFG87777.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | 77uCYFUqv1.dll | Get hash | malicious | Browse | • 178.79.242.0 |
| | taskhost.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | csEX0Bxw6x.dll | Get hash | malicious | Browse | • 178.79.242.128 |
| | GyIsTyzFmc.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | dec.exe | Get hash | malicious | Browse | • 178.79.242.0 |
| | SvmhQnz5E2.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | Quotation.jar | Get hash | malicious | Browse | • 178.79.242.0 |
| | SecuriteInfo.com.W32.AIDetect.malware1.32515.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | frF39bBsa7.exe | Get hash | malicious | Browse | • 178.79.242.0 |
| | in7BcpKNoa.exe | Get hash | malicious | Browse | • 178.79.242.0 |
| | DHL_1012617429350,pdf.exe | Get hash | malicious | Browse | • 178.79.242.0 |
| | Invoice Payment.exe | Get hash | malicious | Browse | • 178.79.242.128 |
| | l5z3Wydh6A.exe | Get hash | malicious | Browse | • 178.79.242.0 |
| | 9nMZE7FjpT.exe | Get hash | malicious | Browse | • 178.79.242.0 |
| | gelfor.dap.dll | Get hash | malicious | Browse | • 178.79.242.0 |
| | ZDEvCI1erK.exe | Get hash | malicious | Browse | • 178.79.242.0 |
| | SOA.exe | Get hash | malicious | Browse | • 178.79.242.128 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| OBE-EUROPEObenetworkEuropeSE | EA1h6jdjHF.exe | Get hash | malicious | Browse | • 185.157.160.136 |
| | Food Inquiry 08.10.2021.doc | Get hash | malicious | Browse | • 185.157.160.136 |
| | Inquiry 001382021.doc | Get hash | malicious | Browse | • 185.157.160.136 |
| | GqdDYUUQzo.exe | Get hash | malicious | Browse | • 185.157.160.136 |
| | Waybill.exe | Get hash | malicious | Browse | • 185.157.162.100 |
| | 5raeCVYesx.exe | Get hash | malicious | Browse | • 185.157.160.136 |
| | Inquiry 001742021.doc | Get hash | malicious | Browse | • 185.157.160.136 |
| | ITG9agvU89.exe | Get hash | malicious | Browse | • 185.157.160.136 |
| | Audio Inquiry 05.10.2021.doc | Get hash | malicious | Browse | • 185.157.160.136 |
| | Inquiry 001752021.doc | Get hash | malicious | Browse | • 185.157.160.136 |
| | PSW0g0KU50.exe | Get hash | malicious | Browse | • 185.157.160.136 |
| | Ht0uCtLD8c.exe | Get hash | malicious | Browse | • 185.157.160.136 |
| | qsFB742ldA.exe | Get hash | malicious | Browse | • 185.157.160.136 |
| | Audio Inquiry 04.10.2021.doc | Get hash | malicious | Browse | • 185.157.160.136 |
| | Document.exe | Get hash | malicious | Browse | • 193.187.91.102 |
| | Document.exe | Get hash | malicious | Browse | • 193.187.91.102 |
| | d9cA4Zayfl | Get hash | malicious | Browse | • 178.132.78.156 |
| | DHL-3009216769976535455627775648893.exe | Get hash | malicious | Browse | • 185.157.160.229 |
| | 51490_Video_Oynat#U0131c#U0131.apk | Get hash | malicious | Browse | • 178.132.78.156 |
| | 94270_Video_Oynat#U0131c#U0131.apk | Get hash | malicious | Browse | • 178.132.78.156 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

**C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Eral_order_8499248_pdf.exe.log**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 525 |
| Entropy (8bit): | 5.2874233355119316 |
| Encrypted: | false |
| SSDEEP: | 12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T |
| MD5: | 61CCF53571C9ABA6511D696CB0D32E45 |
| SHA1: | A13A42A20EC14942F52DB20FB16A0A520F8183CE |
| SHA-256: | 3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B |
| SHA-512: | 90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06 |
| Malicious: | **true** |
| Reputation: | high, very likely benign file |

| C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Eral_order_8499248_pdf.exe.log | |
|---|---|
| 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\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0.. |

| C:\Users\user\AppData\Local\Temp\ijcljyxfxut6da6vqh6 | |
|---|---|
| Process: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 279039 |
| Entropy (8bit): | 7.985907924049885 |
| Encrypted: | false |
| SSDEEP: | 6144:LDVzvv3fBrb0A5tP+a9qSy8TuNNFss0Qxa7HoMmhPr1lK+:13ft0AvGapMldbrzK+ |
| MD5: | 228C47B10B0283F9188ABFA3567302F1 |
| SHA1: | 33A187CA72A3B803EB7B7C9E004B19EE930484EE |
| SHA-256: | C1C8363884A0024C242BAA282190ED422B13999B5D859E2A2374B2245AABC0E9 |
| SHA-512: | DC933819CAB069CC8E9490926DCECBA2B4BAD196A7319735BE34D122B7E0837A6E525197ADF8B329AD65AB8CAA7F2420393DBBD4483732DFA2E1866ACAD9FA3 |
| Malicious: | false |
| Reputation: | low |
| Preview: | ...t...^.S.....:.Nl.%...[....Ot.#..9..Z.Y?....Q.....`.+.....52.....H.....q.....85M....$.1..a.HXQ.....\|:d...(...($...~...h.2...!...../VQg.-..v....6.&q.....5.g.Y.Kn.....Y....b..o..#.v&..gT.....\|....A[..OZ>.....%~..0t)..^19....<.t....%...[.....Z..?....J....t.`.)..^%..%..p.Oy..1..3..:?....Vw....<.....&..}-.A...w..r...l..@.....\|:.S.8.I..h_%t.U%}.Y...=.R...lF=I..*}.y....$....h....B..<...V.a....._..~<....w...H.A.D.6.....-+^.]#..iD...^..:.5I#:.w1.....%~.....^F.....<"Nl.....[....Ot.#.]9..)..... ...C.`....^...%..p..y.`1S..3.}C.`...Vw^...<.Y..M.&.\...Ac.....r.@.f#..`..R.F\|:.S.8.W.\~Mt.AX}....R...l.=I.#...../h.....<...V.a.....9..h<....w...~.A\D.6.....-+^.]#.XiD...^..:.5I#:.w1.....%~..0t)..^.S.....<.Nl.%...[....Ot.#..9..Z.Y?....Q.....`.+..^%..%..p..y.`1S..3..B?....Vw....<.....&..}..Ac.....r.@.l#.@.....\|:.S.8.I..\.Mt.U%}....R...lF=I..*}.y....$.....h.....<...V.a....._..~<....w...~.A\D.6.....-+^.]#.XiD |

| C:\Users\user\AppData\Local\Temp\nsd3EE2.tmp\cbehatjjoa.dll | |
|---|---|
| Process: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe |
| File Type: | PE32 executable (DLL) (console) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 19968 |
| Entropy (8bit): | 6.6547999590544675 |
| Encrypted: | false |
| SSDEEP: | 384:2pVyfmZ9m7mG3gn6RDanqy6NCXkWl+BKm+M1K/GVNKPygh:2pVyu2haqy6ogEaoGVEPy |
| MD5: | A2C9F39FB658E262EC11F2B71E51CCB4 |
| SHA1: | 6346BA3BEE37FD6EE00302D248D100D7AB83A3BF |
| SHA-256: | 014C3580F81D7FEC4940CFB878424686DFB892DCA045FD1AB424500DD228FBC9 |
| SHA-512: | 852DECCDC8041B6457EE24243255A1731134917D48BD18BA79B6C73905541AFD19C8D6F68DDBE8B7A23F364310A1A80763B095A71EBDDF6294EB37C4CA1BD51 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100% |
| Reputation: | low |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~...:h..:h..:h...w..8h...w..>h.....>h.....)h..:h...h...6..;h...6..;h...6..;h...6..;h..Rich:h.....PE..L...t)_a.....!.....$...&.....@.....X3.....`R..L....T.....@R.....P.....text...P".....$..... ..`.bss.....@.....rdata.....P.....(.....@..@.data.....`.....2.....@....rsrc.....L.....@..@..... |

| C:\Users\user\AppData\Local\Temp\nsp5C2E.tmp\cbehatjjoa.dll | |
|---|---|
| Process: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe |
| File Type: | PE32 executable (DLL) (console) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 19968 |
| Entropy (8bit): | 6.6547999590544675 |
| Encrypted: | false |
| SSDEEP: | 384:2pVyfmZ9m7mG3gn6RDanqy6NCXkWl+BKm+M1K/GVNKPygh:2pVyu2haqy6ogEaoGVEPy |
| MD5: | A2C9F39FB658E262EC11F2B71E51CCB4 |
| SHA1: | 6346BA3BEE37FD6EE00302D248D100D7AB83A3BF |
| SHA-256: | 014C3580F81D7FEC4940CFB878424686DFB892DCA045FD1AB424500DD228FBC9 |
| SHA-512: | 852DECCDC8041B6457EE24243255A1731134917D48BD18BA79B6C73905541AFD19C8D6F68DDBE8B7A23F364310A1A80763B095A71EBDDF6294EB37C4CA1BD51 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100% |
| Reputation: | low |

| C:\Users\user\AppData\Local\Temp\nsp5C2E.tmp\cbehatjjoa.dll | |
|---|---|
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~...:h..:h..:h...w..8h...w..>h.....>h.....)h..:h...h...6..;h...6..;h...6..;h...6..;h..Rich:h.....PE..L...t)_a.....!.....$...&.....@.....X3.....`R..L....T.....@R.....P.....text...P".....$..... ..`.bss.....@.....rdata.....P.....(.....@..@.data.....`.....2.....@....rsrc.....L.....@..@..... |

| C:\Users\user\AppData\Local\Temp\tmp8379.tmp | |
|---|---|
| Process: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1312 |
| Entropy (8bit): | 5.133420439692187 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Rxtn:cbk4oL600QydbQxIYODOLedq3Kj |
| MD5: | 28C6CCB4C5E8AACD15CE372D111A1306 |
| SHA1: | 062401C4CC0F0FA07DDFE4F725D53E903F86770A |
| SHA-256: | A04EAF8682A798F8A215362EBBC1ED41856E90126D407ECF168C4D954AEC0AE5 |
| SHA-512: | 7CC328FDBDAC8ACEB9B5EEA06EFC4E97F831D9BEA07AB1557E3EE1E6D71CDD3866188800A71BD57E2F3995CF421C819F69E0295519161EC7F4FB686B0EB9B1A |
| Malicious: | **true** |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <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:\Users\user\Desktop\Eral_order_8499248_pdf.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 8 |
| Entropy (8bit): | 3.0 |
| Encrypted: | false |
| SSDEEP: | 3:ilrUv8t:ilAv8t |
| MD5: | F382205FFA13FF7489C0BBD84EF8AE78 |
| SHA1: | 0A7DB89A589F1A192E82161F8F7CEBADB77B44A6 |
| SHA-256: | BF2307BEDD4BB977A9FD475D1B13E005191626D69E9E30CD34E10E9A9120CEB0 |
| SHA-512: | 1F2A8C598E703B702FA16A2430BEEE75637AF79B699309F07CADA0C093CFD93D7249F0DC8A0F00B9B0B858E0DE280732946A93635EB6EB7ABAD00A56DBAE091 |
| Malicious: | **true** |
| Preview: | .....H |

| C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat | |
|---|---|
| Process: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 49 |
| Entropy (8bit): | 4.441568140944514 |
| Encrypted: | false |
| SSDEEP: | 3:oNWXp5vgSXBy6d3Bd6Vr:oNWXpFgkHdu |
| MD5: | 323122791470119B97405F7A5233F247 |
| SHA1: | 8166BD5CEE0793CC3CA5A0753B98FD03D31DE100 |
| SHA-256: | 3F00D1F39CABC0B0D9F6AF7A702A7C390F7DA1DA1103C8CD7D510A1F53550876 |
| SHA-512: | 5974E471FCA140AF89FF5DB0DA82BE592A753D8051C26F8E6DD8CB886948B62E827BEB6D5BEF1835CDDB8F27251D697B0A849E05B92057174DCC51226F5FEF10 |
| Malicious: | false |
| Preview: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe |

## Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive |
| Entropy (8bit): | 7.9174208912716955 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.96%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | Eral_order_8499248_pdf.exe |
| File size: | 315909 |
| MD5: | c87a4d4a3d7055d3fb628e9f5034200a |
| SHA1: | fcaea92aebebd7ed940e1fab475a99d4bb08c45b |
| SHA256: | 5925ea17cc4efd2b4f52887a3d669aa83c52e3aa14df43c7f275d2d9d33ad5df |
| SHA512: | e7a6e595c137504d07c5aff68492f0432510afcd9e44ee1d241856ffe77b8dffbc8fd00849868b35576c9fcfdb111d3530b43ae5b64fe0cb9638699e8d2cd193 |
| SSDEEP: | 6144:F8LxBsS5zy6UrHrQP6HLqirYp601fyKmbiRbk/tba7HoMmtPr1lKHpl5ebz:/ScvrcCHCp1KKmORbcZfrzKHrz |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich.QF.....PE..L...m:.V.....`.....*1.....p....@ |

## File Icon

| | |
|---|---|
| Icon Hash: | b2a88c96b2ca6a72 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x40312a |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED |
| DLL Characteristics: | TERMINAL_SERVER_AWARE |
| Time Stamp: | 0x56FF3A6D [Sat Apr 2 03:20:13 2016 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| 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: | b76363e9cb88bf9390860da8e50999d2 |

### Entrypoint Preview

### Rich Headers

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x5e66 | 0x6000 | False | 0.670572916667 | data | 6.44065573436 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x7000 | 0x12a2 | 0x1400 | False | 0.4455078125 | data | 5.0583287871 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .data | 0x9000 | 0x25d18 | 0x600 | False | 0.458984375 | data | 4.18773476617 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .ndata | 0x2f000 | 0x8000 | 0x0 | False | 0 | empty | 0.0 | IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .rsrc | 0x37000 | 0x9e0 | 0xa00 | False | 0.45390625 | data | 4.4968702957 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Possible Origin

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| English | United States |  |

## Network Behavior

### Network Port Distribution

### TCP Packets

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Oct 8, 2021 16:12:48.368252039 CEST | 8.8.8.8 | 192.168.2.3 | 0xa8f4 | No error (0) | windowsupdate.s.llnwi.net | | 178.79.242.128 | A (IP address) | IN (0x0001) |
| Oct 8, 2021 16:12:48.368252039 CEST | 8.8.8.8 | 192.168.2.3 | 0xa8f4 | No error (0) | windowsupdate.s.llnwi.net | | 178.79.242.0 | A (IP address) | IN (0x0001) |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: Eral_order_8499248_pdf.exe PID: 6636 Parent PID: 5312

## General

| | |
|---|---|
| Start time: | 16:12:04 |
| Start date: | 08/10/2021 |
| Path: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\Eral_order_8499248_pdf.exe' |
| Imagebase: | 0x400000 |
| File size: | 315909 bytes |
| MD5 hash: | C87A4D4A3D7055D3FB628E9F5034200A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.302913256.000000000E7F0000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.302913256.000000000E7F0000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.302913256.000000000E7F0000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000000.00000002.302913256.000000000E7F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Reputation: | low |

## File Activities

Show Windows behavior

### File Created

### File Deleted

### File Written

### File Read

# Analysis Process: Eral_order_8499248_pdf.exe PID: 2932 Parent PID: 6636

## General

| | |
|---|---|
| Start time: | 16:12:05 |
| Start date: | 08/10/2021 |
| Path: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\Eral_order_8499248_pdf.exe' |
| Imagebase: | 0x400000 |
| File size: | 315909 bytes |
| MD5 hash: | C87A4D4A3D7055D3FB628E9F5034200A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.556639770.00000000038ED000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000001.00000002.556639770.00000000038ED000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.557530361.0000000005220000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.557530361.0000000005220000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.557530361.0000000005220000.00000004.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.556147476.0000000002881000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000001.300118720.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000001.300118720.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000001.300118720.0000000000400000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000001.00000001.300118720.0000000000400000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.553982010.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.553982010.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.553982010.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000001.00000002.553982010.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.557320658.0000000004D90000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.557320658.0000000004D90000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.555999309.00000000023C0000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.555999309.00000000023C0000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.555999309.00000000023C0000.00000004.00020000.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000001.00000002.555999309.00000000023C0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.556927651.0000000004982000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.556927651.0000000004982000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000001.00000002.556927651.0000000004982000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.554316233.000000000051A000.00000004.00000020.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.554316233.000000000051A000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000001.00000002.554316233.000000000051A000.00000004.00000020.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: 4556 Parent PID: 2932

### General

| | |
|---|---|
| Start time: | 16:12:11 |
| Start date: | 08/10/2021 |
| 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\tmp8379.tmp' |
| Imagebase: | 0xf0000 |
| 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: 4508 Parent PID: 4556

### General

| | |
|---|---|
| Start time: | 16:12:11 |
| Start date: | 08/10/2021 |
| 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: Eral_order_8499248_pdf.exe PID: 5284 Parent PID: 664

### General

| | |
|---|---|
| Start time: | 16:12:12 |
| Start date: | 08/10/2021 |
| Path: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe 0 |
| Imagebase: | 0x400000 |
| File size: | 315909 bytes |
| MD5 hash: | C87A4D4A3D7055D3FB628E9F5034200A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |

| | |
|---|---|
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.318858456.000000000E7F0000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.318858456.000000000E7F0000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.318858456.000000000E7F0000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000007.00000002.318858456.000000000E7F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

## Analysis Process: Eral_order_8499248_pdf.exe PID: 6592 Parent PID: 5284

### General

| | |
|---|---|
| Start time: | 16:12:13 |
| Start date: | 08/10/2021 |
| Path: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\Eral_order_8499248_pdf.exe 0 |
| Imagebase: | 0x400000 |
| File size: | 315909 bytes |
| MD5 hash: | C87A4D4A3D7055D3FB628E9F5034200A |
| 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: 00000008.00000001.317135947.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000001.317135947.0000000000414000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000008.00000001.317135947.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.335925171.0000000003661000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.335925171.0000000003661000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000008.00000002.335925171.0000000003661000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.335611612.00000000005C4000.00000004.00000020.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.335611612.00000000005C4000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000008.00000002.335611612.00000000005C4000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.336058089.0000000004800000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.336058089.0000000004800000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.336058089.0000000004800000.00000004.00020000.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000008.00000002.336058089.0000000004800000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.335435218.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.335435218.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.335435218.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000008.00000002.335435218.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.336095821.0000000004842000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.336095821.0000000004842000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000008.00000002.336095821.0000000004842000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: NanoCore, Description: unknown, Source: 00000008.00000002.335899814.000000000266E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Reputation: | low |

**File Activities** Show Windows behavior

**File Created**

**File Written**

**File Read**

# Disassembly

## Code Analysis