ID: 711362
Sample Name: Jens Frodesen CV.exe
Cookbook: default.jbs
Time: 04:10:25
Date: 28/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

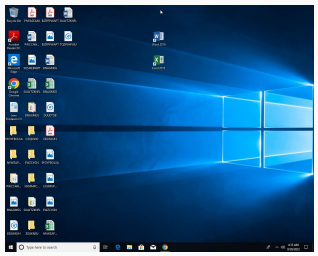
Windows Analysis Report

Jens Frodesen CV.exe

Overview

General Information

Sample Name:	Jens Frodesen CV.exe
Analysis ID:	711362
MD5:	89197e451346ed.
SHA1:	0e9d39ec84881c..
SHA256:	dbab1bf30e571b..
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

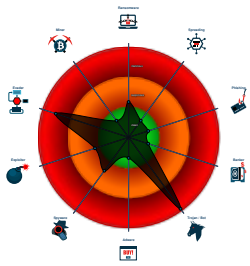
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Jens Frodesen CV.exe (PID: 2932 cmdline: "C:\Users\user\Desktop\Jens Frodesen CV.exe" MD5: 89197E451346ED5A3BA154F394948DE7)
  - schtasks.exe (PID: 5452 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\LrSEeB" /XML "C:\Users\user\AppData\Local\Temp\tmp476F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Jens Frodesen CV.exe (PID: 5344 cmdline: {path} MD5: 89197E451346ED5A3BA154F394948DE7)
    - schtasks.exe (PID: 4188 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp7194.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6072 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmp75AC.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Jens Frodesen CV.exe (PID: 244 cmdline: "C:\Users\user\Desktop\Jens Frodesen CV.exe" 0 MD5: 89197E451346ED5A3BA154F394948DE7)
  - schtasks.exe (PID: 5080 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\LrSEeB" /XML "C:\Users\user\AppData\Local\Temp\tmpBFFB.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5552 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Jens Frodesen CV.exe (PID: 1540 cmdline: {path} MD5: 89197E451346ED5A3BA154F394948DE7)
  - Jens Frodesen CV.exe (PID: 4720 cmdline: {path} MD5: 89197E451346ED5A3BA154F394948DE7)
- dhcpmon.exe (PID: 4320 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 89197E451346ED5A3BA154F394948DE7)
  - schtasks.exe (PID: 5564 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\LrSEeB" /XML "C:\Users\user\AppData\Local\Temp\tmpC1DF.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 3104 cmdline: {path} MD5: 89197E451346ED5A3BA154F394948DE7)
- dhcpmon.exe (PID: 988 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 89197E451346ED5A3BA154F394948DE7)
  - schtasks.exe (PID: 5524 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\LrSEeB" /XML "C:\Users\user\AppData\Local\Temp\tmpE91E.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5628 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 5788 cmdline: {path} MD5: 89197E451346ED5A3BA154F394948DE7)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "fba1bbc6-2cc8-4c94-b6c0-dda5a12f",
  "Group": "Default",
  "Domain1": "brightnano1.ddns.net",
  "Domain2": "",
  "Port": 1989,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.544223992.0000000005DD0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
00000003.00000002.544223992.0000000005DD0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost
00000003.00000002.544223992.0000000005DD0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x227f:$x2: NanoCore.ClientPlugin • 0x2205:$x3: NanoCore.ClientPluginHost • 0x2295:$i3: IClientNetwork • 0x221f:$i6: IClientLoggingHost • 0x223e:$i7: IClientNetworkHost • 0x1f9f:$s1: ClientPlugin • 0x2288:$s1: ClientPlugin
00000003.00000002.544223992.0000000005DD0000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x2205:$a1: NanoCore.ClientPluginHost • 0x227f:$a2: NanoCore.ClientPlugin • 0x29a0:$b7: LogClientException • 0x221f:$b9: IClientLoggingHost
00000003.00000002.548893461.00000000070B0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost

Click to see the 108 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.Jens Frodesen CV.exe.7080000.30.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x39eb:$x1: NanoCore.ClientPluginHost • 0x3a24:$x2: IClientNetworkHost
3.2.Jens Frodesen CV.exe.7080000.30.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x39eb:$x2: NanoCore.ClientPluginHost • 0x3b36:$s4: PipeCreated • 0x3a05:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
3.2.Jens Frodesen CV.exe.7080000.30.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x3a8b:$x2: NanoCore.ClientPlugin • 0x39eb:$x3: NanoCore.ClientPluginHost • 0x3aa1:$i3: IClientNetwork • 0x3a43:$i5: IClientDataHost • 0x3a05:$i6: IClientLoggingHost • 0x3a24:$i7: IClientNetworkHost • 0x426c:$i9: IClientNameObjectCollection • 0x3741:$s1: ClientPlugin • 0x3a94:$s1: ClientPlugin • 0x4680:$s2: EndPoint • 0x4371:$s3: IPAddress • 0x3c83:$s4: IPEndPoint • 0x43a3:$s7: get_Connected
3.2.Jens Frodesen CV.exe.7080000.30.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x39eb:$a1: NanoCore.ClientPluginHost • 0x3a8b:$a2: NanoCore.ClientPlugin • 0x47e1:$b7: LogClientException • 0x3a05:$b9: IClientLoggingHost
3.2.Jens Frodesen CV.exe.2c22150.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x15d53:$x1: NanoCore.ClientPluginHost • 0x1fbe7:$x1: NanoCore.ClientPluginHost • 0x27b51:$x1: NanoCore.ClientPluginHost • 0x2db68:$x1: NanoCore.ClientPluginHost • 0x37617:$x1: NanoCore.ClientPluginHost • 0x41a87:$x1: NanoCore.ClientPluginHost • 0x4caad:$x1: NanoCore.ClientPluginHost • 0x58897:$x1: NanoCore.ClientPluginHost • 0x64656:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost • 0x15d8c:$x2: IClientNetworkHost • 0x1fc20:$x2: IClientNetworkHost • 0x27b8a:$x2: IClientNetworkHost • 0x37774:$x2: IClientNetworkHost • 0x41ac0:$x2: IClientNetworkHost • 0x4cac7:$x2: IClientNetworkHost • 0x588b1:$x2: IClientNetworkHost • 0x64693:$x2: IClientNetworkHost
Click to see the 283 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.170 −

Timestamp:	192.168.2.7171.22.30.1704973019892816766 09/28/22-04:13:14.999476

SID:	2816766
Source Port:	49730
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.170

Timestamp:	192.168.2.7171.22.30.170497161989281676 6 09/28/22-04:12:02.248719
SID:	2816766
Source Port:	49716
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 171.22.30.170 - Destination IP: 192.168.2.7

Timestamp:	171.22.30.170192.168.2.71989497292841753 09/28/22-04:13:08.192973
SID:	2841753
Source Port:	1989
Destination Port:	49729
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 171.22.30.170 - Destination IP: 192.168.2.7

Timestamp:	171.22.30.170192.168.2.71989497142841753 09/28/22-04:11:48.761471
SID:	2841753
Source Port:	1989
Destination Port:	49714
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 171.22.30.170 - Destination IP: 192.168.2.7

Timestamp:	171.22.30.170192.168.2.71989497322841753 09/28/22-04:13:50.237286
SID:	2841753
Source Port:	1989
Destination Port:	49732
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.170

Timestamp:	192.168.2.7171.22.30.170497141989281676 6 09/28/22-04:11:48.872256
SID:	2816766
Source Port:	49714
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 171.22.30.170 - Destination IP: 192.168.2.7

Timestamp:	171.22.30.170192.168.2.71989497312841753 09/28/22-04:13:20.783532
SID:	2841753
Source Port:	1989
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.170

Timestamp:	192.168.2.7171.22.30.170497151989281676 6 09/28/22-04:11:55.135716
SID:	2816766
Source Port:	49715
Destination Port:	1989
Protocol:	TCP

Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

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)

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

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

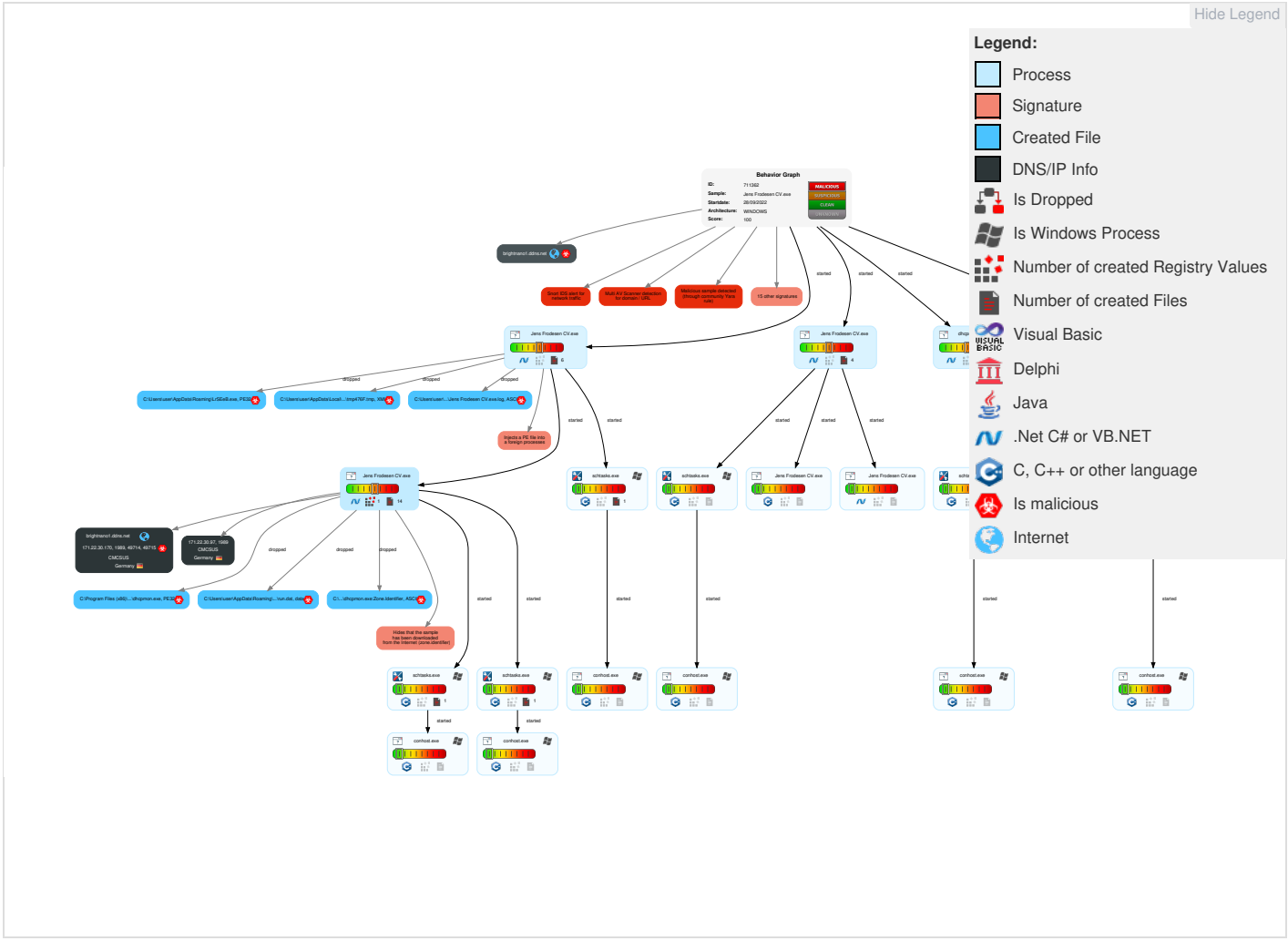
Detected Nanocore Rat

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 2 Process Injection	2 Masquerading	2 1 Input Capture	2 1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

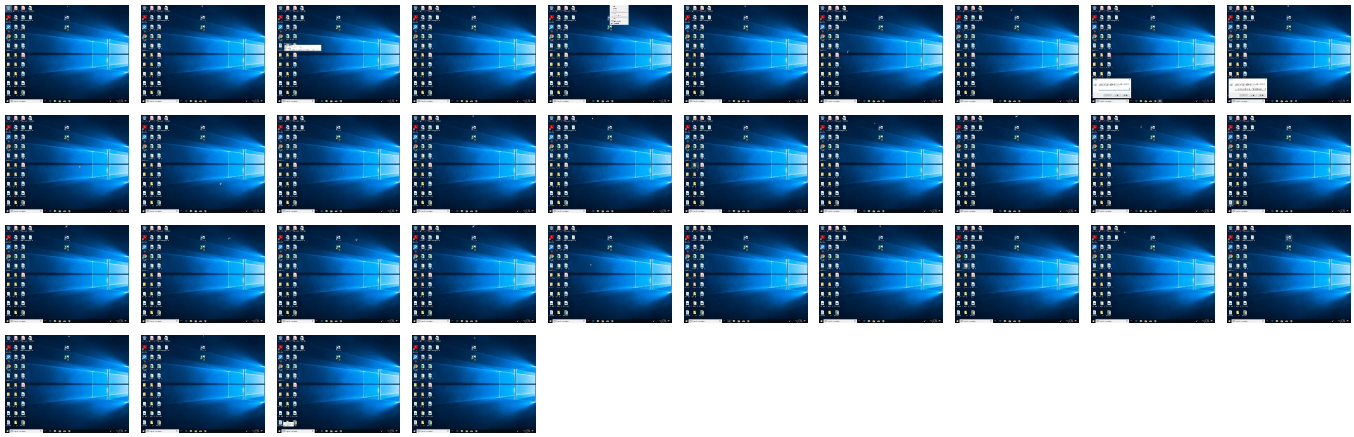
Behavior Graph



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
Jens Frodesen CV.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Jens Frodesen CV.exe	57%	Virustotal		Browse
Jens Frodesen CV.exe	33%	Metadefender		Browse
Jens Frodesen CV.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\LrSEeB.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	57%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	33%	Metadefender		Browse
C:\Users\user\AppData\Roaming\LrSEeB.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\LrSEeB.exe	33%	Metadefender		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.Jens Frodesen CV.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.Jens Frodesen CV.exe.6150000.26.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
brightnano1.ddns.net	14%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
brightnano1.ddns.net	14%	Virustotal		Browse
brightnano1.ddns.net	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
brightnano1.ddns.net	171.22.30.170	true	true	• 14%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
brightnano1.ddns.net	true	• 14%, Virustotal, Browse • Avira URL Cloud: malware	unknown

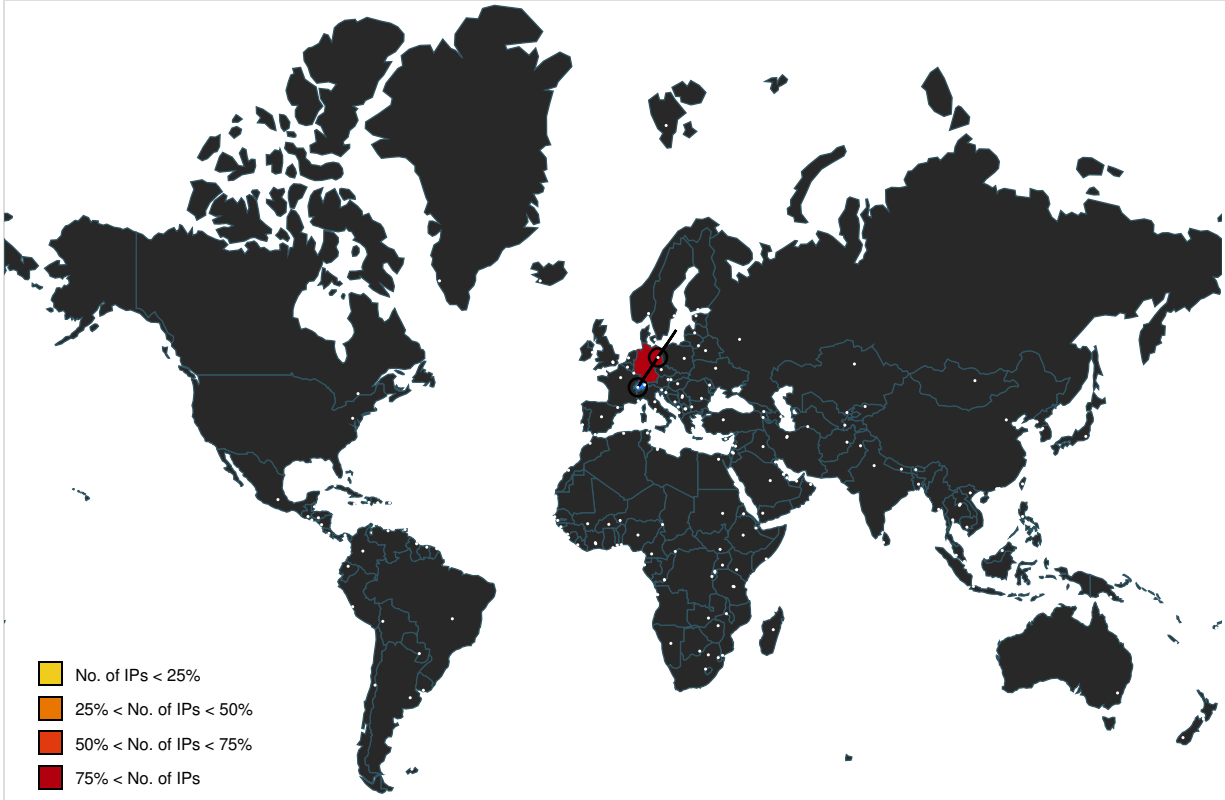
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	Jens Frodesen CV.exe, 00000003.00000002.518836400.0000000002B71000.00000004.00000800.00020000.00000000.sdmp, Jens Frodesen CV.exe, 00000003.00000002.536015397.000000003F25000.00000004.00000800.00020000.00000000.sdmp, Jens Frodesen CV.exe, 00000003.00000002.537384357.0000000004010000.00000004.00000800.00020000.00000000.sdmp, Jens Frodesen CV.exe, 00000003.00000002.531321593.0000000003CDF000.00000004.00000800.00020000.00000000.sdmp, Jens Frodesen CV.exe, 00000003.00000002.535141648.0000000003EAF000.00000004.00000800.00020000.00000000.sdmp, Jens Frodesen CV.exe, 00000003.00000002.548413055.0000000007070000.00000004.08000000.00040000.00000000.sdmp	false		high
http://www.carterandcone.coml	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp, Jens Frodesen CV.exe, 00000000.00000003.240997438.000000000123C000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Jens Frodesen CV.exe, 00000000.00000002.282970188.0000000002F2B000.00000004.00000800.00020000.00000000.sdmp, Jens Frodesen CV.exe, 00000003.00000002.518836400.000000002B71000.00000004.00000800.00020000.00000000.sdmp, Jens Frodesen CV.exe, 0000000C.00000002.370323682.000000003421000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 0000000E.00000002.364394906.000000003 10B000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000014.00000002.398299174.00000000032C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Jens Frodesen CV.exe, 00000000.00000002.297402479.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
171.22.30.97	unknown	Germany		33657	CMCSUS	false
171.22.30.170	brightnano1.ddns.net	Germany		33657	CMCSUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	711362
Start date and time:	2022-09-28 04:10:25 +02:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 11m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Jens Frodesen CV.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	42
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@32/15@7/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.190.159.5, 20.190.159.72, 20.190.159.74, 40.126.31.64, 20.190.159.70, 20.190.159.3, 40.126.31.68, 20.190.159.69, 20.82.210.154
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prda.aadg.msidentity.com, login.live.com, ctldl.windowsupdate.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, arc.msn.com, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:11:31	API Interceptor	813x Sleep call for process: Jens Frodesen CV.exe modified
04:11:42	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
04:11:44	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Jens Frodesen CV.exe" s>$(Arg0)
04:11:44	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
04:12:05	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Jens Frodesen CV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1053184
Entropy (8bit):	6.863226854581627
Encrypted:	false
SSDEEP:	12288:kgqC2JPYZVj5taS55PO88JplF4HwjADqjJ5ndW+/Pi7gvkdCOVy/0BA+l6lhliob:kg52p4J5tz688j4HojrlaE
MD5:	89197E451346ED5A3BA154F394948DE7
SHA1:	0E9D39EC84881CA095A9C1400D64EC586E983402
SHA-256:	DBAB1BF30E571BDDF1C21A19BEDEBFFD5A348145EA76ABDDC34A5172DF49AA3B
SHA-512:	F1C6BBDCB883E3DF94F497B5F7832A02AA455BEC92C680CD4DB0DDD9870E2AB3FBFB012C10B6E1983CDA81F3652C4878639E858D48E311394F8258D06D7E47B6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 60% • Antivirus: Virustotal, Detection: 57%, Browse • Antivirus: Metadefender, Detection: 33%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....<1c.....P..:.....X... ...`....@.. .....`..... ..@.....W..K....`.. .....@..... .....H.....text...48... ...:..... ..`.rsrc... ....`.....<.....@..@.rel oc.....@.....@..B.....X.....H.....`E.....+.....*..(&...*&..('....*.s(.....s).....s*.....s+.....s,.....*Z.....o?.....*&.. (@....*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*...{.....,+.....,rq..psB...z..|....(...+*...{.....,+.....,rq..psB...z..|....(...+*...{.....,+.....,rq..psB...z..|....(...+*...{.....,+.....,rq..psB...z..|....(...+*&.....*"".....*

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

Process:	C:\Users\user\Desktop\Jens Frodesen CV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Jens Frodesen CV.exe.log

Process:	C:\Users\user\Desktop\Jens Frodesen CV.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly \NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly \NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp476F.tmp

Process:	C:\Users\user\Desktop\Jens Frodesen CV.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1655
Entropy (8bit):	5.165507625778931
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBTtn:cbhH7MlNQ8/rydbz9l3YODOLNdq3f
MD5:	55D8D7A9509EE994B96E1EB880C39935
SHA1:	6A017D91DF07846CD90EB5CD160474E905DC06EC
SHA-256:	14A81BBC5132534A225A0B9EA5049B55F10CC24B8AB0B405ED21F3245B41A566
SHA-512:	29918549E4E46A74DFE8F9D99743A1FEA2A4EAD15943A8612AC530208075EE708DF9908E778494F8348C522BC4BBB9A2A3BC43B66B2D6D3A70031511F202679C
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>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmp7194.tmp

Process:	C:\Users\user\Desktop\Jens Frodesen CV.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	1310
Entropy (8bit):	5.096327253513791
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0a5xtn:cbk4oL600QydbQxIYODOLedq3Jj
MD5:	5CBFC2A6DBBF17C97F318924EF5050EA
SHA1:	BA8CBBA30078270B9F3FDA3D3D0FF559DBD1EB26
SHA-256:	A4834B80E5AF7B565790A6D7D6ADF22BE59655EE4912643C97CB5247348B8210
SHA-512:	098DCE276CA97CE47302002AABE396D6FA825F99DB1F4133D722AFA95E5C84A6343BAF818DCA11EC442170CFC7D904A31C57C857065445B77E6DCDAB0FFFF5F5
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\tmp75AC.tmp

Process:	C:\Users\user\Desktop\Jens Frodesen CV.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:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
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\tmpBFFB.tmp

Process:	C:\Users\user\Desktop\Jens Frodesen CV.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1655
Entropy (8bit):	5.165507625778931
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBTtn:cbhH7MlNQ8/rydbz9l3YODOLNdq3f
MD5:	55D8D7A9509EE994B96E1EB880C39935
SHA1:	6A017D91DF07846CD90EB5CD160474E905DC06EC
SHA-256:	14A81BBC5132534A225A0B9EA5049B55F10CC24B8AB0B405ED21F3245B41A566
SHA-512:	29918549E4E46A74DFE8F9D99743A1FEA2A4EAD15943A8612AC530208075EE708DF9908E778494F8348C522BC4BBB9A2A3BC43B66B2D6D3A70031511F202679C
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>.. <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>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmpC1DF.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1655

Entropy (8bit):	5.165507625778931
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBTtn:cbhH7MlNQ8/rydbz9l3YODOLNdq3f
MD5:	55D8D7A9509EE994B96E1EB880C39935
SHA1:	6A017D91DF07846CD90EB5CD160474E905DC06EC
SHA-256:	14A81BBC5132534A225A0B9EA5049B55F10CC24B8AB0B405ED21F3245B41A566
SHA-512:	29918549E4E46A74DFE8F9D99743A1FEA2A4EAD15943A8612AC530208075EE708DF9908E778494F8348C522BC4BBB9A2A3BC43B66B2D6D3A70031511F202679C
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>.. <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>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmpE91E.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1655
Entropy (8bit):	5.165507625778931
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBTtn:cbhH7MlNQ8/rydbz9l3YODOLNdq3f
MD5:	55D8D7A9509EE994B96E1EB880C39935
SHA1:	6A017D91DF07846CD90EB5CD160474E905DC06EC
SHA-256:	14A81BBC5132534A225A0B9EA5049B55F10CC24B8AB0B405ED21F3245B41A566
SHA-512:	29918549E4E46A74DFE8F9D99743A1FEA2A4EAD15943A8612AC530208075EE708DF9908E778494F8348C522BC4BBB9A2A3BC43B66B2D6D3A70031511F202679C
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>.. <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>.. <StartWhenAv

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

Process:	C:\Users\user\Desktop\Jens Frodesen CV.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35(A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

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

Process:	C:\Users\user\Desktop\Jens Frodesen CV.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Jdq:W
MD5:	957331451386AE435E3B86B0084CC12E
SHA1:	4612E788AAA86585B69B5FEA3592B3C62148BE7E

SHA-256:	B4CE45C0E6531694158D06FB628C97C2591C419C009772463F04BFF2C39CA7DB
SHA-512:	1418FD7FA9A1C8DBC593E690F0D8DC3F3E12956FCD97139EED7C69F46AB82715C548A13C2286CE84E8C1BCC46677CDBFC62AF9DE88E96267B1AC6216ED33670
Malicious:	**true**
Preview:	@..8B..H

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

Process:	C:\Users\user\Desktop\Jens Frodesen CV.exe
File Type:	data
Category:	modified
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E926
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV...,...0.... ....n.w6PMl.......v.'".v.......#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...I.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

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

Process:	C:\Users\user\Desktop\Jens Frodesen CV.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	47
Entropy (8bit):	4.027473159958119
Encrypted:	false
SSDEEP:	3:oN0naRRvuSKBsxiN:oNcSRy0iN
MD5:	73E6904F37156BBD5D7A3AE29190ABF2
SHA1:	DA061628C1D1BE6C8648A9F3A26ABAB6F273B8E6
SHA-256:	95727C1D0DD9664E84D3F23C5D499F4B050AFAE9045E3D362F8E47CBC2F3BECD
SHA-512:	1060C4516C7A0F336A53C3D60FACD4E0275885E42743CEEFC0849D55BD99278E1EC051E4033AF3A78675E42F52750932D4C6CE0EAA4B544CD055B8D7AB0615F4
Malicious:	false
Preview:	C:\Users\user\Desktop\Jens Frodesen CV.exe

C:\Users\user\AppData\Roaming\LrSEeB.exe

Process:	C:\Users\user\Desktop\Jens Frodesen CV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1053184
Entropy (8bit):	6.863226854581627
Encrypted:	false
SSDEEP:	12288:kgqC2JPYZVj5taS55PO88JplF4HwjADqjJ5ndW+/Pi7gvkdCOVy/0BA+l6lhliob:kg52p4J5tz688j4HojrlaE
MD5:	89197E451346ED5A3BA154F394948DE7
SHA1:	0E9D39EC84881CA095A9C1400D64EC586E983402
SHA-256:	DBAB1BF30E571BDDF1C21A19BEDEBFFD5A348145EA76ABDDC34A5172DF49AA3B
SHA-512:	F1C6BBDCB883E3DF94F497B5F7832A02AA455BEC92C680CD4DB0DDD9870E2AB3FBFB012C10B6E1983CDA81F3652C4878639E858D48E311394F8258D06D7E47B6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 60% • Antivirus: Metadefender, Detection: 33%, Browse

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....<1c.....P..:.....X... ...`....@.. .....`..... ..@.....W..K....`. .....@..... ..... .....H.....text...48... ...:..... ..`.rsrc... ....`.....<.....@..@.rel oc.....@.....@..B.....X.....H.....`E.....+.....*..(&...*&..('....*.s(.....s).....s*.....s+.....s,.....*Z.....o?.....*&.. (@....*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*...{.....,+.....,rq..psB...z..|....(...+*...{.....,+.....,rq..psB...z..|....(...+*...{.....,+.....,rq..psB ...z..|....(...+*...{.....,+.....,rq..psB...z..|....(...+*&.....*"".....*

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.863226854581627
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Jens Frodesen CV.exe
File size:	1053184
MD5:	89197e451346ed5a3ba154f394948de7
SHA1:	0e9d39ec84881ca095a9c1400d64ec586e983402
SHA256:	dbab1bf30e571bddf1c21a19bedebffd5a348145ea76abddc34a5172df49aa3b
SHA512:	f1c6bbdcb883e3df94f497b5f7832a02aa455bec92c680cd4db0ddd9870e2ab3fbfb012c10b6e1983cda81f3652c4878639e858d48e311394f8258d06d7e47b6
SSDEEP:	12288:kgqC2JPYZVj5taS55PO88JpIF4HwjADqjJ5ndW+/Pi7gvkdCOVy/0BA+l6lhliob:kg52p4J5tz688j4HojrlaE
TLSH:	F125195831E6329EF46BC6B58FD87CF59A56F632431F5177607302898B2ED82CE90872
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....<1c.....P..:.....X... ...`....@.. .....`.....@.....

File Icon

Icon Hash:	64f4d4dcdcdce4ec

Static PE Info

General

Entrypoint:	0x4f582e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63313CDF [Mon Sep 26 05:47:11 2022 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf57e0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf6000	0xd320	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x104000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xf3834	0xf3a00	False	0.6070470834402257	data	6.901351263212902	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xf6000	0xd320	0xd400	False	0.24318248820754718	data	4.756478683576001	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x104000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xf6280	0x176d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xf79f0	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 0		
RT_ICON	0xfbc18	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0xfe1c0	0x1a68	Device independent bitmap graphic, 40 x 80 x 32, image size 0		
RT_ICON	0xffc28	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x100cd0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x101658	0x6b8	Device independent bitmap graphic, 20 x 40 x 32, image size 0		
RT_ICON	0x101d10	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_GROUP_ICON	0x102178	0x76	data		
RT_VERSION	0x1021f0	0x314	data		
RT_MANIFEST	0x102504	0xe15	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

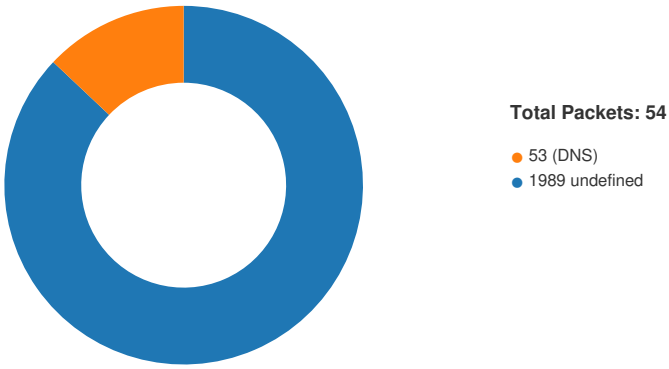
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.7171.22.30.1704973019892816766 09/28/22-04:13:14.999476	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49730	1989	192.168.2.7	171.22.30.170
192.168.2.7171.22.30.1704971619892816766 09/28/22-04:12:02.248719	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	1989	192.168.2.7	171.22.30.170
171.22.30.170192.168.2.71989497292841753 09/28/22-04:13:08.192973	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1989	49729	171.22.30.170	192.168.2.7
171.22.30.170192.168.2.71989497142841753 09/28/22-04:11:48.761471	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1989	49714	171.22.30.170	192.168.2.7
171.22.30.170192.168.2.71989497322841753 09/28/22-04:13:50.237286	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1989	49732	171.22.30.170	192.168.2.7
192.168.2.7171.22.30.1704971419892816766 09/28/22-04:11:48.872256	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49714	1989	192.168.2.7	171.22.30.170

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
171.22.30.170192.168.2.7 1989497312841753 09/28/22-04:13:20.783532	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1989	49731	171.22.30.170	192.168.2.7
192.168.2.7171.22.30.170 4971519892816766 09/28/22-04:11:55.135716	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49715	1989	192.168.2.7	171.22.30.170

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 28, 2022 04:11:47.216166973 CEST	49714	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:11:47.244659901 CEST	1989	49714	171.22.30.170	192.168.2.7
Sep 28, 2022 04:11:47.244803905 CEST	49714	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:11:47.480103970 CEST	49714	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:11:47.561458111 CEST	1989	49714	171.22.30.170	192.168.2.7
Sep 28, 2022 04:11:47.841763973 CEST	49714	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:11:48.081073046 CEST	1989	49714	171.22.30.170	192.168.2.7
Sep 28, 2022 04:11:48.761471033 CEST	1989	49714	171.22.30.170	192.168.2.7
Sep 28, 2022 04:11:48.872256041 CEST	49714	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:11:48.970669985 CEST	1989	49714	171.22.30.170	192.168.2.7
Sep 28, 2022 04:11:49.853272915 CEST	49714	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:11:54.296312094 CEST	49715	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:11:54.323734999 CEST	1989	49715	171.22.30.170	192.168.2.7
Sep 28, 2022 04:11:54.323832989 CEST	49715	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:11:54.324443102 CEST	49715	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:11:54.454488039 CEST	1989	49715	171.22.30.170	192.168.2.7
Sep 28, 2022 04:11:55.135715961 CEST	49715	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:11:55.257941961 CEST	1989	49715	171.22.30.170	192.168.2.7
Sep 28, 2022 04:11:56.283302069 CEST	49715	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:12:00.608197927 CEST	49716	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:12:00.635656118 CEST	1989	49716	171.22.30.170	192.168.2.7
Sep 28, 2022 04:12:00.635793924 CEST	49716	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:12:00.636326075 CEST	49716	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:12:00.711595058 CEST	1989	49716	171.22.30.170	192.168.2.7
Sep 28, 2022 04:12:01.263540983 CEST	49716	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:12:01.411520004 CEST	1989	49716	171.22.30.170	192.168.2.7
Sep 28, 2022 04:12:02.248718977 CEST	49716	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:12:02.411017895 CEST	1989	49716	171.22.30.170	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 28, 2022 04:12:03.264863014 CEST	49716	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:12:07.453716993 CEST	49718	1989	192.168.2.7	171.22.30.97
Sep 28, 2022 04:12:10.477433920 CEST	49718	1989	192.168.2.7	171.22.30.97
Sep 28, 2022 04:12:16.587308884 CEST	49718	1989	192.168.2.7	171.22.30.97
Sep 28, 2022 04:12:28.212622881 CEST	49719	1989	192.168.2.7	171.22.30.97
Sep 28, 2022 04:12:31.197839975 CEST	49719	1989	192.168.2.7	171.22.30.97
Sep 28, 2022 04:12:37.198277950 CEST	49719	1989	192.168.2.7	171.22.30.97
Sep 28, 2022 04:12:49.280534029 CEST	49728	1989	192.168.2.7	171.22.30.97
Sep 28, 2022 04:12:52.387058973 CEST	49728	1989	192.168.2.7	171.22.30.97
Sep 28, 2022 04:12:58.387623072 CEST	49728	1989	192.168.2.7	171.22.30.97
Sep 28, 2022 04:13:08.045222998 CEST	49729	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:08.072586060 CEST	1989	49729	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:08.072699070 CEST	49729	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:08.073422909 CEST	49729	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:08.192972898 CEST	1989	49729	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:08.341450930 CEST	49729	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:08.724486113 CEST	1989	49729	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:08.736243010 CEST	49729	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:08.776987076 CEST	1989	49729	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:08.931526899 CEST	49729	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:08.998291969 CEST	49729	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:13.241271019 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:13.268585920 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:13.268773079 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:13.269579887 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:13.442826033 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:13.998595953 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:14.138187885 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:14.545727015 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:14.546179056 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:14.573961973 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:14.599947929 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:14.739052057 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:14.999475956 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:15.136562109 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.207856894 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.207937956 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.207983971 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.208033085 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.208065033 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:15.208122969 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:15.235377073 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.235421896 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.235445976 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.235471964 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.235495090 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.235518932 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.235543966 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.235569954 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.235621929 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:15.235687971 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:15.263062000 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263102055 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263119936 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263139009 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263158083 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263175964 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263194084 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263212919 CEST	1989	49730	171.22.30.170	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 28, 2022 04:13:15.263231039 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263248920 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263267040 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263283968 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263290882 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:15.263300896 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263319016 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263336897 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.263401985 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:15.263453960 CEST	49730	1989	192.168.2.7	171.22.30.170
Sep 28, 2022 04:13:15.290501118 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.290541887 CEST	1989	49730	171.22.30.170	192.168.2.7
Sep 28, 2022 04:13:15.290563107 CEST	1989	49730	171.22.30.170	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 28, 2022 04:11:47.158247948 CEST	60326	53	192.168.2.7	8.8.8.8
Sep 28, 2022 04:11:47.179531097 CEST	53	60326	8.8.8.8	192.168.2.7
Sep 28, 2022 04:11:54.248167992 CEST	50835	53	192.168.2.7	8.8.8.8
Sep 28, 2022 04:11:54.269999981 CEST	53	50835	8.8.8.8	192.168.2.7
Sep 28, 2022 04:12:00.577048063 CEST	50505	53	192.168.2.7	8.8.8.8
Sep 28, 2022 04:12:00.594331980 CEST	53	50505	8.8.8.8	192.168.2.7
Sep 28, 2022 04:13:08.023263931 CEST	62679	53	192.168.2.7	8.8.8.8
Sep 28, 2022 04:13:08.043982029 CEST	53	62679	8.8.8.8	192.168.2.7
Sep 28, 2022 04:13:13.217652082 CEST	61392	53	192.168.2.7	8.8.8.8
Sep 28, 2022 04:13:13.238759041 CEST	53	61392	8.8.8.8	192.168.2.7
Sep 28, 2022 04:13:20.614382982 CEST	52104	53	192.168.2.7	8.8.8.8
Sep 28, 2022 04:13:20.634161949 CEST	53	52104	8.8.8.8	192.168.2.7
Sep 28, 2022 04:13:25.937551975 CEST	65356	53	192.168.2.7	8.8.8.8
Sep 28, 2022 04:13:25.958398104 CEST	53	65356	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 28, 2022 04:11:47.158247948 CEST	192.168.2.7	8.8.8.8	0x5858	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 04:11:54.248167992 CEST	192.168.2.7	8.8.8.8	0xa4be	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 04:12:00.577048063 CEST	192.168.2.7	8.8.8.8	0xb457	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 04:13:08.023263931 CEST	192.168.2.7	8.8.8.8	0x1871	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 04:13:13.217652082 CEST	192.168.2.7	8.8.8.8	0xf480	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 04:13:20.614382982 CEST	192.168.2.7	8.8.8.8	0x35d3	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 04:13:25.937551975 CEST	192.168.2.7	8.8.8.8	0xdcfb	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false

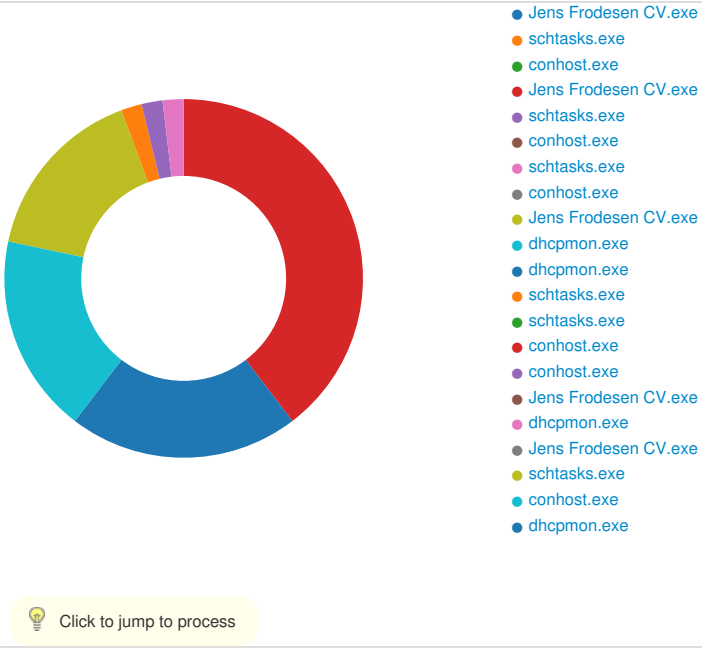
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 28, 2022 04:11:47.179531097 CEST	8.8.8.8	192.168.2.7	0x5858	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 04:11:54.269999981 CEST	8.8.8.8	192.168.2.7	0xa4be	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 04:12:00.594331980 CEST	8.8.8.8	192.168.2.7	0xb457	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 28, 2022 04:13:08.043982029 CEST	8.8.8.8	192.168.2.7	0x1871	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 04:13:13.238759041 CEST	8.8.8.8	192.168.2.7	0xf480	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 04:13:20.634161949 CEST	8.8.8.8	192.168.2.7	0x35d3	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 04:13:25.958398104 CEST	8.8.8.8	192.168.2.7	0xdcfb	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Jens Frodesen CV.exe PID: **2932**, Parent PID: **5128**

General

Target ID:	0
Start time:	04:11:17
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\Jens Frodesen CV.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Jens Frodesen CV.exe"
Imagebase:	0x930000
File size:	1053184 bytes
MD5 hash:	89197E451346ED5A3BA154F394948DE7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.286466691.0000000003EF9000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.286466691.0000000003EF9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.286466691.0000000003EF9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.286466691.0000000003EF9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.290258767.00000000041C1000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.290258767.00000000041C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.290258767.00000000041C1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.290258767.00000000041C1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	unknown
C:\Users\user\AppData\Roaming\LrSEeB.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C651E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp476F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C657038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Jens Frodesen CV.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DB1C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp476F.tmp	success or wait	1	6C656A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\LrSEeB.exe	0	1053184	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 3c 31 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 3a 0f 00 00 fd 00 00 00 00 00 00 2e 58 0f 00 00 20 00 00 00 60 0f 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 10 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL<1cP:.X `@ `@	success or wait	1	6C651B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp476F.tmp	0	1655	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?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> </Registrati	success or wait	1	6C651B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Jens Frodesen CV.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DB1C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Users\user\Desktop\Jens Frodesen CV.exe	unknown	1053184	success or wait	1	6C651B4F	ReadFile

Analysis Process: schtasks.exe PID: **5452**, Parent PID: **2932**

General

Target ID:	1
Start time:	04:11:38
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\LrSEeB" /XML "C:\Users\user\AppData\Local\Temp\tmp476F.tmp
Imagebase:	0x12c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp476F.tmp	unknown	2	success or wait	1	12CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp476F.tmp	unknown	1656	success or wait	1	12CABD9	ReadFile

Analysis Process: conhost.exe PID: **5320**, Parent PID: **5452**

General

Target ID:	2
Start time:	04:11:38
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: Jens Frodesen CV.exe PID: **5344**, Parent PID: **2932**

General

Target ID:	3
Start time:	04:11:38
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\Jens Frodesen CV.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x610000
File size:	1053184 bytes
MD5 hash:	89197E451346ED5A3BA154F394948DE7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.544223992.0000000005DD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.544223992.0000000005DD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.544223992.0000000005DD0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.544223992.0000000005DD0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.548893461.00000000070B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.548893461.00000000070B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.548893461.00000000070B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.548893461.00000000070B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.536015397.0000000003F25000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.536015397.0000000003F25000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.518836400.0000000002B71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.518836400.0000000002B71000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.518836400.0000000002B71000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.278495402.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.278495402.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000003.00000000.278495402.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000000.278495402.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.526400449.0000000002E2B000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.526400449.0000000002E2B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.544737083.0000000006150000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.544737083.0000000006150000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.544737083.0000000006150000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.544737083.0000000006150000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.544737083.0000000006150000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.537384357.0000000004010000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.537384357.0000000004010000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.537384357.0000000004010000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.541798909.0000000005400000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.541798909.0000000005400000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.541798909.0000000005400000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.541798909.0000000005400000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.548537445.0000000007080000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.548537445.0000000007080000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.548537445.0000000007080000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.548537445.0000000007080000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.531321593.0000000003CDF000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.531321593.0000000003CDF000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.549029017.00000000070C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.549029017.00000000070C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.549029017.00000000070C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.549029017.00000000070C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.542986660.0000000005DC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.542986660.0000000005DC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.542986660.0000000005DC0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.542986660.0000000005DC0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.542226366.0000000005D60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.542226366.0000000005D60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.542226366.0000000005D60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.542226366.0000000005D60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.548413055.0000000007070000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.548413055.0000000007070000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.548413055.0000000007070000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.548413055.0000000007070000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.542387318.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.542387318.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth

	• Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.542387318.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.542387318.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000003.486665310.0000000006A38000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.542908530.0000000005DB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.542908530.0000000005DB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.542908530.0000000005DB0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.542908530.0000000005DB0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.549521024.0000000007100000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.549521024.0000000007100000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.549521024.0000000007100000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.549521024.0000000007100000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.548343986.0000000007060000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.548343986.0000000007060000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.548343986.0000000007060000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.548343986.0000000007060000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.535141648.0000000003EAF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.535141648.0000000003EAF000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.535141648.0000000003EAF000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.548639274.0000000007090000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.548639274.0000000007090000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.548639274.0000000007090000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.548639274.0000000007090000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C65BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C651E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C65BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C65DD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C65DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7194.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C657038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C651E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp75AC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C657038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C65BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C65BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	6C651E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C651E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7194.tmp	success or wait	1	6C656A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp75AC.tmp	success or wait	1	6C656A95	DeleteFileW
C:\Users\user\Desktop\Jens Frodesen CV.exe:Zone.Identifier	success or wait	1	6C5D2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	40 02 fd 38 42 fd fd 48	@8BH	success or wait	1	6C651B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 3c 31 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 3a 0f 00 00 fd 00 00 00 00 00 00 2e 58 0f 00 00 20 00 00 00 60 0f 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 10 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL<1cP:.X `@ `@	success or wait	5	6C65DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6C65DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7194.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	6C651B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	47	43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 44 65 73 6b 74 6f 70 5c 4a 65 6e 73 20 46 72 6f 64 65 73 65 6e 20 43 56 2e 65 78 65	C:\Users\user\Desktop\Jens Frodesen CV.exe	success or wait	1	6C651B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp75AC.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	6C651B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	2	6C651B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327432	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	6C651B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D7CD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D7CD72F	unknown
C:\Users\user\Desktop\Jens Frodesen CV.exe	unknown	4096	success or wait	1	6D7CD72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Jens Frodesen CV.exe	unknown	512	success or wait	1	6D7CD72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6C65646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **4188**, Parent PID: **5344**

General

Target ID:	5
Start time:	04:11:42
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp7194.tmp
Imagebase:	0x12c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7194.tmp	unknown	2	success or wait	1	12CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7194.tmp	unknown	1311	success or wait	1	12CABD9	ReadFile

Analysis Process: conhost.exe PID: **2600**, Parent PID: **4188**

General

Target ID:	6
Start time:	04:11:42
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: **6072**, Parent PID: **5344**

General	
Target ID:	8
Start time:	04:11:43
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp75AC.tmp
Imagebase:	0x12c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp75AC.tmp	unknown	2	success or wait	1	12CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp75AC.tmp	unknown	1311	success or wait	1	12CABD9	ReadFile

Analysis Process: conhost.exe PID: **5556**, Parent PID: **6072**

General	
Target ID:	10
Start time:	04:11:43
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: Jens Frodesen CV.exe PID: **244**, Parent PID: **1100**

General	
Target ID:	12
Start time:	04:11:44
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\Jens Frodesen CV.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Jens Frodesen CV.exe" 0
Imagebase:	0xe80000
File size:	1053184 bytes
MD5 hash:	89197E451346ED5A3BA154F394948DE7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpBFFB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C657038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBFFB.tmp	success or wait	1	6C656A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBFFB.tmp	0	1655	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?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> </Registrati	success or wait	1	6C651B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C651B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **4320**, Parent PID: **1100**

General

Target ID:	14
Start time:	04:11:45
Start date:	28/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xd30000
File size:	1053184 bytes
MD5 hash:	89197E451346ED5A3BA154F394948DE7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 60%, ReversingLabs • Detection: 57%, Virustotal, Browse • Detection: 33%, Metadefender, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpC1DF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C657038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DB1C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC1DF.tmp	success or wait	1	6C656A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC1DF.tmp	0	1655	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?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> </Registrati	success or wait	1	6C651B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DB1C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C651B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **988**, Parent PID: **3320**

General	
Target ID:	20
Start time:	04:11:51
Start date:	28/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xe10000
File size:	1053184 bytes
MD5 hash:	89197E451346ED5A3BA154F394948DE7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: schtasks.exe PID: **5080**, Parent PID: **244**

General	
Target ID:	22
Start time:	04:12:09
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\LrSEeB" /XML "C:\Users\user\AppData\Local\Temp\tmpBFFB.tmp
Imagebase:	0x12c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **5564**, Parent PID: **4320**

General	
Target ID:	23
Start time:	04:12:12
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\LrSEeB" /XML "C:\Users\user\AppData\Local\Temp\tmpC1DF.tmp
Imagebase:	0x12c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5552**, Parent PID: **5080**

General	
Target ID:	24
Start time:	04:12:12
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5200**, Parent PID: **5564**

General	
Target ID:	25
Start time:	04:12:12
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Jens Frodesen CV.exe PID: **1540**, Parent PID: **244**

General	
Target ID:	27
Start time:	04:12:13
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\Jens Frodesen CV.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0xf0000
File size:	1053184 bytes
MD5 hash:	89197E451346ED5A3BA154F394948DE7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **3104**, Parent PID: **4320**

General	
Target ID:	28
Start time:	04:12:14
Start date:	28/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true

Commandline:	{path}
Imagebase:	0xfe0000
File size:	1053184 bytes
MD5 hash:	89197E451346ED5A3BA154F394948DE7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001C.00000002.411921875.0000000004408000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.405231773.0000000003391000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.405231773.0000000003391000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001C.00000002.405231773.0000000003391000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001C.00000002.411534974.00000000043EF000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001C.00000002.410904877.00000000043DB000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: Jens Frodesen CV.exe PID: **4720**, Parent PID: **244**

General

Target ID:	29
Start time:	04:12:14
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\Jens Frodesen CV.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc70000
File size:	1053184 bytes
MD5 hash:	89197E451346ED5A3BA154F394948DE7
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: 0000001D.00000002.405844203.0000000003101000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.405844203.0000000003101000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001D.00000002.405844203.0000000003101000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: schtasks.exe PID: **5524**, Parent PID: **988**

General

Target ID:	30
Start time:	04:12:20
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\LrSEeB" /XML "C:\Users\user\AppData\Local\Temp\tmpE91E.tmp
Imagebase:	0x12c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5628**, Parent PID: **5524**

General

Target ID:	31
Start time:	04:12:21
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **5788**, Parent PID: **988**

General	
Target ID:	32
Start time:	04:12:23
Start date:	28/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd30000
File size:	1053184 bytes
MD5 hash:	89197E451346ED5A3BA154F394948DE7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Disassembly

No disassembly