ID: 526200
Sample Name: purchase order NI32855 (1).exe
Cookbook: default.jbs
Time: 11:36:24
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report purchase order Nl32855 (1).exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
System Summary: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Jbx Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
Operating System Destruction: 7
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 17
General 17
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Data Directories 18
Sections 18
Resources 18
Imports 18
Version Infos 18
Network Behavior 18
Snort IDS Alerts 18
Network Port Distribution 19
TCP Packets 19
UDP Packets 19

DNS Queries 19
DNS Answers 20
Code Manipulations 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: purchase order NI32855 (1).exe PID: 6824 Parent PID: 6012 21
General 21
File Activities 21
File Created 21
File Deleted 21
File Written 21
File Read 21
Analysis Process: schtasks.exe PID: 5936 Parent PID: 6824 21
General 22
File Activities 22
File Read 22
Analysis Process: conhost.exe PID: 1328 Parent PID: 5936 22
General 22
Analysis Process: purchase order NI32855 (1).exe PID: 1668 Parent PID: 6824 22
General 22
File Activities 23
File Created 23
File Deleted 23
File Written 23
File Read 23
Registry Activities 23
Key Value Created 24
Analysis Process: schtasks.exe PID: 3396 Parent PID: 1668 24
General 24
File Activities 24
File Read 24
Analysis Process: conhost.exe PID: 5732 Parent PID: 3396 24
General 24
Analysis Process: purchase order NI32855 (1).exe PID: 4864 Parent PID: 968 24
General 24
File Activities 25
File Created 25
File Deleted 25
File Written 25
File Read 25
Analysis Process: schtasks.exe PID: 3296 Parent PID: 1668 25
General 25
File Activities 25
File Read 25
Analysis Process: conhost.exe PID: 5648 Parent PID: 3296 25
General 25
Analysis Process: schtasks.exe PID: 6764 Parent PID: 4864 26
General 26
File Activities 26
File Read 26
Analysis Process: dhcpmon.exe PID: 6700 Parent PID: 968 26
General 26
File Activities 26
File Created 26
File Deleted 26
File Written 26
File Read 26
Analysis Process: conhost.exe PID: 7028 Parent PID: 6764 26
General 27
Analysis Process: purchase order NI32855 (1).exe PID: 5580 Parent PID: 4864 27
General 27
Analysis Process: dhcpmon.exe PID: 7084 Parent PID: 3424 28
General 28
Analysis Process: schtasks.exe PID: 7044 Parent PID: 6700 29
General 29
Analysis Process: conhost.exe PID: 4592 Parent PID: 7044 29
General 29
Analysis Process: dhcpmon.exe PID: 6252 Parent PID: 6700 29
General 29
Analysis Process: schtasks.exe PID: 6864 Parent PID: 7084 30
General 30
Analysis Process: conhost.exe PID: 7152 Parent PID: 6864 31
General 31
Analysis Process: dhcpmon.exe PID: 5820 Parent PID: 7084 31
General 31
Analysis Process: dhcpmon.exe PID: 2044 Parent PID: 7084 31
General 31
Analysis Process: dhcpmon.exe PID: 5984 Parent PID: 7084 31
General 31
Disassembly 32
Code Analysis 32

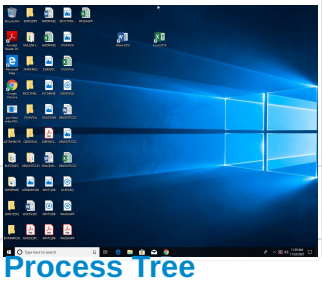
Windows Analysis Report purchase order Nl32855 (1).exe

Overview

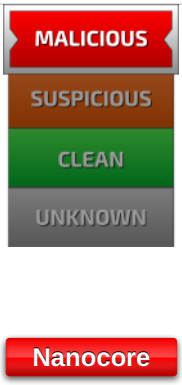
General Information

Sample Name:	purchase order Nl32855 (1).exe
Analysis ID:	526200
MD5:	c466151570c893..
SHA1:	3e779ff5c71f319…
SHA256:	dee5267af261b8e.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

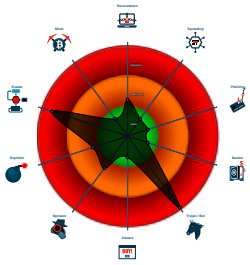


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a …
- Connects to many ports of the same…
- Protects its processes via BreakOnT…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- purchase order Nl32855 (1).exe (PID: 6824 cmdline: "C:\Users\user\Desktop\purchase order Nl32855 (1).exe" MD5: C466151570C893F56D548A9689155656)
  - schtasks.exe (PID: 5936 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qZEskWcTYJLciB" /XML "C:\Users\user\AppData\Local\Temp\tmpB6B0.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - purchase order Nl32855 (1).exe (PID: 1668 cmdline: {path} MD5: C466151570C893F56D548A9689155656)
    - schtasks.exe (PID: 3396 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp1F1D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 3296 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp2A39.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- purchase order Nl32855 (1).exe (PID: 4864 cmdline: "C:\Users\user\Desktop\purchase order Nl32855 (1).exe" 0 MD5: C466151570C893F56D548A9689155656)
  - schtasks.exe (PID: 6764 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qZEskWcTYJLciB" /XML "C:\Users\user\AppData\Local\Temp\tmpE496.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - purchase order Nl32855 (1).exe (PID: 5580 cmdline: {path} MD5: C466151570C893F56D548A9689155656)
- dhcpmon.exe (PID: 6700 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: C466151570C893F56D548A9689155656)
  - schtasks.exe (PID: 7044 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qZEskWcTYJLciB" /XML "C:\Users\user\AppData\Local\Temp\tmpF1A6.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6252 cmdline: {path} MD5: C466151570C893F56D548A9689155656)
- dhcpmon.exe (PID: 7084 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: C466151570C893F56D548A9689155656)
  - schtasks.exe (PID: 6864 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qZEskWcTYJLciB" /XML "C:\Users\user\AppData\Local\Temp\tmpD.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 5820 cmdline: {path} MD5: C466151570C893F56D548A9689155656)
  - dhcpmon.exe (PID: 2044 cmdline: {path} MD5: C466151570C893F56D548A9689155656)
  - dhcpmon.exe (PID: 5984 cmdline: {path} MD5: C466151570C893F56D548A9689155656)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6c7be0fb-d973-4d3c-b342-92a2df7c",
  "Group": "Wiz",
  "Domain1": "lizaelock.ddns.net",
  "Domain2": "",
  "Port": 52149,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8009,
  "BufferSize": "02000100",
  "MaxPacketSize": "",
  "GCThreshold": "",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task>"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.922693720.000000000600 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000007.00000002.922693720.000000000600 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000007.00000002.922693720.000000000600 0000.00000004.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000010.00000000.700142323.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000010.00000000.700142323.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 115 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.purchase order NI32855 (1).exe.434ec86.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4083:$x1: NanoCore.ClientPluginHost
16.2.purchase order NI32855 (1).exe.434ec86.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x4083:$x2: NanoCore.ClientPluginHost • 0x4161:$s4: PipeCreated • 0x409d:$s5: IClientLoggingHost
27.2.dhcpmon.exe.4513ac3.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1646:$x1: NanoCore.ClientPluginHost • 0x151e3:$x1: NanoCore.ClientPluginHost • 0x2e17a:$x1: NanoCore.ClientPluginHost • 0x15210:$x2: IClientNetworkHost • 0x2e1a7:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
27.2.dhcpmon.exe.4513ac3.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1646:$x2: NanoCore.ClientPluginHost • 0x151e3:$x2: NanoCore.ClientPluginHost • 0x2e17a:$x2: NanoCore.ClientPluginHost • 0x1724:$s4: PipeCreated • 0x162be:$s4: PipeCreated • 0x2f255:$s4: PipeCreated • 0x1660:$s5: IClientLoggingHost • 0x151fd:$s5: IClientLoggingHost • 0x2e194:$s5: IClientLoggingHost
27.2.dhcpmon.exe.4513ac3.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 222 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

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

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

Operating System Destruction:

Protects its processes via BreakOnTermination flag

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

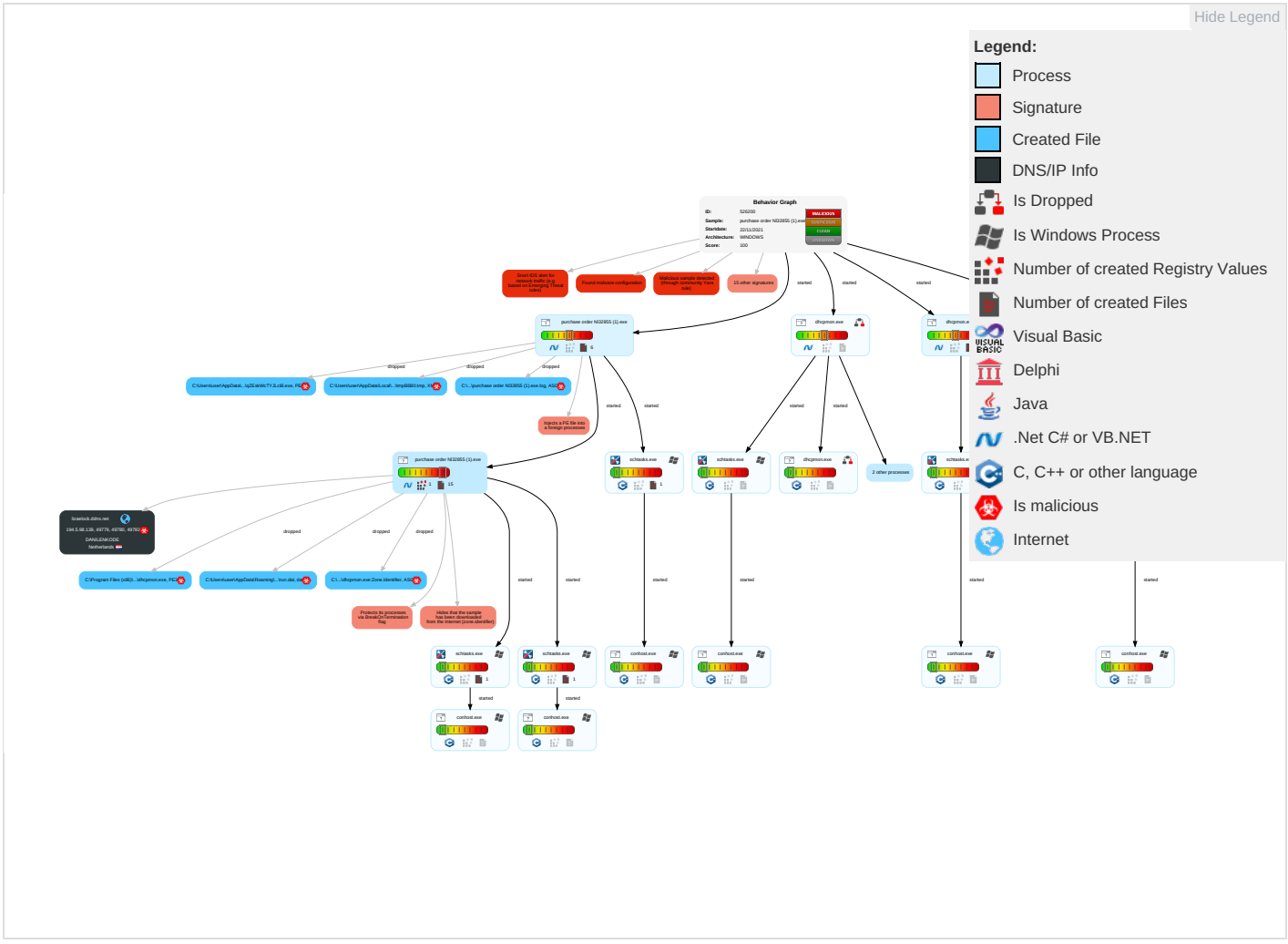
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Command and Scripting Interpreter 2	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	Exploi Track Locati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 1	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base

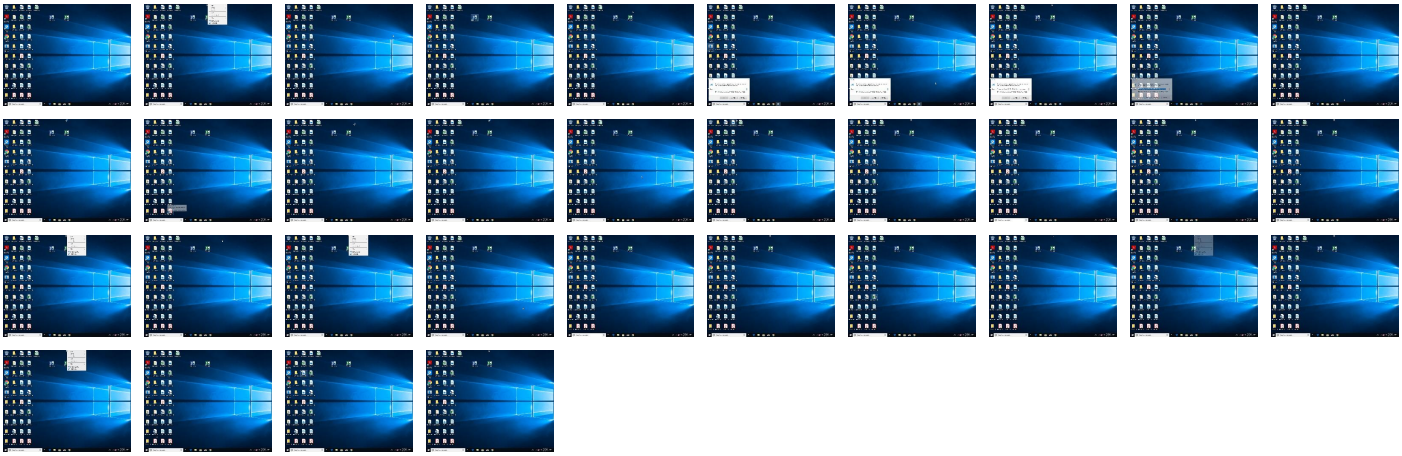
Behavior Graph



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
purchase order NI32855 (1).exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\qZEskWcTYJLciB.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.Mardom	
C:\Users\user\AppData\Roaming\qZEskWcTYJLciB.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.Mardom	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.purchase order NI32855 (1).exe.4482490.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File
20.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
20.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
20.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
20.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.purchase order NI32855 (1).exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.purchase order NI32855 (1).exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.purchase order NI32855 (1).exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.purchase order NI32855 (1).exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.purchase order NI32855 (1).exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.2.purchase order NI32855 (1).exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.purchase order NI32855 (1).exe.6000000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File
20.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
20.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.purchase order NI32855 (1).exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.purchase order NI32855 (1).exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.purchase order NI32855 (1).exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.purchase order NI32855 (1).exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.purchase order NI32855 (1).exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.purchase order NI32855 (1).exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.fontbureau.commiv	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fonts.comro	0%	Avira URL Cloud	safe	
http://www.tiro.com8	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomov	0%	Avira URL Cloud	safe	
http://www.carterandcone.comal	0%	URL Reputation	safe	
http://www.tiro.com.	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fonts.comicy	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://tempuri.org/REFRWFWFGB.xsdX1	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comtteo	0%	Avira URL Cloud	safe	
http://www.carterandcone.com8	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.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.comx	0%	URL Reputation	safe	
http://www.fontbureau.comueed	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.carterandcone.comgy	0%	Avira URL Cloud	safe	
http://www.carterandcone.comc	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.fonts.comTF	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krn	0%	Avira URL Cloud	safe	
lizaelock.ddns.net	0%	Avira URL Cloud	safe	
http://www.tiro.comcoo	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com-d	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.fontbureau.comiond	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comlvfet	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sajatypeworks.coma-d	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.sandoll.co.krl)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lizaelock.ddns.net	194.5.98.139	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
lizaelock.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.139	lizaelock.ddns.net	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526200
Start date:	22.11.2021
Start time:	11:36:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	purchase order NI32855 (1).exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
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@34/14@18/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.8% (good quality ratio 1.6%) • Quality average: 58.3% • Quality standard deviation: 19.5%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:37:20	API Interceptor	890x Sleep call for process: purchase order NI32855 (1).exe modified
11:37:29	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\purchase order NI32855 (1).exe" s>$(Arg0)
11:37:29	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
11:37:34	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
11:37:35	API Interceptor	4x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	8mTwU7uNFV.exe	Get hash	malicious	Browse	• 194.5.97.131
	KNpmkMT5f3.exe	Get hash	malicious	Browse	• 194.5.98.12
	scvRj4lo1E.exe	Get hash	malicious	Browse	• 194.5.98.11
	#RFQ ORDER484425083-NJ.exe	Get hash	malicious	Browse	• 194.5.98.120
	RzUbuIerbF.exe	Get hash	malicious	Browse	• 194.5.97.207
	SIGNED_COPY_IMG_ORDER_...REQUEST_IMG_123456.exe	Get hash	malicious	Browse	• 194.5.98.5
	NOA MU21S0029729.exe	Get hash	malicious	Browse	• 194.5.97.207
	New purchase order 4940009190,pdf.exe	Get hash	malicious	Browse	• 194.5.97.23
	Fattura_del_cliente_V406307-scan.exe	Get hash	malicious	Browse	• 194.5.97.165
	ML822VOG-R11.doc	Get hash	malicious	Browse	• 194.5.97.131
	6Xzgfme0z6.exe	Get hash	malicious	Browse	• 194.5.97.131
	ESTADO+10+DE+NOVIEMBRE+DE+2021-101121.pdf.js	Get hash	malicious	Browse	• 194.5.98.48
	RTQFHtPW9x.exe	Get hash	malicious	Browse	• 194.5.98.107
	Document#053681.exe	Get hash	malicious	Browse	• 194.5.98.204
	4vo6jE1nlG.exe	Get hash	malicious	Browse	• 194.5.97.54
	ORDEN DE COMPRA-PDF.exe	Get hash	malicious	Browse	• 194.5.97.149
	Confirmation Transfer Copy MT102-Ref No#01018.exe	Get hash	malicious	Browse	• 194.5.98.105
	Confirmation Transfer Copy MT102-Ref No-01018.exe	Get hash	malicious	Browse	• 194.5.98.105
	PAYMENT COPY EXPORT1024 SCANNED DOCUMENT_pdf.exe	Get hash	malicious	Browse	• 194.5.98.30
	proforma invoice.exe	Get hash	malicious	Browse	• 194.5.97.24

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\purchase order NI32855 (1).exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	905728
Entropy (8bit):	7.6297829537885145
Encrypted:	false
SSDEEP:	24576:PrvL1uC0ETv0RlhBWDhor6xb39C0UxKe4:zjMC0EUWoWxbtC0Ux
MD5:	C466151570C893F56D548A9689155656
SHA1:	3E779FF5C71F319FC2D3BD4FC577C4769873C47C
SHA-256:	DEE5267AF261B8E291B83B01B12C4149204B20754CD1714BD974AE1DAE447A44
SHA-512:	3905DEA297E356FD7E79CF78FF74DD3991B982D8644DA7764490AF16E3805D0D5F4008875F84E9963A1108402A7552C2BBBC34C47CBC0BA49DB58FC5E0912D7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...aA.a.....P..... .....@.. ....@.....W..... ....H.....text...$.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....4.....0.....+G.. .D.L I...Xe [X.#X(....8m..... .L|Y.c 5._.Yf(.....#..xKs.;@(.....+.....+..(....(....,. .+..+.-.s....z+...(....(.....(.....o....+..+..*.....q.....+"...(.....(.....(.....(....+.(....+..*....0.....+F.. .t.. .x.ae.b(....+d....f.b.cf(.....#].j...6@(.....(....(.....+.....+...(....#.....4 .s....z+...(....o....(....+..+..*&..(.....*...0.....+:.. ._..

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

Process:	C:\Users\user\Desktop\purchase order NI32855 (1).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

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\purchase order NI32855 (1).exe.log	
Process:	C:\Users\user\Desktop\purchase order NI32855 (1).exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp1F1D.tmp	
Process:	C:\Users\user\Desktop\purchase order NI32855 (1).exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1316
Entropy (8bit):	5.121919122223019
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Yqoxtn:cbk4oL600QydbQxIYODOLedq3/j
MD5:	B3EA453FCBEB8FBF6CAB740016195F59
SHA1:	451555DF676B904C4DBB60658A46E29F653010EC
SHA-256:	2B040C3DA540034472349FC447F9937078FADD816184A7F32B4E884022591331
SHA-512:	B82F4B94E3AF9BE25BD2449AB63438B652F406A66DB75BF8A1C96567F0519A9E413316FC3403E778A7D51699D5318E4BC1339EE65F5608E9036BC82134ECE055
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\tmp2A39.tmp	
Process:	C:\Users\user\Desktop\purchase order NI32855 (1).exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
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\tmpB6B0.tmp	
Process:	C:\Users\user\Desktop\purchase order NI32855 (1).exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.194002325084267
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGBtn:cbhK79lNQR/rydbz9I3YODOLNdq34
MD5:	F59692EC8A4A1CAF77DF808660F8773D
SHA1:	FB7428EEEAB5557BD7B2D86328000D0504F801D4
SHA-256:	D6C3A95C1A7F4725FC9DA533F37AE246913F3B247729B5560B0EC34022590C1C
SHA-512:	9D3FC95B70EE777A1B5605F92E124C5F4F512760C7303AE3B6914186FA9616AC384FCEE170D31DDF7F28965231F7DFFDD83CBFF932E8BEB293C4347938818B68
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpD.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):	1647
Entropy (8bit):	5.194002325084267
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGBtn:cbhK79lNQR/rydbz9I3YODOLNdq34
MD5:	F59692EC8A4A1CAF77DF808660F8773D
SHA1:	FB7428EEEAB5557BD7B2D86328000D0504F801D4
SHA-256:	D6C3A95C1A7F4725FC9DA533F37AE246913F3B247729B5560B0EC34022590C1C
SHA-512:	9D3FC95B70EE777A1B5605F92E124C5F4F512760C7303AE3B6914186FA9616AC384FCEE170D31DDF7F28965231F7DFFDD83CBFF932E8BEB293C4347938818B68
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>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpE496.tmp	
Process:	C:\Users\user\Desktop\purchase order NI32855 (1).exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.194002325084267
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmpE496.tmp	
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGBtn:cbhK79lNQR/rydbz9I3YODOLNdq34
MD5:	F59692EC8A4A1CAF77DF808660F8773D
SHA1:	FB7428EEEAB5557BD7B2D86328000D0504F801D4
SHA-256:	D6C3A95C1A7F4725FC9DA533F37AE246913F3B247729B5560B0EC34022590C1C
SHA-512:	9D3FC95B70EE777A1B5605F92E124C5F4F512760C7303AE3B6914186FA9616AC384FCEE170D31DDF7F28965231F7DFFDD83CBFF932E8BEB293C4347938818B68
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>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpF1A6.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):	1647
Entropy (8bit):	5.194002325084267
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGBtn:cbhK79lNQR/rydbz9I3YODOLNdq34
MD5:	F59692EC8A4A1CAF77DF808660F8773D
SHA1:	FB7428EEEAB5557BD7B2D86328000D0504F801D4
SHA-256:	D6C3A95C1A7F4725FC9DA533F37AE246913F3B247729B5560B0EC34022590C1C
SHA-512:	9D3FC95B70EE777A1B5605F92E124C5F4F512760C7303AE3B6914186FA9616AC384FCEE170D31DDF7F28965231F7DFFDD83CBFF932E8BEB293C4347938818B68
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>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\purchase order Nl32855 (1).exe
File Type:	data
Category:	modified
Size (bytes):	248
Entropy (8bit):	7.094528505897445
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7r3l3TmKEt5mT1DhFtMhXvvHOxHB3GDq:X4LEnybgCFCtvd7bl3ThE4T19FtMhXvs
MD5:	061E700FE27D852034A5A44BF5985CCF
SHA1:	15B072DE6D6FDD92AE36F074345FA41985833E8D
SHA-256:	4BBB88AF530693EB4A710B0591D4BAF585837242C5690F5A821BF2FC9CC587CD
SHA-512:	CF6C5458AB50C859740490985D1E7E887D1116F3FA947FF2EC49AF9997A42F3402C63EF42B93498544195D9859FBB19CCC295966564B30F5ADB4A36D4E8886C6
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....f.Z#.|...@HkG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.w

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\purchase order Nl32855 (1).exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:qxUn:qGn
MD5:	70C5D1CA98E20B48E039DC2D2F27E9AC
SHA1:	1FF2A12B26BBF01273382148CBD51F620C9E9F37
SHA-256:	AF8F8563BFAE6FA1C9533608D08204BB60F1B493526451F31946600293BA5E93
SHA-512:	415E287E7359A1586B8A0AF6F04E19EA692B22BE0337D0B3ADB374D37F81749695B923C7CE5577D696CDD0F633F150B18D901A28D96B2B81FD706E7C3F646981
Malicious:	**true**
Preview:	I.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\purchase order Nl32855 (1).exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	53
Entropy (8bit):	4.581299701107217
Encrypted:	false
SSDEEP:	3:oNt+WfWVQXPlKRAXviFJ:oNwv6flAAXsJ
MD5:	39C4FD27C1A6910541DD4EDC5CE47CF3
SHA1:	0CE74106ADF74582B293815D490CBA3ED810D48A
SHA-256:	89D32A70C724C479490D80EF9840196B498283C1EB5E83A7E753B5BD3DB0461A
SHA-512:	910192D172B971BBDD30E3A693876738DB5E43C010A99C8BA3A59498F906F3FC3B61560A05A2311A594DC948BB9FA6DAA39BFD28635FA240C417C6C403D79BE
Malicious:	false
Preview:	C:\Users\user\Desktop\purchase order Nl32855 (1).exe

C:\Users\user\AppData\Roaming\qZEskWcTYJLciB.exe	
Process:	C:\Users\user\Desktop\purchase order Nl32855 (1).exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	905728
Entropy (8bit):	7.6297829537885145
Encrypted:	false
SSDEEP:	24576:PrvL1uC0ETv0RlhBWDhor6xb39C0UxKe4:zjMC0EUWoWxbtC0Ux
MD5:	C466151570C893F56D548A9689155656
SHA1:	3E779FF5C71F319FC2D3BD4FC577C4769873C47C
SHA-256:	DEE5267AF261B8E291B83B01B12C4149204B20754CD1714BD974AE1DAE447A44
SHA-512:	3905DEA297E356FD7E79CF78FF74DD3991B982D8644DA7764490AF16E3805D0D5F4008875F84E9963A1108402A7552C2BBBC34C47CBC0BA49DB58FC5E0912D7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...aA.a.....P..... ....@.. ....@.....W..... ....H.....text...$.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....4.....0.....+G.. .D.L I...Xe [X.#X(....8m..... .L|Y.c 5._.Yf(.....#..xKs.;@(.....+.....+..(....(....,. .+..+.-.s....z+...(....(.....(.....o....+..+..*.....q.....+"...(.....(.....(.....(....+.(....+..*....0.....+F.. .t.. .x.ae.b(....+d....f.b.cf(.....#].j...6@(.....(....(.....+.....+...(....#.....4 .s....z+...(....o....(....+..+..*&..(.....*...0.....+:.. ._.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.6297829537885145
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:	purchase order Nl32855 (1).exe
File size:	905728
MD5:	c466151570c893f56d548a9689155656
SHA1:	3e779ff5c71f319fc2d3bd4fc577c4769873c47c
SHA256:	dee5267af261b8e291b83b01b12c4149204b20754cd1714bd974ae1dae447a44
SHA512:	3905dea297e356fd7e79cf78ff74dd3991b982d8644da7764490af16e3805d0d5f4008875f84e9963a1108402a7552c2bbbc34c47cbc0ba49db58fc5e0912d7e
SSDEEP:	24576:PrvL1uC0ETv0RlhBWDhor6xb39C0UxKe4:zjMC0EUWoWxbtC0Ux
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...aA.a.....P..... ....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ddb1e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619A4161 [Sun Nov 21 12:53:53 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xdbb24	0xdbc00	False	0.766134945606	data	7.63859252241	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xde000	0x1200	0x1200	False	0.366970486111	data	4.74333942103	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-11:37:34.054226	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	52149	192.168.2.4	194.5.98.139
11/22/21-11:37:39.981039	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64549	8.8.8.8	192.168.2.4
11/22/21-11:37:40.280703	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	52149	192.168.2.4	194.5.98.139
11/22/21-11:37:45.790795	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	52149	192.168.2.4	194.5.98.139
11/22/21-11:37:50.784357	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53700	8.8.8.8	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-11:37:51.093945	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	52149	192.168.2.4	194.5.98.139
11/22/21-11:37:56.610307	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	52149	192.168.2.4	194.5.98.139
11/22/21-11:38:02.474522	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56794	8.8.8.8	192.168.2.4
11/22/21-11:38:02.840365	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	52149	192.168.2.4	194.5.98.139
11/22/21-11:38:09.136075	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	52149	192.168.2.4	194.5.98.139
11/22/21-11:38:15.386754	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49794	52149	192.168.2.4	194.5.98.139
11/22/21-11:38:20.593700	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49823	52149	192.168.2.4	194.5.98.139
11/22/21-11:38:27.289261	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49825	52149	192.168.2.4	194.5.98.139
11/22/21-11:38:33.447629	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49831	52149	192.168.2.4	194.5.98.139
11/22/21-11:38:39.313657	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56448	8.8.8.8	192.168.2.4
11/22/21-11:38:39.748357	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49833	52149	192.168.2.4	194.5.98.139
11/22/21-11:38:45.971112	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49852	52149	192.168.2.4	194.5.98.139
11/22/21-11:38:52.042406	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62420	8.8.8.8	192.168.2.4
11/22/21-11:38:52.332306	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49857	52149	192.168.2.4	194.5.98.139
11/22/21-11:38:58.397492	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50183	8.8.8.8	192.168.2.4
11/22/21-11:38:58.714276	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49860	52149	192.168.2.4	194.5.98.139
11/22/21-11:39:05.164608	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49863	52149	192.168.2.4	194.5.98.139
11/22/21-11:39:11.138794	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59794	8.8.8.8	192.168.2.4
11/22/21-11:39:11.560279	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49864	52149	192.168.2.4	194.5.98.139
11/22/21-11:39:17.458297	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55916	8.8.8.8	192.168.2.4
11/22/21-11:39:17.857507	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49865	52149	192.168.2.4	194.5.98.139

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2021 11:37:33.626980066 CET	192.168.2.4	8.8.8.8	0xea7e	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:39.959726095 CET	192.168.2.4	8.8.8.8	0xb95c	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:45.372292995 CET	192.168.2.4	8.8.8.8	0x5a37	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:50.764760971 CET	192.168.2.4	8.8.8.8	0xcbba	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:56.182887077 CET	192.168.2.4	8.8.8.8	0xf125	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:02.453110933 CET	192.168.2.4	8.8.8.8	0x210	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:08.798513889 CET	192.168.2.4	8.8.8.8	0xd416	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:15.088176966 CET	192.168.2.4	8.8.8.8	0x396c	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2021 11:38:20.087798119 CET	192.168.2.4	8.8.8.8	0xc84c	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:26.719784975 CET	192.168.2.4	8.8.8.8	0xb72b	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:33.171699047 CET	192.168.2.4	8.8.8.8	0x486f	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:39.291726112 CET	192.168.2.4	8.8.8.8	0x1b2f	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:45.632385969 CET	192.168.2.4	8.8.8.8	0x97fc	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:52.021179914 CET	192.168.2.4	8.8.8.8	0x80ca	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:58.375895023 CET	192.168.2.4	8.8.8.8	0x122e	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:39:04.771280050 CET	192.168.2.4	8.8.8.8	0x8969	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:39:11.117847919 CET	192.168.2.4	8.8.8.8	0x207e	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 11:39:17.438092947 CET	192.168.2.4	8.8.8.8	0x5eda	Standard query (0)	lizaelock.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2021 11:37:33.647224903 CET	8.8.8.8	192.168.2.4	0xea7e	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:39.981039047 CET	8.8.8.8	192.168.2.4	0xb95c	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:45.391844988 CET	8.8.8.8	192.168.2.4	0x5a37	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:50.784357071 CET	8.8.8.8	192.168.2.4	0xcbba	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:37:56.202613115 CET	8.8.8.8	192.168.2.4	0xf125	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:02.474522114 CET	8.8.8.8	192.168.2.4	0x210	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:08.816556931 CET	8.8.8.8	192.168.2.4	0xd416	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:15.107410908 CET	8.8.8.8	192.168.2.4	0x396c	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:20.107250929 CET	8.8.8.8	192.168.2.4	0xc84c	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:26.739308119 CET	8.8.8.8	192.168.2.4	0xb72b	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:33.191854000 CET	8.8.8.8	192.168.2.4	0x486f	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:39.313657045 CET	8.8.8.8	192.168.2.4	0x1b2f	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:45.652359962 CET	8.8.8.8	192.168.2.4	0x97fc	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:52.042406082 CET	8.8.8.8	192.168.2.4	0x80ca	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:38:58.397491932 CET	8.8.8.8	192.168.2.4	0x122e	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:39:04.789175987 CET	8.8.8.8	192.168.2.4	0x8969	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)
Nov 22, 2021 11:39:11.138793945 CET	8.8.8.8	192.168.2.4	0x207e	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2021 11:39:17.458297014 CET	8.8.8.8	192.168.2.4	0x5eda	No error (0)	lizaelock.ddns.net		194.5.98.139	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: purchase order NI32855 (1).exe PID: 6824 Parent PID: 6012

General

Start time:	11:37:14
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\purchase order NI32855 (1).exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\purchase order NI32855 (1).exe"
Imagebase:	0x610000
File size:	905728 bytes
MD5 hash:	C466151570C893F56D548A9689155656
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: 00000000.00000002.677615387.0000000003F01000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.677615387.0000000003F01000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.677615387.0000000003F01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5936 Parent PID: 6824

General

Start time:	11:37:22
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qZEskWcTYJLciB" /XML "C:\Users\user\AppData\Local\Temp\tmpB6B0.tmp
Imagebase:	0xc20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 1328 Parent PID: 5936

General

Start time:	11:37:23
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: purchase order Nl32855 (1).exe PID: 1668 Parent PID: 6824

General

Start time:	11:37:24
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\purchase order Nl32855 (1).exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc30000
File size:	905728 bytes
MD5 hash:	C466151570C893F56D548A9689155656
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.922693720.0000000006000000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.922693720.0000000006000000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.922693720.0000000006000000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.672319406.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.672319406.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.672319406.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.917874645.000000000446B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.922681658.0000000005FF0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.922681658.0000000005FF0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.915976815.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.915976815.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.915976815.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.672759409.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.672759409.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.672759409.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.922602924.0000000005D50000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.922602924.0000000005D50000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.673837687.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.673837687.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.673837687.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.673297217.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.673297217.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.673297217.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 3396 Parent PID: 1668

General

Start time:	11:37:27
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp1F1D.tmp
Imagebase:	0xc20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5732 Parent PID: 3396

General

Start time:	11:37:28
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: purchase order NI32855 (1).exe PID: 4864 Parent PID: 968

General

Start time:	11:37:29
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\purchase order NI32855 (1).exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\purchase order NI32855 (1).exe" 0
Imagebase:	0xcf0000
File size:	905728 bytes
MD5 hash:	C466151570C893F56D548A9689155656
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.704899996.0000000004391000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.704899996.0000000004391000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.704899996.0000000004391000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 3296 Parent PID: 1668

General

Start time:	11:37:32
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp2A39.tmp
Imagebase:	0xc20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5648 Parent PID: 3296

General

Start time:	11:37:32
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6764 Parent PID: 4864

General

Start time:	11:37:34
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qZEskWcTYJLciB" /XML "C:\Users\user\AppData\Local\Temp\tmpE496.tmp
Imagebase:	0xc20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: dhcpmon.exe PID: 6700 Parent PID: 968

General

Start time:	11:37:34
Start date:	22/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x870000
File size:	905728 bytes
MD5 hash:	C466151570C893F56D548A9689155656
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: 0000000E.00000002.715852193.00000000041D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.715852193.00000000041D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.715852193.00000000041D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 20%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 7028 Parent PID: 6764

General

Start time:	11:37:35
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: purchase order NI32855 (1).exe PID: 5580 Parent PID: 4864

General

Start time:	11:37:36
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\purchase order NI32855 (1).exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa60000
File size:	905728 bytes
MD5 hash:	C466151570C893F56D548A9689155656
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: 00000010.00000000.700142323.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.700142323.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.700142323.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.699611919.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.699611919.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.699611919.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.698759095.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.698759095.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.698759095.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.716328250.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.716328250.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.716328250.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.717558485.0000000004301000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.717558485.0000000004301000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.717504195.0000000003301000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.717504195.0000000003301000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.700948566.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.700948566.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.700948566.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 7084 Parent PID: 3424

General

Start time:	11:37:37
Start date:	22/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x3c0000
File size:	905728 bytes
MD5 hash:	C466151570C893F56D548A9689155656
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: 00000011.00000002.732518649.0000000003C91000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.732518649.0000000003C91000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.732518649.0000000003C91000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: schtasks.exe PID: 7044 Parent PID: 6700

General

Start time:	11:37:37
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qZEskWcTYJLciB" /XML "C:\Users\user\AppData\Local\Temp\tmpF1A6.tmp
Imagebase:	0xc20000
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: conhost.exe PID: 4592 Parent PID: 7044

General

Start time:	11:37:38
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6252 Parent PID: 6700

General

Start time:	11:37:39
Start date:	22/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xfd0000
File size:	905728 bytes
MD5 hash:	C466151570C893F56D548A9689155656
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: 00000014.00000002.729145629.0000000004881000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.729145629.0000000004881000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000000.710553542.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000000.710553542.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000000.710553542.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000000.708011695.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000000.708011695.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000000.708011695.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000000.709668715.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000000.709668715.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000000.709668715.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.728891545.0000000003881000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.728891545.0000000003881000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.728031423.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.728031423.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.728031423.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000000.708878421.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000000.708878421.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000000.708878421.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: schtasks.exe PID: 6864 Parent PID: 7084

General

Start time:	11:37:41
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qZEskWcTYJLciB" /XML "C:\Users\user\AppData\Local\Temp\tmpD.tmp
Imagebase:	0xc20000
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: 7152 Parent PID: 6864

General

Start time:	11:37:42
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 5820 Parent PID: 7084

General

Start time:	11:37:43
Start date:	22/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x20000
File size:	905728 bytes
MD5 hash:	C466151570C893F56D548A9689155656
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 2044 Parent PID: 7084

General

Start time:	11:37:45
Start date:	22/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x320000
File size:	905728 bytes
MD5 hash:	C466151570C893F56D548A9689155656
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 5984 Parent PID: 7084

General

Start time:	11:37:46
Start date:	22/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd40000

File size:	905728 bytes
MD5 hash:	C466151570C893F56D548A9689155656
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: 0000001B.00000002.744724197.00000000044C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.744724197.00000000044C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.727842390.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.727842390.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.727842390.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.744635827.00000000034C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.744635827.00000000034C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.727053343.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.727053343.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.727053343.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.726440276.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.726440276.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.726440276.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.728365037.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.728365037.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.728365037.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000002.743854657.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.743854657.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.743854657.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis