ID: 708889
Sample Name:
2P4OWESFNE.exe
Cookbook: default.jbs
Time: 10:03:59
Date: 24/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

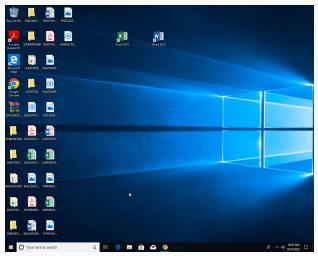
Windows Analysis Report

2P4OWESFNE.exe

Overview

General Information

Sample Name:	2P4OWESFNE.exe
Analysis ID:	708889
MD5:	69956e7cc66b2e..
SHA1:	63e96a654fd677..
SHA256:	38403140be1532..
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

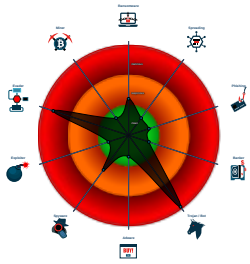
Nanocore

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**
- 2P4OWESFNE.exe (PID: 612 cmdline: "C:\Users\user\Desktop\2P4OWESFNE.exe" MD5: 69956E7CC66B2E6B4A15DC779D63B459)
  - 2P4OWESFNE.exe (PID: 6076 cmdline: C:\Users\user\Desktop\2P4OWESFNE.exe MD5: 69956E7CC66B2E6B4A15DC779D63B459)
  - 2P4OWESFNE.exe (PID: 4148 cmdline: C:\Users\user\Desktop\2P4OWESFNE.exe MD5: 69956E7CC66B2E6B4A15DC779D63B459)
    - schtasks.exe (PID: 812 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpD28D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 2108 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpDA9C.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 2P4OWESFNE.exe (PID: 6132 cmdline: C:\Users\user\Desktop\2P4OWESFNE.exe 0 MD5: 69956E7CC66B2E6B4A15DC779D63B459)
  - 2P4OWESFNE.exe (PID: 612 cmdline: C:\Users\user\Desktop\2P4OWESFNE.exe MD5: 69956E7CC66B2E6B4A15DC779D63B459)
- dhcpmon.exe (PID: 2328 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 69956E7CC66B2E6B4A15DC779D63B459)
  - dhcpmon.exe (PID: 4300 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 69956E7CC66B2E6B4A15DC779D63B459)
- dhcpmon.exe (PID: 3788 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 69956E7CC66B2E6B4A15DC779D63B459)
  - dhcpmon.exe (PID: 4648 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 69956E7CC66B2E6B4A15DC779D63B459)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "9c6d4c8a-884b-4287-8ce0-7edf4a23",
  "Group": "X File",
  "Domain1": "jasonbourne.bounceme.net",
  "Domain2": "127.0.0.1",
  "Port": 4032,
  "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
0000000B.00000002.545805454.0000000002D81000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000002.545805454.0000000002D81000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x2c939:$a1: NanoCore.ClientPluginHost • 0x2c8fc:$a2: NanoCore.ClientPlugin • 0x2ccd0:$b1: get_BuilderSettings • 0x2c987:$b4: IClientAppHost • 0x2cd41:$b6: AddHostEntry • 0x2cdb0:$b7: LogClientException • 0x2cd25:$b8: PipeExists • 0x2c974:$b9: IClientLoggingHost
0000000B.00000000.311191616.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000B.00000000.311191616.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000000.311191616.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
Click to see the 109 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.2P4OWESFNE.exe.6ec0000.23.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost
11.2.2P4OWESFNE.exe.6ec0000.23.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x8ba5:$x2: NanoCore.ClientPluginHost • 0x9b74:$s2: FileCommand • 0xe576:$s4: PipeCreated • 0x8bbf:$s5: IClientLoggingHost
11.2.2P4OWESFNE.exe.6ec0000.23.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x8b7f:$x2: NanoCore.ClientPlugin • 0x8ba5:$x3: NanoCore.ClientPluginHost • 0x8b70:$i3: IClientNetwork • 0x8b95:$i5: IClientDataHost • 0x8bbf:$i6: IClientLoggingHost • 0x8bd2:$i7: IClientNetworkHost • 0x8be5:$i9: IClientNameObjectCollection • 0x8902:$s1: ClientPlugin • 0x8b88:$s1: ClientPlugin
11.2.2P4OWESFNE.exe.6ec0000.23.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x8ba5:$a1: NanoCore.ClientPluginHost • 0x8b7f:$a2: NanoCore.ClientPlugin • 0x8bbf:$b9: IClientLoggingHost
11.2.2P4OWESFNE.exe.72f0000.27.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13a8:$x1: NanoCore.ClientPluginHost
Click to see the 290 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

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970840322816766 09/24/22-10:06:53.636236
SID:	2816766
Source Port:	49708
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970340322025019 09/24/22-10:06:04.969403
SID:	2025019
Source Port:	49703
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970040322025019 09/24/22-10:05:35.183673
SID:	2025019
Source Port:	49700
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970740322025019 09/24/22-10:06:45.272787
SID:	2025019
Source Port:	49707
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970440322816718 09/24/22-10:06:19.996354
SID:	2816718
Source Port:	49704
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 79.110.62.187 - Destination IP: 192.168.2.3	
Timestamp:	79.110.62.187192.168.2.34032497042810290 09/24/22-10:06:20.563916
SID:	2810290
Source Port:	4032
Destination Port:	49704
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970940322816766 09/24/22-10:06:59.700744
SID:	2816766
Source Port:	49709
Destination Port:	4032

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970240322816766 09/24/22-10:05:50.043192
SID:	2816766
Source Port:	49702
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970240322025019 09/24/22-10:05:48.835604
SID:	2025019
Source Port:	49702
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970540322816766 09/24/22-10:06:30.444040
SID:	2816766
Source Port:	49705
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970640322025019 09/24/22-10:06:38.454304
SID:	2025019
Source Port:	49706
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970340322816766 09/24/22-10:06:11.169922
SID:	2816766
Source Port:	49703
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970540322025019 09/24/22-10:06:29.331655
SID:	2025019
Source Port:	49705
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 79.110.62.187 - Destination IP: 192.168.2.3	
Timestamp:	79.110.62.187192.168.2.34032497002841753 09/24/22-10:05:39.949299
SID:	2841753
Source Port:	4032
Destination Port:	49700
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187

Timestamp:	192.168.2.379.110.62.1874971140322025019 09/24/22-10:07:30.021020
SID:	2025019
Source Port:	49711
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187

Timestamp:	192.168.2.379.110.62.1874970640322816766 09/24/22-10:06:39.820524
SID:	2816766
Source Port:	49706
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187

Timestamp:	192.168.2.379.110.62.1874971040322816766 09/24/22-10:07:06.791276
SID:	2816766
Source Port:	49710
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187

Timestamp:	192.168.2.379.110.62.1874970940322025019 09/24/22-10:06:58.980960
SID:	2025019
Source Port:	49709
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187

Timestamp:	192.168.2.379.110.62.1874970440322025019 09/24/22-10:06:16.738677
SID:	2025019
Source Port:	49704
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187

Timestamp:	192.168.2.379.110.62.1874970440322816766 09/24/22-10:06:19.996354
SID:	2816766
Source Port:	49704
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187

Timestamp:	192.168.2.379.110.62.1874970040322816766 09/24/22-10:05:41.035836
SID:	2816766
Source Port:	49700
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187

Timestamp:	192.168.2.379.110.62.1874971040322025019 09/24/22-10:07:05.908978
SID:	2025019
Source Port:	49710
Destination Port:	4032

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 79.110.62.187 - Destination IP: 192.168.2.3	
Timestamp:	79.110.62.187192.168.2.34032497032841753 09/24/22-10:06:09.982472
SID:	2841753
Source Port:	4032
Destination Port:	49703
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970740322816766 09/24/22-10:06:46.278312
SID:	2816766
Source Port:	49707
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 79.110.62.187	
Timestamp:	192.168.2.379.110.62.1874970840322025019 09/24/22-10:06:51.652364
SID:	2025019
Source Port:	49708
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 79.110.62.187 - Destination IP: 192.168.2.3	
Timestamp:	79.110.62.187192.168.2.34032497112841753 09/24/22-10:07:35.065229
SID:	2841753
Source Port:	4032
Destination Port:	49711
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 79.110.62.187 - Destination IP: 192.168.2.3	
Timestamp:	79.110.62.187192.168.2.34032497102841753 09/24/22-10:07:20.944242
SID:	2841753
Source Port:	4032
Destination Port:	49710
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

Networking

- Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

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

Remote Access Functionality

Detected Nanocore Rat

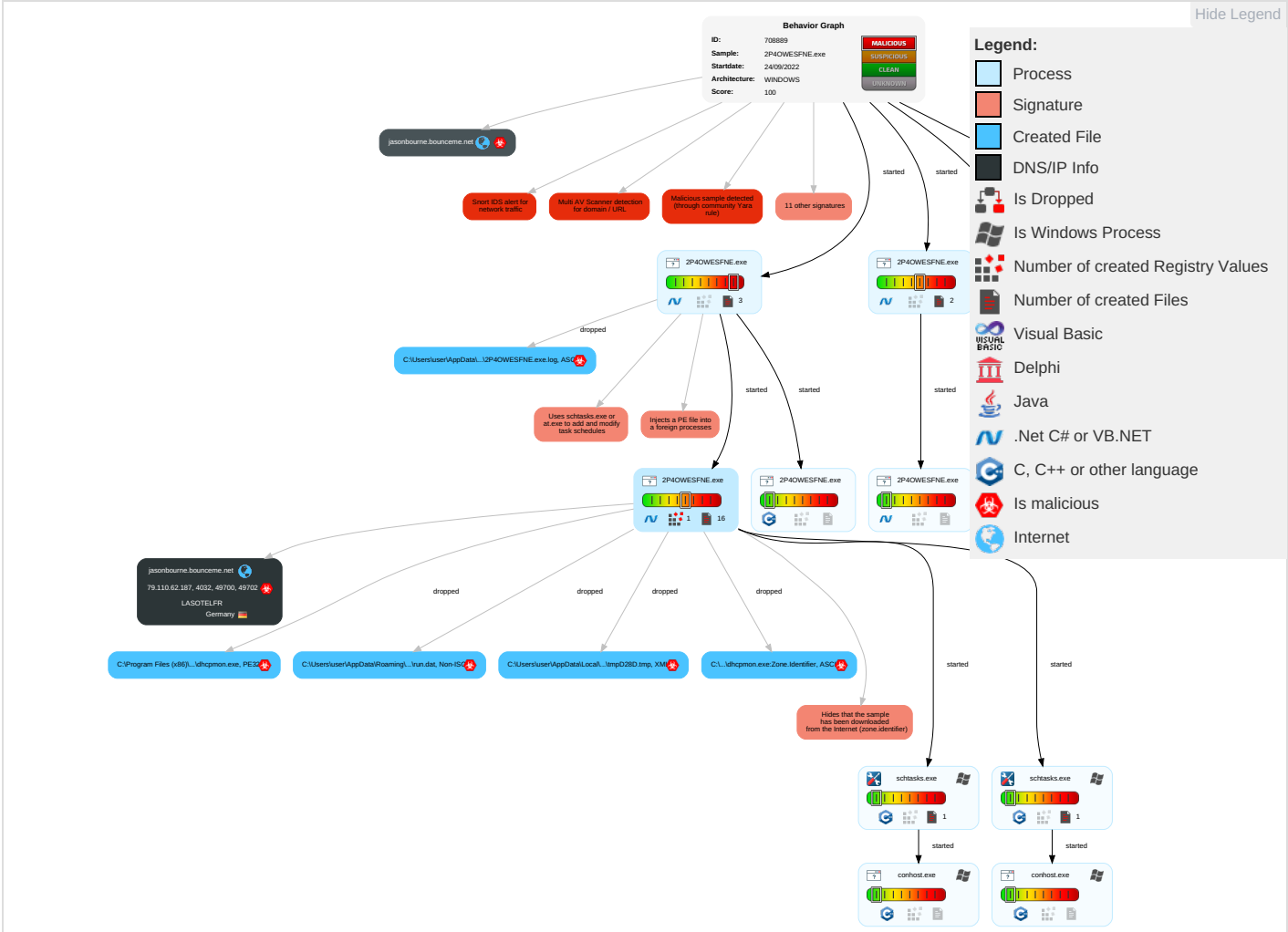
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 2 Process Injection	2 Masquerading	2 1 Input Capture	2 1 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	1 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	1 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	System Owner/User 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	1 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 3 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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Timestomp	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
2P4OWESFNE.exe	30%	ReversingLabs	Win32.Trojan.Pwsx	
2P4OWESFNE.exe	38%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.2P4OWESFNE.exe.3555928.8.unpack	100%	Avira	HEUR/AGEN.1244307		Download File
11.0.2P4OWESFNE.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.2P4OWESFNE.exe.6390000.20.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
jasonbourne.bounceme.net	22%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comb	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comlt	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comueto	0%	URL Reputation	safe	
http://www.fonts.comW	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	
jasonbourne.bounceme.net	22%	Virustotal		Browse
http://www.fontbureau.comK	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
jasonbourne.bounceme.net	100%	Avira URL Cloud	malware	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	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.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	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.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/X	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnP	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jasonbourne.bounceme.net	79.110.62.187	true	true	• 22%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
jasonbourne.bounceme.net	true	• 22%, Virustotal, Browse • Avira URL Cloud: malware	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comb	2P4OWESFNE.exe, 00000000.00000003.276563437.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276587282.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276454457.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276430334.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276470377.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276493423.000000000587E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	2P4OWESFNE.exe, 00000000.00000002.315982825.0000000000AD8000.00000004.00000020.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comK	2P4OWESFNE.exe, 00000000.00000002.315982825.0000000000AD8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlu	2P4OWESFNE.exe, 00000000.00000003.281277497.0000000005883000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comlt	2P4OWESFNE.exe, 00000000.00000003.277157816.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.277253089.000000000587F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://google.com	2P4OWESFNE.exe, 0000000B.00000002.562954773.0000000004671000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 0000000B.00000002.567018160.00000000048B7000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 0000000B.00000002.550686759.0000000002DED000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 0000000B.00000002.566126701.0000000004842000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 0000000B.00000002.582324415.0000000007300000.00000004.08000000.00040000.00000000.sdmp, 2P4OWESFNE.exe, 0000000B.00000002.568370273.00000000049A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.com	2P4OWESFNE.exe, 00000000.00000003.276965761.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.277157816.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276860526.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276563437.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276587282.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276770607.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276649732.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276409952.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276610677.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276454457.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276690868.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.277253089.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276430334.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276470377.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276493423.000000000587E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comueto	2P4OWESFNE.exe, 00000000.00000002.315982825.0000000000AD8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comW	2P4OWESFNE.exe, 00000000.00000003.273424033.0000000005885000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.273551028.0000000005885000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.273501204.0000000005885000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/X	2P4OWESFNE.exe, 00000000.00000003.275854585.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.275871672.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.275890999.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.275649189.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.275833969.000000000587E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	2P4OWESFNE.exe, 00000000.00000003.281609306.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.281684901.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.281306484.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.281498740.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.281466035.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.281525771.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.281277497.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.281568026.0000000005883000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.monotype.	2P4OWESFNE.exe, 00000000.00000003.282453873.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.282058555.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.282015592.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.282145563.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.281979992.0000000005883000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.282387327.0000000005883000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	2P4OWESFNE.exe, 00000000.00000003.276384161.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276409952.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276454457.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276430334.000000000587F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cnP	2P4OWESFNE.exe, 00000000.00000003.276322256.000000000587F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.273551028.0000000005885000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.273501204.0000000005885000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	2P4OWESFNE.exe, 00000000.00000003.276322256.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276384161.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	2P4OWESFNE.exe, 00000000.00000002.316838120.0000000002511000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 0000000B.00000002.545805454.0000000002D81000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 0000000F.00000002.396880865.0000000003281000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000011.00000002.405949937.0000000003021000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000012.00000002.436640584.0000000002DA1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.como.	2P4OWESFNE.exe, 00000000.00000003.276965761.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276860526.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276563437.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276587282.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276770607.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276649732.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276610677.000000000587E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276470377.000000000587F000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.276493423.000000000587E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	2P4OWESFNE.exe, 00000000.00000002.325916784.0000000006AE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designerst	2P4OWESFNE.exe, 00000000.00000003.280044708.000000000585E000.00000004.00000800.00020000.00000000.sdmp, 2P4OWESFNE.exe, 00000000.00000003.313553405.0000000005850000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.110.62.187	jasonbourne.bounceme.net	Germany		39180	LASOTELFR	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708889
Start date and time:	2022-09-24 10:03:59 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2P4OWESFNE.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:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@19/12@11/1
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, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- 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 NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:05:04	API Interceptor	928x Sleep call for process: 2P4OWESFNE.exe modified
10:05:30	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\2P4OWESFNE.exe" s>$(Arg0)
10:05:31	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
10:05:33	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
10:05:41	API Interceptor	222x 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\2P4OWESFNE.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1000448

Entropy (8bit):	7.037105846383947
Encrypted:	false
SSDEEP:	12288:0QhLuyAHRzxXSG2tmkgHAkC7trKPGCoY3qyfnkgl9TnmVuLkQDsGE1qF:lhLuyy6LtC+7ZKoifnHTn01GEc
MD5:	69956E7CC66B2E6B4A15DC779D63B459
SHA1:	63E96A654FD677DA56B73D14FC588A3581E8D57E
SHA-256:	38403140BE153292B9FA08BCD87DAE41E0F9E26327AAAC95A05FEA54DECC291B
SHA-512:	FFA9729470E7CFDE290CE3A406637D0B1E35A9D3AF912F826C879FF4021FB4AC2DE0A2ADB183B881836CA3E073AE196E8B50F9BE91FF10091E0D2700B4B1DC77
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....g.....0.....J..... ... .@.. ....@.....@...O.... ...F.....$..... ....H.....text..... ....`.rsrc....F... ...H.....@..@.reloc.....B.....@..B.....t.....H.....$....X.....6.....s}...}.....}.....(.....(.....*..0.....s.....o.....(.....*...0.....{....o....r...p(....,..{....o....r...p(....,..{....o....r...p(....+....9.....{....o.....{....o....(.....,W..{....{....o....{....o....o|....,#.r...p(....&s.....o.....(.....+.r)..p(....&.+.rK..p(....&.r...p(....&*....0..+.....,..{.....+....,..{....o.....(.....*..0.....s....}.....s....}.....s....}..

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

Process:	C:\Users\user\Desktop\2P4OWESFNE.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\2P4OWESFNE.exe.log

Process:	C:\Users\user\Desktop\2P4OWESFNE.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1394
Entropy (8bit):	5.340883346054895
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84F0:MIHK5HKXE1qHbHKnYHKhQnoPtHoxHhAR
MD5:	B51A52A837298BCF7A6EB58551AEF99C
SHA1:	61EEFCC20AC255B8651769E5C48E27B2A983FC4A
SHA-256:	1D393FBB3CE754EA699462C2778587A7F2451EB23BE2BD5084C95A46B20BE8AF
SHA-512:	138544399787651C847837719606197E539857206CCB271E0F4A86E2017FBADABADF5A235B6F6F1DA8ADE7EF29DBA3115CD1996AD01F92CA30C57D0BF217C11
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, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.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.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e08

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):	1394
Entropy (8bit):	5.340883346054895
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84F0:MIHK5HKXE1qHbHKnYHKhQnoPtHoxHhAR
MD5:	B51A52A837298BCF7A6EB58551AEF99C
SHA1:	61EEFCC20AC255B8651769E5C48E27B2A983FC4A

SHA-256:	1D393FBB3CE754EA699462C2778587A7F2451EB23BE2BD5084C95A46B20BE8AF
SHA-512:	138544399787651C847837719606197E539857206CCB271E0F4A86E2017FBADABADF5A235B6F6F1DA8ADE7EF29DBA3115CD1996AD01F92CA30C57D0BF217C11
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, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.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.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e08

C:\Users\user\AppData\Local\Temp\tmpD28D.tmp

Process:	C:\Users\user\Desktop\2P4OWESFNE.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.1160203935308814
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK05xtn:cbk4oL600QydbQxIYODOLedq3Sj
MD5:	BBD60B5934FEFE16364F0B45F08803EB
SHA1:	E60E779BD933C4FCEE0E15BE3320693A4870BD6F
SHA-256:	7BDEBD98B4E35A8C8D6200E016F2DB9B30B5248770491A217CBCDE110639AD80
SHA-512:	FB3852D91CF3650FEEE9EB158AE31EE0F50282B1FFA46DF508CD98D9A1F5A18F42BAFF0E1E1679676043CD8FF2F3A4514380989028CAC0571C7714E156E6810
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 />.. <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\tmpDA9C.tmp

Process:	C:\Users\user\Desktop\2P4OWESFNE.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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\Desktop\2P4OWESFNE.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:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35A5
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\2P4OWESFNE.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Fln:v
MD5:	7FB7ABD229F9A0F89181486D7EA04586
SHA1:	1A6F55BB4979E5D352DADDAC1D2EF4C4E2AC8761
SHA-256:	EBDFB2D20090C2B0EBAFC8B8EC78F0037F43FC0DD1226454804DFD726A8531D4
SHA-512:	98ABBA87DCCA807971F4ED1E926D262F5811CA78184FC75104B6A26D965B69AE37D4CB9B8CD1D10A998BFE9253FCDDE6CCBA2F1CE4C08D52BFBD15381452C43
Malicious:	**true**
Preview:	.6P.N..H

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

Process:	C:\Users\user\Desktop\2P4OWESFNE.exe
File Type:	data
Category:	modified
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F697
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

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

Process:	C:\Users\user\Desktop\2P4OWESFNE.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

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

Process:	C:\Users\user\Desktop\2P4OWESFNE.exe
File Type:	data
Category:	dropped
Size (bytes):	327432

Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. 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\2P4OWESFNE.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.540402352056965
Encrypted:	false
SSDEEP:	3:oNWXp5vXOrN:oNWXpFep
MD5:	539311B7FFA0BBE75465062AFA248697
SHA1:	100651CB385C480A88DD975894C1319281FEC5D9
SHA-256:	C88DA514977455D956906E192247F714A5191C861138170EB0E77265F6446F57
SHA-512:	E9370F2C60DF1CAE69475D80B2DA0BF70909EDB9728026DD1EF126D37BA9FB3B64FC4AE7E2E483FC009324B0BCC4F6669E5D3C2A4A2AA96B14BE38EBC8544A7C
Malicious:	false
Preview:	C:\Users\user\Desktop\2P4OWESFNE.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.037105846383947
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	2P4OWESFNE.exe
File size:	1000448
MD5:	69956e7cc66b2e6b4a15dc779d63b459
SHA1:	63e96a654fd677da56b73d14fc588a3581e8d57e
SHA256:	38403140be153292b9fa08bcd87dae41e0f9e26327aaac95a05fea54decc291b
SHA512:	ffa9729470e7cfde290ce3a406637d0b1e35a9d3af912f826c879ff4021fb4ac2de0a2adb183b881836ca3e073ae196e8b50f9be91ff10091e0d2700b4b1dc77
SSDEEP:	12288:0QhLuyAHRzxXSG2tmkgHAkC7trKPGCoY3qyfnkgl9TnmVuLkQDsGE1qF:lhLuyy6LtC+7ZKoifnHTn01GEc
TLSH:	FF25D0272AEA5F0BD02463B8C1E1D6F193A99C51E027C38B6FC67D9FB0A77209750752
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....g.....0.....J..... ... .@.. .....@.....

File Icon

Icon Hash:	ce9c9496e4949c9e

Static PE Info

General

Entrypoint:	0x4f1792
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:	0xDF67EFF8 [Sat Oct 9 03:26:48 2088 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
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
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	0xf1740	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf2000	0x46b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xf1724	0x1c	.text
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
.text	0x2000	0xef798	0xef800	False	0.7431202293188935	data	7.049986344828056	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xf2000	0x46b0	0x4800	False	0.5461154513888888	data	6.168153894151936	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf8000	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	0xf20e8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xf6310	0x14	data		
RT_VERSION	0xf6324	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

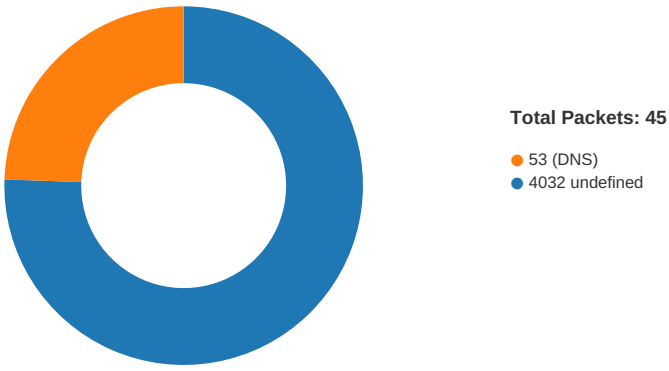
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.379.110.62.187 4970840322816766 09/24/22-10:06:53.636236	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970340322025019 09/24/22-10:06:04.969403	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970040322025019 09/24/22-10:05:35.183673	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	4032	192.168.2.3	79.110.62.187

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.379.110.62.187 4970740322025019 09/24/22-10:06:45.272787	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970440322816718 09/24/22-10:06:19.996354	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49704	4032	192.168.2.3	79.110.62.187
79.110.62.187192.168.2.3 4032497042810290 09/24/22-10:06:20.563916	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	4032	49704	79.110.62.187	192.168.2.3
192.168.2.379.110.62.187 4970940322816766 09/24/22-10:06:59.700744	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49709	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970240322816766 09/24/22-10:05:50.043192	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970240322025019 09/24/22-10:05:48.835604	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970540322816766 09/24/22-10:06:30.444040	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49705	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970640322025019 09/24/22-10:06:38.454304	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970340322816766 09/24/22-10:06:11.169922	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970540322025019 09/24/22-10:06:29.331655	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	4032	192.168.2.3	79.110.62.187
79.110.62.187192.168.2.3 4032497002841753 09/24/22-10:05:39.949299	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4032	49700	79.110.62.187	192.168.2.3
192.168.2.379.110.62.187 4971140322025019 09/24/22-10:07:30.021020	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49711	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970640322816766 09/24/22-10:06:39.820524	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49706	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4971040322816766 09/24/22-10:07:06.791276	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49710	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970940322025019 09/24/22-10:06:58.980960	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970440322025019 09/24/22-10:06:16.738677	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49704	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970440322816766 09/24/22-10:06:19.996354	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4970040322816766 09/24/22-10:05:41.035836	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49700	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.187 4971040322025019 09/24/22-10:07:05.908978	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49710	4032	192.168.2.3	79.110.62.187

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
79.110.62.187192.168.2.34032497032841753 09/24/22-10:06:09.982472	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4032	49703	79.110.62.187	192.168.2.3
192.168.2.379.110.62.1874970740322816766 09/24/22-10:06:46.278312	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49707	4032	192.168.2.3	79.110.62.187
192.168.2.379.110.62.1874970840322025019 09/24/22-10:06:51.652364	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	4032	192.168.2.3	79.110.62.187
79.110.62.187192.168.2.34032497112841753 09/24/22-10:07:35.065229	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4032	49711	79.110.62.187	192.168.2.3
79.110.62.187192.168.2.34032497102841753 09/24/22-10:07:20.944242	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4032	49710	79.110.62.187	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 24, 2022 10:05:34.885418892 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:34.916404963 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:34.916532040 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.183672905 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.263597012 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.300030947 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.330948114 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.564114094 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.695219994 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.777033091 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.799921036 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.799948931 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.799964905 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.799983025 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.800055027 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.800079107 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.830508947 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.830534935 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.830550909 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.830566883 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.830583096 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.830599070 CEST	4032	49700	79.110.62.187	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 24, 2022 10:05:35.830615044 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.830631018 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.830636978 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.830688000 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.861063957 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861093998 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861110926 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861129045 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861145973 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861164093 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861181021 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861197948 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861201048 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.861215115 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861231089 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861232042 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.861258030 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.861262083 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861279011 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861294031 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861299992 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.861311913 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.861340046 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.861399889 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.892014027 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892045021 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892061949 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892079115 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892102003 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.892127991 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.892174006 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892282963 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892323017 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892326117 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.892399073 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892438889 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.892474890 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892606020 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892657995 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.892678976 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892843008 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892874956 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892887115 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.892959118 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.892997026 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.893032074 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893075943 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893115044 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893115997 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.893151999 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893188000 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.893240929 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893258095 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893300056 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.893320084 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893356085 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893388987 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893404007 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.893404961 CEST	4032	49700	79.110.62.187	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 24, 2022 10:05:35.893461943 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.893556118 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893593073 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893634081 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893637896 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.893677950 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.893721104 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.910644054 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.922661066 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.922688007 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.922704935 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.922720909 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.922736883 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.922760963 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.922770977 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.922777891 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.922789097 CEST	4032	49700	79.110.62.187	192.168.2.3
Sep 24, 2022 10:05:35.922817945 CEST	49700	4032	192.168.2.3	79.110.62.187
Sep 24, 2022 10:05:35.922841072 CEST	4032	49700	79.110.62.187	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 24, 2022 10:05:34.848011971 CEST	58921	53	192.168.2.3	8.8.8.8
Sep 24, 2022 10:05:34.867635012 CEST	53	58921	8.8.8.8	192.168.2.3
Sep 24, 2022 10:05:48.781843901 CEST	49977	53	192.168.2.3	8.8.8.8
Sep 24, 2022 10:05:48.801285982 CEST	53	49977	8.8.8.8	192.168.2.3
Sep 24, 2022 10:06:04.869580984 CEST	57840	53	192.168.2.3	8.8.8.8
Sep 24, 2022 10:06:04.889889956 CEST	53	57840	8.8.8.8	192.168.2.3
Sep 24, 2022 10:06:16.652563095 CEST	57990	53	192.168.2.3	8.8.8.8
Sep 24, 2022 10:06:16.674304962 CEST	53	57990	8.8.8.8	192.168.2.3
Sep 24, 2022 10:06:28.701721907 CEST	52387	53	192.168.2.3	8.8.8.8
Sep 24, 2022 10:06:28.723304033 CEST	53	52387	8.8.8.8	192.168.2.3
Sep 24, 2022 10:06:38.351696968 CEST	56924	53	192.168.2.3	8.8.8.8
Sep 24, 2022 10:06:38.371471882 CEST	53	56924	8.8.8.8	192.168.2.3
Sep 24, 2022 10:06:45.221066952 CEST	60625	53	192.168.2.3	8.8.8.8
Sep 24, 2022 10:06:45.238692045 CEST	53	60625	8.8.8.8	192.168.2.3
Sep 24, 2022 10:06:51.599821091 CEST	49302	53	192.168.2.3	8.8.8.8
Sep 24, 2022 10:06:51.619574070 CEST	53	49302	8.8.8.8	192.168.2.3
Sep 24, 2022 10:06:58.926563025 CEST	53975	53	192.168.2.3	8.8.8.8
Sep 24, 2022 10:06:58.948337078 CEST	53	53975	8.8.8.8	192.168.2.3
Sep 24, 2022 10:07:05.830044031 CEST	51139	53	192.168.2.3	8.8.8.8
Sep 24, 2022 10:07:05.848072052 CEST	53	51139	8.8.8.8	192.168.2.3
Sep 24, 2022 10:07:29.964632034 CEST	52955	53	192.168.2.3	8.8.8.8
Sep 24, 2022 10:07:29.986562967 CEST	53	52955	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 24, 2022 10:05:34.848011971 CEST	192.168.2.3	8.8.8.8	0x90f9	Standard query (0)	jasonbourne.bounceme.net	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:05:48.781843901 CEST	192.168.2.3	8.8.8.8	0xe25e	Standard query (0)	jasonbourne.bounceme.net	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:04.869580984 CEST	192.168.2.3	8.8.8.8	0x475	Standard query (0)	jasonbourne.bounceme.net	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:16.652563095 CEST	192.168.2.3	8.8.8.8	0xcada	Standard query (0)	jasonbourne.bounceme.net	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:28.701721907 CEST	192.168.2.3	8.8.8.8	0xfa4b	Standard query (0)	jasonbourne.bounceme.net	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:38.351696968 CEST	192.168.2.3	8.8.8.8	0x7280	Standard query (0)	jasonbourne.bounceme.net	A (IP address)	IN (0x0001)	false

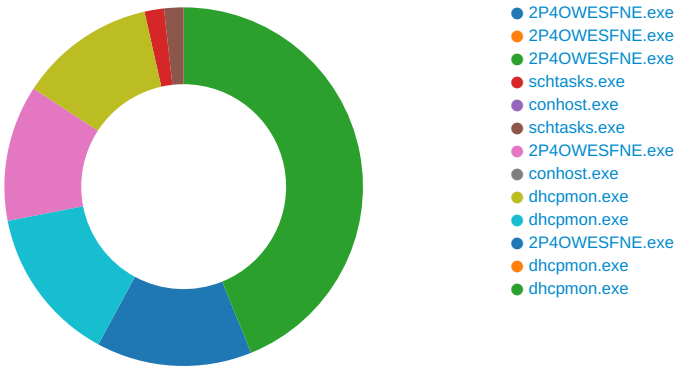
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 24, 2022 10:06:45.221066952 CEST	192.168.2.3	8.8.8.8	0xb3e8	Standard query (0)	jasonbourne.bounceme.net	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:51.599821091 CEST	192.168.2.3	8.8.8.8	0x2558	Standard query (0)	jasonbourne.bounceme.net	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:58.926563025 CEST	192.168.2.3	8.8.8.8	0x6094	Standard query (0)	jasonbourne.bounceme.net	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:07:05.830044031 CEST	192.168.2.3	8.8.8.8	0x283c	Standard query (0)	jasonbourne.bounceme.net	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:07:29.964632034 CEST	192.168.2.3	8.8.8.8	0xea36	Standard query (0)	jasonbourne.bounceme.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 24, 2022 10:05:34.867635012 CEST	8.8.8.8	192.168.2.3	0x90f9	No error (0)	jasonbourne.bounceme.net		79.110.62.187	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:05:48.801285982 CEST	8.8.8.8	192.168.2.3	0xe25e	No error (0)	jasonbourne.bounceme.net		79.110.62.187	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:04.889889956 CEST	8.8.8.8	192.168.2.3	0x475	No error (0)	jasonbourne.bounceme.net		79.110.62.187	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:16.674304962 CEST	8.8.8.8	192.168.2.3	0xcada	No error (0)	jasonbourne.bounceme.net		79.110.62.187	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:28.723304033 CEST	8.8.8.8	192.168.2.3	0xfa4b	No error (0)	jasonbourne.bounceme.net		79.110.62.187	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:38.371471882 CEST	8.8.8.8	192.168.2.3	0x7280	No error (0)	jasonbourne.bounceme.net		79.110.62.187	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:45.238692045 CEST	8.8.8.8	192.168.2.3	0xb3e8	No error (0)	jasonbourne.bounceme.net		79.110.62.187	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:51.619574070 CEST	8.8.8.8	192.168.2.3	0x2558	No error (0)	jasonbourne.bounceme.net		79.110.62.187	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:06:58.948337078 CEST	8.8.8.8	192.168.2.3	0x6094	No error (0)	jasonbourne.bounceme.net		79.110.62.187	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:07:05.848072052 CEST	8.8.8.8	192.168.2.3	0x283c	No error (0)	jasonbourne.bounceme.net		79.110.62.187	A (IP address)	IN (0x0001)	false
Sep 24, 2022 10:07:29.986562967 CEST	8.8.8.8	192.168.2.3	0xea36	No error (0)	jasonbourne.bounceme.net		79.110.62.187	A (IP address)	IN (0x0001)	false

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 2P4OWESFNE.exe PID: **612**, Parent PID: **6056**

General

Target ID:	0
Start time:	10:05:01
Start date:	24/09/2022
Path:	C:\Users\user\Desktop\2P4OWESFNE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\2P4OWESFNE.exe"
Imagebase:	0x20000
File size:	1000448 bytes
MD5 hash:	69956E7CC66B2E6B4A15DC779D63B459
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.317159998.0000000002568000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.323536613.0000000003951000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.323536613.0000000003951000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.323536613.0000000003951000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.323536613.0000000003951000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.320178874.0000000003555000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.320178874.0000000003555000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.320178874.0000000003555000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.320178874.0000000003555000.00000004.00000800.00020000.00000000.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	6D3BCF06	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	6D3BCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2P4OWESFNE.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6CC78D	CreateFileW

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\Microsoft\CLR_v4.0_32\UsageLogs\2P4OWESFNE.exe.log	0	1394	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	6D6CC907	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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C201B4F	ReadFile

Analysis Process: 2P4OWESFNE.exe PID: **6076**, Parent PID: **612**

General

Target ID:	10
Start time:	10:05:21
Start date:	24/09/2022
Path:	C:\Users\user\Desktop\2P4OWESFNE.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\2P4OWESFNE.exe
Imagebase:	0xb0000
File size:	1000448 bytes
MD5 hash:	69956E7CC66B2E6B4A15DC779D63B459
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Analysis Process: 2P4OWESFNE.exe PID: **4148**, Parent PID: **612**

General

Target ID:	11
Start time:	10:05:22
Start date:	24/09/2022
Path:	C:\Users\user\Desktop\2P4OWESFNE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\2P4OWESFNE.exe
Imagebase:	0x850000
File size:	1000448 bytes
MD5 hash:	69956E7CC66B2E6B4A15DC779D63B459
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: 0000000B.00000002.545805454.0000000002D81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.545805454.0000000002D81000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.311191616.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.311191616.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.311191616.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000000.311191616.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.582445955.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.582445955.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.582445955.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.582445955.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.582899602.0000000007350000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.582899602.0000000007350000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.582899602.0000000007350000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.582899602.0000000007350000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.581802158.0000000007180000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.581802158.0000000007180000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.581802158.0000000007180000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.581802158.0000000007180000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.582528929.0000000007320000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.582528929.0000000007320000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.582528929.0000000007320000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.582528929.0000000007320000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.583497422.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.583497422.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.583497422.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.583497422.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.577143081.00000000062F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.577143081.00000000062F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.577143081.00000000062F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.577143081.00000000062F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.582324415.0000000007300000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source:

0000000B.00000002.582324415.0000000007300000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.582324415.0000000007300000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.582324415.0000000007300000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.550686759.0000000002DED000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.550686759.0000000002DED000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.567018160.00000000048B7000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.567018160.00000000048B7000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.566126701.0000000004842000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.566126701.0000000004842000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.566126701.0000000004842000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.562954773.0000000004671000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.562954773.0000000004671000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.562954773.0000000004671000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.582073536.00000000072E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.582073536.00000000072E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.582073536.00000000072E0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.582073536.00000000072E0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.582795269.0000000007340000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.582795269.0000000007340000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.582795269.0000000007340000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.582795269.0000000007340000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.577485717.0000000006390000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.577485717.0000000006390000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.577485717.0000000006390000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.577485717.0000000006390000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.577485717.0000000006390000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.568370273.00000000049A2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.568370273.00000000049A2000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.568370273.00000000049A2000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.578555669.0000000006760000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.578555669.0000000006760000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.578555669.0000000006760000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.578555669.0000000006760000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.582233122.00000000072F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.582233122.00000000072F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.582233122.00000000072F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.582233122.00000000072F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.581897432.0000000007190000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.581897432.0000000007190000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.581897432.0000000007190000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.581897432.0000000007190000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000003.348304401.00000000068C1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.581164411.0000000006EC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.581164411.0000000006EC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000B.00000002.581164411.0000000006EC0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.581164411.0000000006EC0000.00000004.08000000.00040000.00000000.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	6D3BCF06	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	6D3BCF06	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	6C20BEFF	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	6C201E60	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	6C20BEFF	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	6C20DD66	CopyFileW
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	6C20DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD28D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	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	6C201E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpDA9C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	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	6C20BEFF	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	6C20BEFF	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	8	6C201E60	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	6C201E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C201E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C20DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD28D.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpDA9C.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\Desktop\2P4OWESFNE.exe:Zone.Identifier	success or wait	1	6C182935	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	success or wait	1	6C206A95	DeleteFileW

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	fd 36 50 fd 4e fd fd 48	6PNH	success or wait	1	6C201B4F	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 fd 67 fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0e 00 00 4a 00 00 00 00 00 00 fd 17 0f 00 00 20 00 00 00 20 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 fd 0f 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.$PELg0J @ @	success or wait	4	6C20DD66	CopyFileW
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	6C20DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD28D.tmp	0	1300	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	6C201B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	37	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 32 50 34 4f 57 45 53 46 4e 45 2e 65 78 65	C:\Users\user\Desktop\2P4OWESFNE.exe	success or wait	1	6C201B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpDA9C.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	6C201B4F	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	10	6C201B4F	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	6C201B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	24	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd	9iH}Z4f~a	success or wait	2	6C201B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	0	24	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d fd 4a 22 fd 43 3b 22 61	9iH}Z4fJ"C;"a	success or wait	1	6C20DD66	CopyFileW

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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C201B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D37D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D37D72F	unknown
C:\Users\user\Desktop\2P4OWESFNE.exe	unknown	4096	success or wait	1	6D37D72F	unknown
C:\Users\user\Desktop\2P4OWESFNE.exe	unknown	512	success or wait	1	6D37D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6D37D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6D37D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6D37D72F	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	6C20646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **812**, Parent PID: **4148**

General

Target ID:	12
Start time:	10:05:28
Start date:	24/09/2022
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\tmpD28D.tmp
Imagebase:	0x11c0000
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\tmpD28D.tmp	unknown	2	success or wait	1	11CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD28D.tmp	unknown	1301	success or wait	1	11CABD9	ReadFile

Analysis Process: conhost.exe PID: **5680**, Parent PID: **812**

General

Target ID:	13
Start time:	10:05:29
Start date:	24/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000

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: **2108**, Parent PID: **4148**

General

Target ID:	14
Start time:	10:05:30
Start date:	24/09/2022
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\tmpDA9C.tmp
Imagebase:	0x11c0000
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\tmpDA9C.tmp	unknown	2	success or wait	1	11CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpDA9C.tmp	unknown	1311	success or wait	1	11CABD9	ReadFile

Analysis Process: 2P4OWESFNE.exe PID: **6132**, Parent PID: **1080**

General

Target ID:	15
Start time:	10:05:30
Start date:	24/09/2022
Path:	C:\Users\user\Desktop\2P4OWESFNE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\2P4OWESFNE.exe 0
Imagebase:	0xbe0000
File size:	1000448 bytes
MD5 hash:	69956E7CC66B2E6B4A15DC779D63B459
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000F.00000002.398922786.00000000032D8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6D3BCF06	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	6D3BCF06	unknown

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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C201B4F	ReadFile

Analysis Process: conhost.exe PID: **848**, Parent PID: **2108**

General

Target ID:	16
Start time:	10:05:31
Start date:	24/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **2328**, Parent PID: **1080**

General

Target ID:	17
Start time:	10:05:33
Start date:	24/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xc50000

File size:	1000448 bytes
MD5 hash:	69956E7CC66B2E6B4A15DC779D63B459
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000011.00000002.407355851.0000000003078000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	6D3BCF06	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	6D3BCF06	unknown

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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C201B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **3788**, Parent PID: **3452**

General

Target ID:	18
Start time:	10:05:40
Start date:	24/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x9a0000
File size:	1000448 bytes
MD5 hash:	69956E7CC66B2E6B4A15DC779D63B459
Has elevated privileges:	false
Has administrator privileges:	false
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	6D3BCF06	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	6D3BCF06	unknown
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	6D6CC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	1394	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	6D6CC907	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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C201B4F	ReadFile

Analysis Process: 2P4OWESFNE.exe PID: **612**, Parent PID: **6132**

General	
Target ID:	19
Start time:	10:05:51
Start date:	24/09/2022
Path:	C:\Users\user\Desktop\2P4OWESFNE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\2P4OWESFNE.exe
Imagebase:	0x8d0000
File size:	1000448 bytes
MD5 hash:	69956E7CC66B2E6B4A15DC779D63B459
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: 00000013.00000002.439587910.0000000002CE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.439587910.0000000002CE1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.439587910.0000000002CE1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.442755164.0000000003CE9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.442755164.0000000003CE9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.442755164.0000000003CE9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: dhcpmon.exe PID: **4300**, Parent PID: **2328**

General	
Target ID:	20
Start time:	10:06:00
Start date:	24/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x550000
File size:	1000448 bytes
MD5 hash:	69956E7CC66B2E6B4A15DC779D63B459
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: 00000014.00000002.454333239.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.454333239.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000014.00000002.454333239.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: dhcpmon.exe PID: **4648**, Parent PID: **3788**

General	
Target ID:	21
Start time:	10:06:07
Start date:	24/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x750000
File size:	1000448 bytes

MD5 hash:	69956E7CC66B2E6B4A15DC779D63B459
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Disassembly

No disassembly