ID: 624809
Sample Name: Bank Details.exe
Cookbook: default.jbs
Time: 04:17:07
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

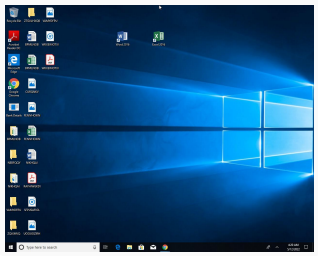
Windows Analysis Report

Bank Details.exe

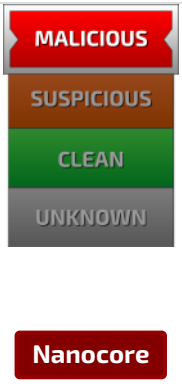
Overview

General Information

Sample Name:	Bank Details.exe
Analysis ID:	624809
MD5:	e62e3496deb3ee.
SHA1:	2b7942225b4d43.
SHA256:	a9ee1fbee3b6bd..
Tags:	exe NanoCore RAT
Infos:	



Detection



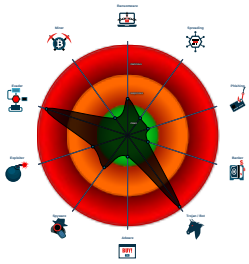
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- Bank Details.exe (PID: 1900 cmdline: "C:\Users\user\Desktop\Bank Details.exe" MD5: E62E3496DEB3EE2C512CA61CF2642A0D)
  - powershell.exe (PID: 580 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4192 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nOcstjdWFAT" /XML "C:\Users\user\AppData\Local\Temp\tmpEA4C.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Bank Details.exe (PID: 3560 cmdline: C:\Users\user\Desktop\Bank Details.exe MD5: E62E3496DEB3EE2C512CA61CF2642A0D)
- dhcpmon.exe (PID: 6400 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: E62E3496DEB3EE2C512CA61CF2642A0D)
  - powershell.exe (PID: 6572 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6580 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6588 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nOcstjdWFAT" /XML "C:\Users\user\AppData\Local\Temp\tmp5C9D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6784 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: E62E3496DEB3EE2C512CA61CF2642A0D)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "55e3c1f3-bf1e-4980-afea-8df9e139",
  "Group": "Default",
  "Domain1": "chima2022.ddns.net",
  "Domain2": "",
  "Port": 2022,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "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"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.501615739.00000000050E0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000008.00000002.501615739.00000000050E0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000008.00000002.501615739.00000000050E0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
00000008.00000002.495963136.0000000000E40000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost
00000008.00000002.495963136.0000000000E40000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost

Click to see the 107 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.Bank Details.exe.e50000.9.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1deb:$x1: NanoCore.ClientPluginHost • 0x1e24:$x2: IClientNetworkHost
8.2.Bank Details.exe.e50000.9.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1deb:$x2: NanoCore.ClientPluginHost • 0x1f36:$s4: PipeCreated • 0x1e05:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
8.2.Bank Details.exe.e50000.9.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x1e8b:$x2: NanoCore.ClientPlugin • 0x1deb:$x3: NanoCore.ClientPluginHost • 0x1ea1:$i3: IClientNetwork • 0x1e43:$i5: IClientDataHost • 0x1e05:$i6: IClientLoggingHost • 0x1e24:$i7: IClientNetworkHost • 0x266c:$i9: IClientNameObjectCollection • 0x1b41:$s1: ClientPlugin • 0x1e94:$s1: ClientPlugin • 0x2a80:$s2: EndPoint • 0x2771:$s3: IPAddress • 0x2083:$s4: IPEndPoint • 0x27a3:$s7: get_Connected
8.2.Bank Details.exe.ae0000.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
8.2.Bank Details.exe.ae0000.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
Click to see the 321 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116 −

Timestamp:	192.168.2.4194.31.98.1164983020222816766 05/12/22-04:19:36.011525
SID:	2816766
Source Port:	49830
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116 −

Timestamp:	192.168.2.4194.31.98.1164977320222816766 05/12/22-04:19:20.018597
SID:	2816766
Source Port:	49773
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116 −

Timestamp:	192.168.2.4194.31.98.1164986320222816766 05/12/22-04:20:10.853853
SID:	2816766

Source Port:	49863
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.31.98.116 - Destination IP: 192.168.2.4	
Timestamp:	194.31.98.116192.168.2.42022497582841753 05/12/22-04:18:37.050338
SID:	2841753
Source Port:	2022
Destination Port:	49758
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164983320222816766 05/12/22-04:19:42.105532
SID:	2816766
Source Port:	49833
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164977120222025019 05/12/22-04:19:11.899573
SID:	2025019
Source Port:	49771
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.31.98.116 - Destination IP: 192.168.2.4	
Timestamp:	194.31.98.116192.168.2.42022497972841753 05/12/22-04:19:25.210300
SID:	2841753
Source Port:	2022
Destination Port:	49797
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164976920222025019 05/12/22-04:18:58.075804
SID:	2025019
Source Port:	49769
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164976920222816766 05/12/22-04:19:00.725683
SID:	2816766
Source Port:	49769
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164983320222025019 05/12/22-04:19:41.132097
SID:	2025019
Source Port:	49833
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.31.98.116 - Destination IP: 192.168.2.4	
Timestamp:	194.31.98.116192.168.2.42022498332841753 05/12/22-04:19:46.171498
SID:	2841753
Source Port:	2022
Destination Port:	49833
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164986320222025019 05/12/22-04:20:10.583511
SID:	2025019
Source Port:	49863
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164977320222816718 05/12/22-04:19:19.399645
SID:	2816718
Source Port:	49773
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164977320222025019 05/12/22-04:19:18.977182
SID:	2025019
Source Port:	49773
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164983020222025019 05/12/22-04:19:35.133701
SID:	2025019
Source Port:	49830
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164975820222816766 05/12/22-04:18:37.020536
SID:	2816766
Source Port:	49758
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164976120222816766 05/12/22-04:18:44.803258
SID:	2816766
Source Port:	49761
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164977120222816766 05/12/22-04:19:12.897247
SID:	2816766
Source Port:	49771

Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 3 - Source IP: 194.31.98.116 - Destination IP: 192.168.2.4	
Timestamp:	194.31.98.116192.168.2.42022498632810451 05/12/22-04:20:20.632430
SID:	2810451
Source Port:	2022
Destination Port:	49863
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.31.98.116 - Destination IP: 192.168.2.4	
Timestamp:	194.31.98.116192.168.2.42022498632841753 05/12/22-04:20:20.632430
SID:	2841753
Source Port:	2022
Destination Port:	49863
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164983420222025019 05/12/22-04:19:47.368674
SID:	2025019
Source Port:	49834
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.31.98.116 - Destination IP: 192.168.2.4	
Timestamp:	194.31.98.116192.168.2.42022498162841753 05/12/22-04:19:30.172998
SID:	2841753
Source Port:	2022
Destination Port:	49816
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164985920222816766 05/12/22-04:20:05.810359
SID:	2816766
Source Port:	49859
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164985420222025019 05/12/22-04:19:56.611527
SID:	2025019
Source Port:	49854
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164979720222025019 05/12/22-04:19:25.160988
SID:	2025019
Source Port:	49797
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 194.31.98.116 - Destination IP: 192.168.2.4	
Timestamp:	194.31.98.116192.168.2.42022498592810290 05/12/22-04:20:04.821759
SID:	2810290
Source Port:	2022
Destination Port:	49859
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164976120222025019 05/12/22-04:18:43.016236
SID:	2025019
Source Port:	49761
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164976420222025019 05/12/22-04:18:49.975269
SID:	2025019
Source Port:	49764
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164977020222816766 05/12/22-04:19:06.711904
SID:	2816766
Source Port:	49770
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164975820222025019 05/12/22-04:18:36.685534
SID:	2025019
Source Port:	49758
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164983420222816766 05/12/22-04:19:48.215646
SID:	2816766
Source Port:	49834
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164981620222025019 05/12/22-04:19:30.131962
SID:	2025019
Source Port:	49816
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	
Timestamp:	192.168.2.4194.31.98.1164985920222025019 05/12/22-04:20:03.455105
SID:	2025019
Source Port:	49859

Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	−
Timestamp:	192.168.2.4194.31.98.1164977020222025019 05/12/22-04:19:05.824499
SID:	2025019
Source Port:	49770
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.31.98.116 - Destination IP: 192.168.2.4	−
Timestamp:	194.31.98.116192.168.2.42022497642841753 05/12/22-04:18:50.082261
SID:	2841753
Source Port:	2022
Destination Port:	49764
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 194.31.98.116	−
Timestamp:	192.168.2.4194.31.98.1164985420222816766 05/12/22-04:19:58.208455
SID:	2816766
Source Port:	49854
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for dropped file
- Yara detected Nanocore RAT
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- Snort IDS alert for network traffic
- Yara detected Generic Downloader
- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud

- Yara detected Nanocore RAT

System Summary

- Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

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

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

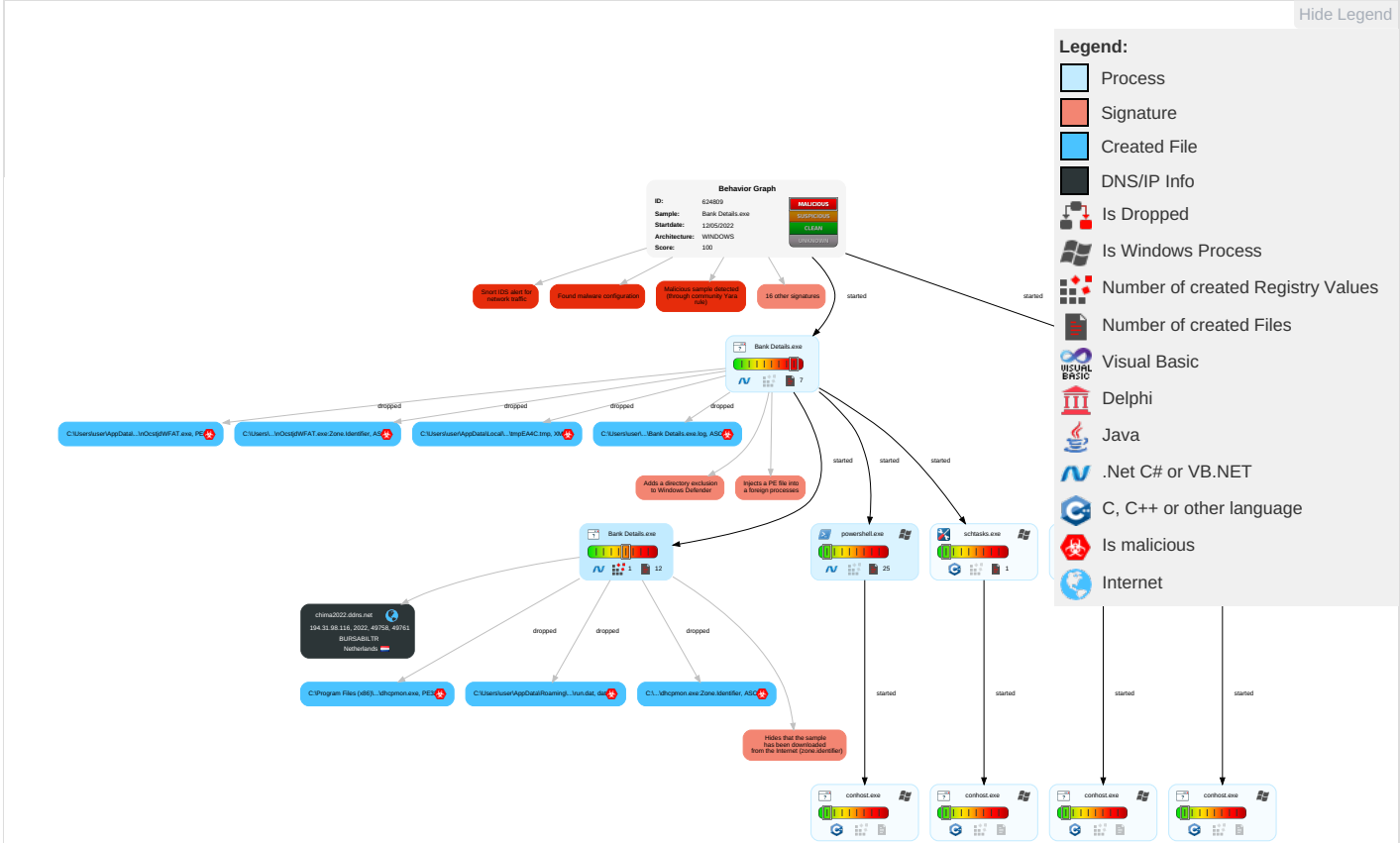
Yara detected Nanocore RAT

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	1 1 Input Capture	1 Query Registry	Remote Services	1 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 1 Disable or Modify Tools	LSASS Memory	2 2 1 Security Software 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 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	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 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	1 2 System Information Discovery	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	2 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

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
Bank Details.exe	12%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
Bank Details.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	12%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe	12%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
27.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.Bank Details.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.Bank Details.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.Bank Details.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.Bank Details.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.Bank Details.exe.52e0000.34.unpack	100%	Avira	TR/NanoCore.fadte		Download File
27.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.Bank Details.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.Bank Details.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fonts.comcxe	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
chima2022.ddns.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.com(V~	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html;	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chima2022.ddns.net	194.31.98.116	true	false		high

Contacted URLs

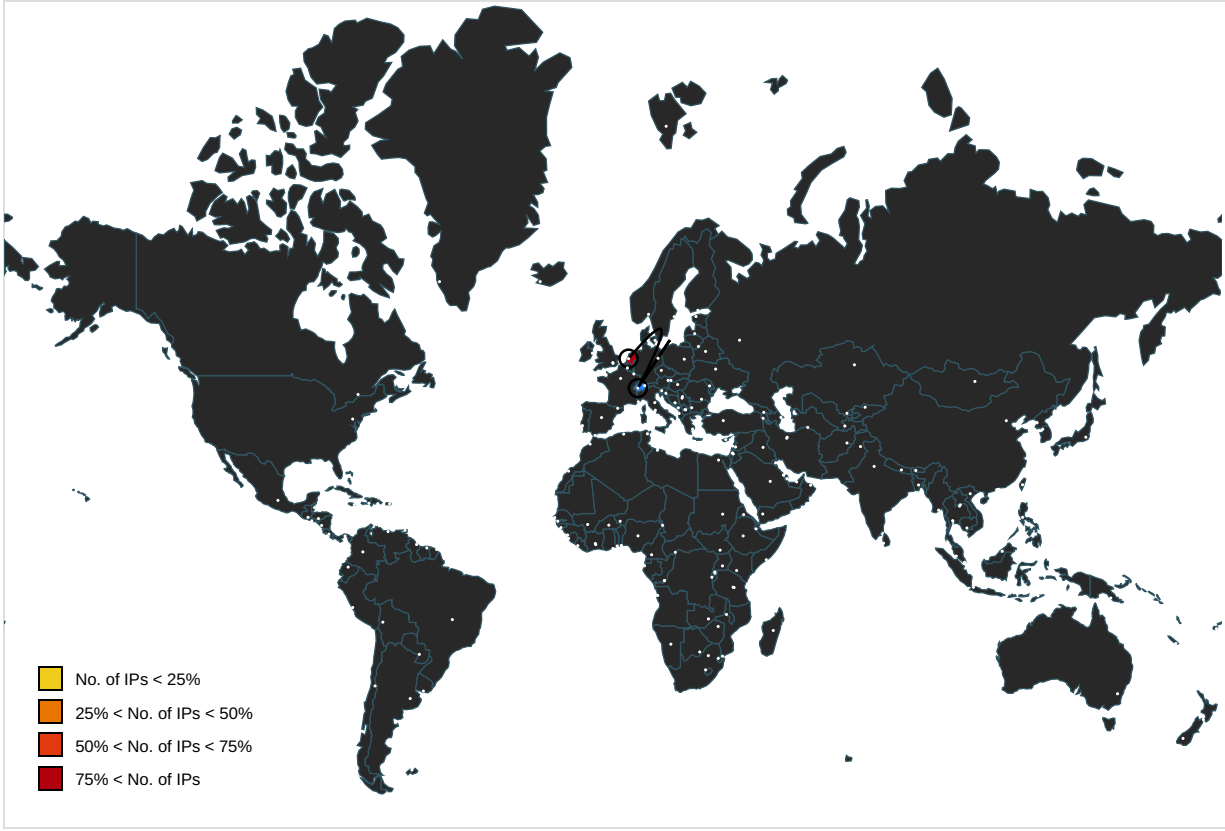
Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
chima2022.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Bank Details.exe, 00000000.00000002.2847 73874.0000000006632000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Bank Details.exe, 00000000.00000002.2847 73874.0000000006632000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Bank Details.exe, 00000000.00000002.2847 73874.0000000006632000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	Bank Details.exe, 00000000.00000003.2398 77331.00000000053E8000.00000004.00000800 .00020000.00000000.sdmp, Bank Details.exe, 00000000.00000003.239900469.000000000 53E8000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Bank Details.exe, 00000000.00000002.2847 73874.0000000006632000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Bank Details.exe, 00000000.00000002.2847 73874.0000000006632000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comcxe	Bank Details.exe, 00000000.00000003.2293 38584.00000000053BB000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Bank Details.exe, 00000000.00000002.2847 73874.0000000006632000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.tiro.com	Bank Details.exe, 00000000.00000002.2847 73874.0000000006632000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Bank Details.exe, 00000000.00000002.2847 73874.0000000006632000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Bank Details.exe, 00000000.00000002.2847 73874.0000000006632000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	Bank Details.exe, 00000008.00000002.4959 63136.0000000000E40000.00000004.08000000 .00040000.00000000.sdmp, Bank Details.exe, 00000008.00000002.499495990.000000000 45ED000.00000004.00000800.00020000.00000 000.sdmp, Bank Details.exe, 00000008.000 00002.500271666.00000000047BE000.0000000 4.00000800.00020000.00000000.sdmp, Bank Details.exe, 00000008.00000002.501096037 .0000000004834000.00000004.00000800.0002 0000.00000000.sdmp, Bank Details.exe, 00 000008.00000002.503251204.0000000006D210 00.00000004.00000800.00020000.00000000.sdmp, Bank Details.exe, 00000008.00000002.496960213 .000000000296C000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://www.fontbureau.com(V~	Bank Details.exe, 00000000.00000002.2844 49354.00000000053A0000.00000004.00000800 .00020000.00000000.sdmp, Bank Details.exe, 00000000.00000003.279101275.000000000 53A0000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	Bank Details.exe, 00000000.00000002.2847 73874.0000000006632000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Bank Details.exe, 00000000.00000002.2847 73874.0000000006632000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp, Bank Details.exe, 00000000.00000003.239968119.00000000053B8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html;	Bank Details.exe, 00000000.00000003.233452339.00000000053B9000.00000004.00000800.00020000.00000000.sdmp, Bank Details.exe, 00000000.00000003.233385137.00000000053B8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	Bank Details.exe, 00000000.00000003.229367383.00000000053DE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Bank Details.exe, 00000000.00000002.280585839.00000000024B1000.00000004.00000800.00020000.00000000.sdmp, Bank Details.exe, 00000000.00000002.280695946.0000000002545000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000014.00000002.343046224.0000000002F43000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000014.00000002.342911345.0000000002EB1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Bank Details.exe, 00000000.00000002.284773874.0000000006632000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.31.98.116	chima2022.ddns.net	Netherlands		60721	BURSABILTR	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	624809
Start date and time: 12/05/202204:17:07	2022-05-12 04:17:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bank Details.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	37
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@18/19@15/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 63.7% • Quality standard deviation: 36.1%

HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.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.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:18:16	API Interceptor	814x Sleep call for process: Bank Details.exe modified
04:18:26	API Interceptor	80x Sleep call for process: powershell.exe modified
04:18:34	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
04:18:46	API Interceptor	1x 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\Bank Details.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	573440
Entropy (8bit):	7.798214289782311
Encrypted:	false
SSDEEP:	12288:M4GvSfRMVmvlcY3bUP01EZ46IeXuLJxK1AXmq0sSNIiEq402Kbe:M78N3/EZ46I7JxK+qjU0n
MD5:	E62E3496DEB3EE2C512CA61CF2642A0D
SHA1:	2B7942225B4D43EC944622E2B80D0D18C5376F70
SHA-256:	A9EE1FBEE3B6BD1C9C449774B8ED2F02FB89BDE7CBF72B2E348C61240971238E
SHA-512:	E133E01095011D17DE5373B2FE486F49CA0F75B26FD23BC246F3AA94D8C2A8F7925835124EC1104D038EEBB24ACE9941F27A05886079F1892C88E78333E4B7CA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 12%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...4c|b.....0..`...@.....s... .....@.. ... ..... ..... ..@.....s..O.....\r..... ..... ..H.....text....S... ...`... ....`.rsrc..... .....@..@.reloc..... ... .@..B..... .....

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

Process:	C:\Users\user\Desktop\Bank Details.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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Users\user\Desktop\Bank Details.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE8:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHJ
MD5:	EA78C102145ED608EF0E407B978AF339
SHA1:	66C9179ED9675B9271A97AB1FC878077E09AB731
SHA-256:	8BF01E0C445BD07C0B4EDC7199B7E17DAF1CA55CA52D4A6EAC4EF211C2B1A73E
SHA-512:	8C04139A1FC3C3BDACB680EC443615A43EB18E73B5A0CFCA644CB4A5E71746B275B3E238DD1A5A205405313E457BB75F9BBB93277C67AFA5D78DCFA30E5DA02B
Malicious:	**true**
Reputation:	unknown
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,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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

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

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE8:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHJ
MD5:	EA78C102145ED608EF0E407B978AF339
SHA1:	66C9179ED9675B9271A97AB1FC878077E09AB731
SHA-256:	8BF01E0C445BD07C0B4EDC7199B7E17DAF1CA55CA52D4A6EAC4EF211C2B1A73E
SHA-512:	8C04139A1FC3C3BDACB680EC443615A43EB18E73B5A0CFCA644CB4A5E71746B275B3E238DD1A5A205405313E457BB75F9BBB93277C67AFA5D78DCFA30E5DA02B
Malicious:	false
Reputation:	unknown
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,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22280
Entropy (8bit):	5.602104023194985
Encrypted:	false
SSDEEP:	384:gtCDLq0Ra1MzD68TQBG0lRcS0n4jultIaPpaeQ99gbpbcxyT1MaDZlbAV75slqhP:SWD6wJrT4Clt1Bat8hZC6fw2tVY
MD5:	C7C33EB8763FDC52CC134C147FC22367
SHA1:	F09E2F251F926894F6821FC334D71DE7407D6348
SHA-256:	94C72D6CD39BE72210B304CC182819D44B9EBBBAA3F2F3ADCCC0F222BB3DCC44
SHA-512:	6FF98BB2BC846B0C1EE91DE810E78902C8B3B58F21BDA52285853A597E3964F9C0D87DAFF3BEB872C44E65A6796EC0C44E4D9291BA3D6CC598E749F6FB7E6EBF
Malicious:	false
Reputation:	unknown
Preview:	@...e.....y.....Z.:.1.1...S.u...r.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0jupmy4m.iym.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3bgoyhja.ke3.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)

Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_c54pb3wi.g5d.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_havwfre0.tqn.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp5C9D.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.136648748218081
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaDb+xvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTpv
MD5:	67036E15EF31876136F320B5FCECE52C
SHA1:	D301B3A0B0FDA38115B2A028A3B0F0518E549775
SHA-256:	124C5059D2D3FAB1B1E4C49E41CB1820217495F98074A6E563513512F15A8908

SHA-512:	A03F8FEFF1A19135B78F4612106A6B044552EDF5784E78D3B2C6485CBB2D0F328417C1BB349F35FA327C69981AC99681E0CF840DB49D9A9E1A2B28F779A5B7A
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmpEA4C.tmp

Process:	C:\Users\user\Desktop\Bank Details.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.136648748218081
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaDb+xvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTpv
MD5:	67036E15EF31876136F320B5FCECE52C
SHA1:	D301B3A0B0FDA38115B2A028A3B0F0518E549775
SHA-256:	124C5059D2D3FAB1B1E4C49E41CB1820217495F98074A6E563513512F15A8908
SHA-512:	A03F8FEFF1A19135B78F4612106A6B044552EDF5784E78D3B2C6485CBB2D0F328417C1BB349F35FA327C69981AC99681E0CF840DB49D9A9E1A2B28F779A5B7A
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

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

Process:	C:\Users\user\Desktop\Bank Details.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
Reputation:	unknown
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\Bank Details.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:ZN:/
MD5:	A8DD010F1502D96AF41BB635E99D3521
SHA1:	067B3897AEEB9F203CF93C9F67D5B953091796F0
SHA-256:	B23B0F8F7174FFDDF023626CBC2F110A2A75FFD41FF30502C0FA9F1C44A0424E
SHA-512:	C562AD89951160151F6D2E97A4FF9A3B4976F5CC1455DB7C553EF32BF2CD951D9428FF649E8F962148F49E5B5CCFCB8A3B11187FD09379AD170A7BD4D7F9C1C
Malicious:	**true**

Reputation:	unknown
Preview:	.`...3.H

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

Process:	C:\Users\user\Desktop\Bank Details.exe
File Type:	data
Category:	modified
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
Reputation:	unknown
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\Bank Details.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
Reputation:	unknown
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\nOcstjdWFAT.exe

Process:	C:\Users\user\Desktop\Bank Details.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	573440
Entropy (8bit):	7.798214289782311
Encrypted:	false
SSDEEP:	12288:M4GvSfRMVmvIcY3bUP01EZ46IeXuLJxK1AXmq0sSNIiEq402Kbe:M78N3/EZ46I7JxK+qjU0n
MD5:	E62E3496DEB3EE2C512CA61CF2642A0D
SHA1:	2B7942225B4D43EC944622E2B80D0D18C5376F70
SHA-256:	A9EE1FBEE3B6BD1C9C449774B8ED2F02FB89BDE7CBF72B2E348C61240971238E
SHA-512:	E133E01095011D17DE5373B2FE486F49CA0F75B26FD23BC246F3AA94D8C2A8F7925835124EC1104D038EEBB24ACE9941F27A05886079F1892C88E78333E4B7CA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 12%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...4c|b.....0..`...@.....s... .....@.. ... ..... ..... ..@.....s..O.....\r..... ..... ..H.....text...S... ...`... ....`.rsrc..... .....@..@.reloc..... ... .@..B..... .....

C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Bank Details.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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220512\PowerShell_transcript.124406.56i4y25Q.20220512041851.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5793
Entropy (8bit):	5.388896054676983
Encrypted:	false
SSDEEP:	96:BZ8jFNzqDo1ZDZUtjFNzqDo1Z/0GsjZzjFNzqDo1ZzV88KZ6:1m
MD5:	8228C39283F5BEFF7E37C8691849664F
SHA1:	B877538AEA027D05F3977764068EB6F9A94AB773
SHA-256:	87F73FDE539243A5C4369A11335E28624DE59136044BBFB1B0F6BE80AA1890C9
SHA-512:	47EFC4ECE3D2B0086159502948DD93036B9C821DBADFEEDEFE5C412B69C71352962516EB8EB8BFF511F2516E45F29C33AA73759C48682316FFD6880822899648
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220512041852..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe..Process ID: 6572..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220512041852..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe..**********..Windows PowerShell transcript start..Start time: 20220512042240..Username: computer\user..RunAs User: computer\jo

C:\Users\user\Documents\20220512\PowerShell_transcript.124406.b92XxzZg.20220512041824.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5790
Entropy (8bit):	5.386889511878751
Encrypted:	false
SSDEEP:	96:BZtjFN8qDo1ZWZcjFN8qDo1Zw0GsjZ6gjFN8qDo1ZwKV88QZv:0CF
MD5:	CA470292FE80BFA3FC81C85E7969D89D
SHA1:	9D3662B9D81069FA5CD9F4841BECFDECB5667C2D
SHA-256:	0F1CB65C83C1FC586F111BFB3FBD0229FDBC8400270CCE23D8F8D44E52EC6923
SHA-512:	304F9F95375EAA817C412421098D216641E634DBE986A26B381B757219555B26580E83B494C1757F90CED499750663F39DF6D2441AB23B91652F75B5F4B8F6DA
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220512041826..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe..Process ID: 580..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220512041826..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe..**********..Windows PowerShell transcript start..Start time: 20220512042149..Username: computer\user..RunAs User: computer\jon

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.798214289782311
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Bank Details.exe
File size:	573440
MD5:	e62e3496deb3ee2c512ca61cf2642a0d
SHA1:	2b7942225b4d43ec944622e2b80d0d18c5376f70
SHA256:	a9ee1fbee3b6bd1c9c449774b8ed2f02fb89bde7cbf72b2e348c61240971238e
SHA512:	e133e01095011d17de5373b2fe486f49ca0f75b26fd23bc246f3aa94d8c2a8f7925835124ec1104d038eebb24ace9941f27a05886079f1892c88e78333e4b7ca
SSDEEP:	12288:M4GvSfRMVmvlcY3bUP01EZ46IeXuLJxK1AXmq0sSNIiEq402Kbe:M78N3/EZ46I7JxK+qjU0n
TLSH:	C1C4225407A52736E86C0BB5EE8229CD17B5AD835D25EB0FCCE4F1C949B874A42E132F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...4c|b.....0..`...@.....s... .....@.. ... .@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4873e6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627C6334 [Thu May 12 01:30:28 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x87394	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x88000	0x5f4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x8725c	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	0x853ec	0x86000	False	0.952762432952	data	7.94302903264	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x88000	0x5f4	0x2000	False	0.084716796875	data	1.0972336531	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0xc	0x2000	False	0.0050048828125	data	0.00881485270734	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x88090	0x364	data		
RT_MANIFEST	0x88404	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013
Assembly Version	0.0.1.0
InternalName	CreateValueCallb.exe
FileVersion	0.0.1.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	PagedOptionsDialog
ProductVersion	0.0.1.0
FileDescription	PagedOptionsDialog
OriginalFilename	CreateValueCallb.exe

Network Behavior

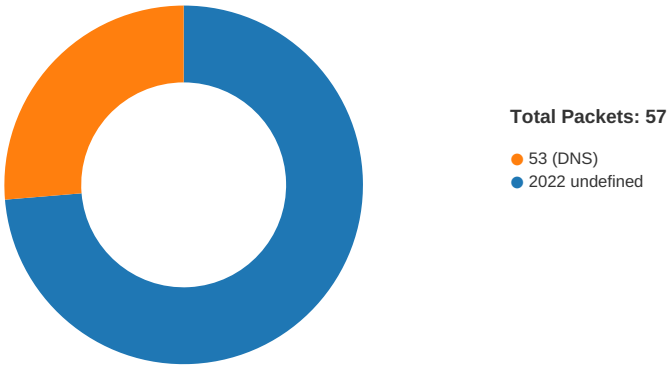
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4194.31.98.1164983020222816766 05/12/22-04:19:36.011525	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49830	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.1164977320222816766 05/12/22-04:19:20.018597	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49773	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.1164986320222816766 05/12/22-04:20:10.853853	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49863	2022	192.168.2.4	194.31.98.116
194.31.98.116192.168.2.42022497582841753 05/12/22-04:18:37.050338	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	2022	49758	194.31.98.116	192.168.2.4
192.168.2.4194.31.98.1164983320222816766 05/12/22-04:19:42.105532	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49833	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.1164977120222025019 05/12/22-04:19:11.899573	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	2022	192.168.2.4	194.31.98.116
194.31.98.116192.168.2.42022497972841753 05/12/22-04:19:25.210300	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	2022	49797	194.31.98.116	192.168.2.4
192.168.2.4194.31.98.1164976920222025019 05/12/22-04:18:58.075804	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.1164976920222816766 05/12/22-04:19:00.725683	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49769	2022	192.168.2.4	194.31.98.116

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4194.31.98.116 4983320222025019 05/12/22-04:19:41.132097	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49833	2022	192.168.2.4	194.31.98.116
194.31.98.116192.168.2.4 2022498332841753 05/12/22-04:19:46.171498	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	2022	49833	194.31.98.116	192.168.2.4
192.168.2.4194.31.98.116 4986320222025019 05/12/22-04:20:10.583511	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49863	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4977320222816718 05/12/22-04:19:19.399645	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49773	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4977320222025019 05/12/22-04:19:18.977182	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4983020222025019 05/12/22-04:19:35.133701	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49830	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4975820222816766 05/12/22-04:18:37.020536	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49758	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4976120222816766 05/12/22-04:18:44.803258	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49761	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4977120222816766 05/12/22-04:19:12.897247	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49771	2022	192.168.2.4	194.31.98.116
194.31.98.116192.168.2.4 2022498632810451 05/12/22-04:20:20.632430	TCP	2810451	ETPRO TROJAN NanoCore RAT Keepalive Response 3	2022	49863	194.31.98.116	192.168.2.4
194.31.98.116192.168.2.4 2022498632841753 05/12/22-04:20:20.632430	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	2022	49863	194.31.98.116	192.168.2.4
192.168.2.4194.31.98.116 4983420222025019 05/12/22-04:19:47.368674	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49834	2022	192.168.2.4	194.31.98.116
194.31.98.116192.168.2.4 2022498162841753 05/12/22-04:19:30.172998	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	2022	49816	194.31.98.116	192.168.2.4
192.168.2.4194.31.98.116 4985920222816766 05/12/22-04:20:05.810359	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49859	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4985420222025019 05/12/22-04:19:56.611527	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49854	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4979720222025019 05/12/22-04:19:25.160988	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49797	2022	192.168.2.4	194.31.98.116
194.31.98.116192.168.2.4 2022498592810290 05/12/22-04:20:04.821759	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	2022	49859	194.31.98.116	192.168.2.4
192.168.2.4194.31.98.116 4976120222025019 05/12/22-04:18:43.016236	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4976420222025019 05/12/22-04:18:49.975269	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	2022	192.168.2.4	194.31.98.116

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4194.31.98.116 4977020222816766 05/12/22- 04:19:06.711904	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49770	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4975820222025019 05/12/22- 04:18:36.685534	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4983420222816766 05/12/22- 04:19:48.215646	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49834	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4981620222025019 05/12/22- 04:19:30.131962	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4985920222025019 05/12/22- 04:20:03.455105	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49859	2022	192.168.2.4	194.31.98.116
192.168.2.4194.31.98.116 4977020222025019 05/12/22- 04:19:05.824499	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	2022	192.168.2.4	194.31.98.116
194.31.98.116192.168.2.4 2022497642841753 05/12/22- 04:18:50.082261	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	2022	49764	194.31.98.116	192.168.2.4
192.168.2.4194.31.98.116 4985420222816766 05/12/22- 04:19:58.208455	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49854	2022	192.168.2.4	194.31.98.116

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 04:18:36.577502012 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:36.608098030 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:36.608289957 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:36.685534000 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:36.742813110 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:36.758797884 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.020535946 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.050338030 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.050493002 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.109476089 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.109595060 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.383436918 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.535440922 CEST	2022	49758	194.31.98.116	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 04:18:37.583087921 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.615088940 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.615145922 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.615257025 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.646132946 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.646193027 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.646265984 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.646342039 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.677642107 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.677719116 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.677763939 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.677794933 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.677799940 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.677898884 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.709156036 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.709216118 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.709269047 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.709270954 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.709327936 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.709386110 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.709393024 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.709465027 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.741178989 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.741233110 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.741287947 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.741341114 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.741359949 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.741394997 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.741399050 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.741447926 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.741612911 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.773022890 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.773081064 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.773134947 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.773190022 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.773219109 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.773242950 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.773256063 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.773300886 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.773363113 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.804007053 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.804075956 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.804135084 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.804187059 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.804240942 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.804292917 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.804326057 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.804347038 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.804399014 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.804405928 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.835463047 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.835540056 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.835596085 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.835597038 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.835654974 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.835658073 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.835709095 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.835762978 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.835814953 CEST	2022	49758	194.31.98.116	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 04:18:37.835824013 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.835870981 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.835870981 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.867137909 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.867208958 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.867346048 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.867403030 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.899913073 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.901063919 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.931911945 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.932055950 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.962966919 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.963032007 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.963084936 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.963094950 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.963159084 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.963166952 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.995317936 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.995388985 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.995441914 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.995498896 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:37.995538950 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.995604038 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.995611906 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:37.995618105 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:38.021573067 CEST	49758	2022	192.168.2.4	194.31.98.116
May 12, 2022 04:18:38.026906013 CEST	2022	49758	194.31.98.116	192.168.2.4
May 12, 2022 04:18:38.028120041 CEST	49758	2022	192.168.2.4	194.31.98.116

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 04:18:36.547081947 CEST	64454	53	192.168.2.4	8.8.8.8
May 12, 2022 04:18:36.568968058 CEST	53	64454	8.8.8.8	192.168.2.4
May 12, 2022 04:18:42.931068897 CEST	64277	53	192.168.2.4	8.8.8.8
May 12, 2022 04:18:42.953504086 CEST	53	64277	8.8.8.8	192.168.2.4
May 12, 2022 04:18:49.904836893 CEST	60758	53	192.168.2.4	8.8.8.8
May 12, 2022 04:18:49.926238060 CEST	53	60758	8.8.8.8	192.168.2.4
May 12, 2022 04:18:54.971676111 CEST	64909	53	192.168.2.4	8.8.8.8
May 12, 2022 04:18:54.990967035 CEST	53	64909	8.8.8.8	192.168.2.4
May 12, 2022 04:19:05.763829947 CEST	60381	53	192.168.2.4	8.8.8.8
May 12, 2022 04:19:05.781066895 CEST	53	60381	8.8.8.8	192.168.2.4
May 12, 2022 04:19:11.760876894 CEST	56509	53	192.168.2.4	8.8.8.8
May 12, 2022 04:19:11.860119104 CEST	53	56509	8.8.8.8	192.168.2.4
May 12, 2022 04:19:17.909548044 CEST	57747	53	192.168.2.4	8.8.8.8
May 12, 2022 04:19:17.929116011 CEST	53	57747	8.8.8.8	192.168.2.4
May 12, 2022 04:19:25.096853018 CEST	58816	53	192.168.2.4	8.8.8.8
May 12, 2022 04:19:25.115648031 CEST	53	58816	8.8.8.8	192.168.2.4
May 12, 2022 04:19:30.064125061 CEST	61081	53	192.168.2.4	8.8.8.8
May 12, 2022 04:19:30.083575964 CEST	53	61081	8.8.8.8	192.168.2.4
May 12, 2022 04:19:35.064435005 CEST	60418	53	192.168.2.4	8.8.8.8
May 12, 2022 04:19:35.085571051 CEST	53	60418	8.8.8.8	192.168.2.4
May 12, 2022 04:19:41.077682972 CEST	61068	53	192.168.2.4	8.8.8.8
May 12, 2022 04:19:41.099010944 CEST	53	61068	8.8.8.8	192.168.2.4
May 12, 2022 04:19:47.313771963 CEST	58715	53	192.168.2.4	8.8.8.8
May 12, 2022 04:19:47.334959984 CEST	53	58715	8.8.8.8	192.168.2.4
May 12, 2022 04:19:53.554749012 CEST	57816	53	192.168.2.4	8.8.8.8
May 12, 2022 04:19:53.573904037 CEST	53	57816	8.8.8.8	192.168.2.4
May 12, 2022 04:20:03.402129889 CEST	51787	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 04:20:03.420929909 CEST	53	51787	8.8.8.8	192.168.2.4
May 12, 2022 04:20:10.445477009 CEST	53916	53	192.168.2.4	8.8.8.8
May 12, 2022 04:20:10.466628075 CEST	53	53916	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2022 04:18:36.547081947 CEST	192.168.2.4	8.8.8.8	0x8850	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:18:42.931068897 CEST	192.168.2.4	8.8.8.8	0x640	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:18:49.904836893 CEST	192.168.2.4	8.8.8.8	0x419c	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:18:54.971676111 CEST	192.168.2.4	8.8.8.8	0x99d8	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:19:05.763829947 CEST	192.168.2.4	8.8.8.8	0xa5bf	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:19:11.760876894 CEST	192.168.2.4	8.8.8.8	0xe1a4	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:19:17.909548044 CEST	192.168.2.4	8.8.8.8	0x6cfb	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:19:25.096853018 CEST	192.168.2.4	8.8.8.8	0x48f1	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:19:30.064125061 CEST	192.168.2.4	8.8.8.8	0xd699	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:19:35.064435005 CEST	192.168.2.4	8.8.8.8	0x98ad	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:19:41.077682972 CEST	192.168.2.4	8.8.8.8	0x9c1a	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:19:47.313771963 CEST	192.168.2.4	8.8.8.8	0xc9e8	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:19:53.554749012 CEST	192.168.2.4	8.8.8.8	0xa0db	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:20:03.402129889 CEST	192.168.2.4	8.8.8.8	0xa487	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 04:20:10.445477009 CEST	192.168.2.4	8.8.8.8	0x7769	Standard query (0)	chima2022.ddns.net	A (IP address)	IN (0x0001)

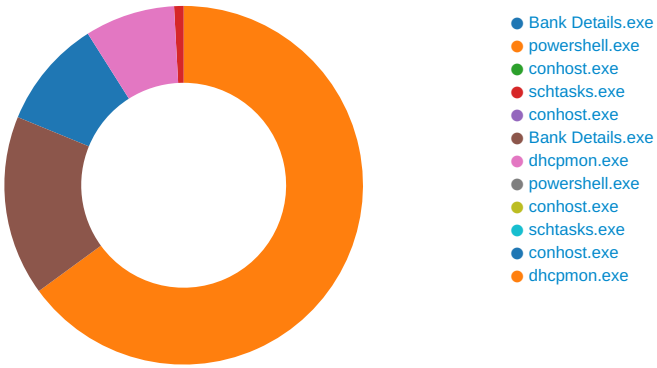
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2022 04:18:36.568968058 CEST	8.8.8.8	192.168.2.4	0x8850	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:18:42.953504086 CEST	8.8.8.8	192.168.2.4	0x640	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:18:49.926238060 CEST	8.8.8.8	192.168.2.4	0x419c	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:18:54.990967035 CEST	8.8.8.8	192.168.2.4	0x99d8	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:19:05.781066895 CEST	8.8.8.8	192.168.2.4	0xa5bf	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:19:11.860119104 CEST	8.8.8.8	192.168.2.4	0xe1a4	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:19:17.929116011 CEST	8.8.8.8	192.168.2.4	0x6cfb	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:19:25.115648031 CEST	8.8.8.8	192.168.2.4	0x48f1	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:19:30.083575964 CEST	8.8.8.8	192.168.2.4	0xd699	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:19:35.085571051 CEST	8.8.8.8	192.168.2.4	0x98ad	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:19:41.099010944 CEST	8.8.8.8	192.168.2.4	0x9c1a	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:19:47.334959984 CEST	8.8.8.8	192.168.2.4	0xc9e8	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:19:53.573904037 CEST	8.8.8.8	192.168.2.4	0xa0db	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)
May 12, 2022 04:20:03.420929909 CEST	8.8.8.8	192.168.2.4	0xa487	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2022 04:20:10.466628075 CEST	8.8.8.8	192.168.2.4	0x7769	No error (0)	chima2022.ddns.net		194.31.98.116	A (IP address)	IN (0x0001)

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Bank Details.exe PID: **1900**, Parent PID: **680**

General

Target ID:	0
Start time:	04:18:06
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\Bank Details.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Bank Details.exe"
Imagebase:	0xc0000
File size:	573440 bytes
MD5 hash:	E62E3496DEB3EE2C512CA61CF2642A0D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.281839784.000000000360F000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.281839784.000000000360F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.281839784.000000000360F000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.280585839.00000000024B1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.280695946.0000000002545000.00000004.00000800.00020000.00000000.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	6D94CF06	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	6D94CF06	unknown
C:\Users\user\AppData\Roaming\nOcstjdWFAT.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	6C79DD66	CopyFileW
C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C79DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpEA4C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C797038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Bank Details.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC5C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEA4C.tmp	success or wait	1	6C796A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\nOcstjdWFAT.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 34 63 7c 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 60 08 00 00 40 00 00 00 00 00 00 fd 73 08 00 00 20 00 00 00 fd 08 00 00 00 40 00 00 20 00 00 00 20 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 08 00 00 20 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.$PEL4c|b0`@s @ @	success or wait	3	6C79DD66	CopyFileW
C:\Users\user\AppData\Roaming\nOcstjdWFAT.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	6C79DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEA4C.tmp	0	1598	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 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 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo>	success or wait	1	6C791B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Bank Details.exe.log	0	1308	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	6DC5C907	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	6D925705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D925705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D92CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D925705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D925705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C791B4F	ReadFile

Analysis Process: powershell.exe PID: **580**, Parent PID: **1900**

General

Target ID:	4
Start time:	04:18:20
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe
Imagebase:	0xd50000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	6D94CF06	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	6D94CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0jupmy4m.iym.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C791E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c54pb3wi.g5d.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C791E60	CreateFileW
C:\Users\user\Documents\20220512	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C79BEFF	CreateDirectoryW
C:\Users\user\Documents\20220512\PowerShell_transcript.124406.b92XxzZg.20220512041824.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C791E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0jupmy4m.iym.ps1	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c54pb3wi.g5d.psm1	success or wait	1	6C796A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0jupmy4m.iym.ps1	0	1	31	1	success or wait	1	6C791B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c54pb3wi.g5d.psm1	0	1	31	1	success or wait	1	6C791B4F	WriteFile
C:\Users\user\Documents\20220512\PowerShell_transcript.124406.b92XxzZg.20220512041824.txt	0	3	ff		success or wait	1	6C791B4F	WriteFile
C:\Users\user\Documents\20220512\PowerShell_transcript.124406.b92XxzZg.20220512041824.txt	3	677	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 31 32 30 34 31 38 32 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 32 34 34 30 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220512041826Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 124406 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6C791B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 79 14 00 00 1a 00 00 00 fd 0d 5a 05 3a 08 31 08 31 08 00 00 53 00 75 00 11 00 72 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eyZ:11Sur@	success or wait	1	6DC176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6DC176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DC176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DC176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DC176FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@BMDmEEMqqS%n4&5&7&	success or wait	11	6DC176FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D925705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D925705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D925705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D925705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D92CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D92CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D92CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D925705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D925705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D925705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D925705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D925705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D925705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D931F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6D93203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8803DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C791B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	126	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C791B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D925705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D925705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D925705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D925705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C791B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C791B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C791B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C791B4F	ReadFile

Analysis Process: conhost.exe PID: **1724**, Parent PID: **580**

General

Target ID:	5
Start time:	04:18:21
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: **4192**, Parent PID: **1900**

General

Target ID:	6
Start time:	04:18:22
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nOcstjdWFAT" /XML "C:\Users\user\AppData\Local\Temp\tmpEA4C.tmp
Imagebase:	0x1060000
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\tmpEA4C.tmp	unknown	2	success or wait	1	106AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpEA4C.tmp	unknown	1599	success or wait	1	106ABD9	ReadFile

Analysis Process: conhost.exe PID: **5848**, Parent PID: **4192**

General

Target ID:	7
Start time:	04:18:24
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: Bank Details.exe PID: **3560**, Parent PID: **1900**

General

Target ID:	8
Start time:	04:18:27
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\Bank Details.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Bank Details.exe
Imagebase:	0x530000
File size:	573440 bytes
MD5 hash:	E62E3496DEB3EE2C512CA61CF2642A0D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.501615739.00000000050E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.501615739.00000000050E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.501615739.00000000050E0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.495963136.0000000000E40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.495963136.0000000000E40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.495963136.0000000000E40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.277836279.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.277836279.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.277836279.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.497746331.0000000003901000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.497746331.0000000003901000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.495078358.0000000000B50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.495078358.0000000000B50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.495078358.0000000000B50000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.493375086.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.493375086.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.493375086.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.501831791.00000000052E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.501831791.00000000052E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.501831791.00000000052E0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.501831791.00000000052E0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.496914217.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.500271666.00000000047BE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.500271666.00000000047BE000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.496292504.0000000000E80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.496292504.0000000000E80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.496292504.0000000000E80000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.275861261.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.275861261.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000008.00000000.275861261.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.496440723.0000000000EA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.496440723.0000000000EA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.496440723.0000000000EA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.499495990.00000000045ED000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000008.00000002.499495990.00000000045ED000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.495027956.0000000000B30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.495027956.0000000000B30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.495027956.0000000000B30000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.501096037.0000000004834000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000008.00000002.501096037.0000000004834000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.276616550.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.276616550.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000008.00000000.276616550.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.494831319.0000000000AE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.494831319.0000000000AE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.494831319.0000000000AE0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: NanoCore, Description: unknown, Source: 00000008.00000002.503251204.0000000006D21000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.494865056.0000000000AF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.494865056.0000000000AF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.494865056.0000000000AF0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.496185988.0000000000E60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.496185988.0000000000E60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.496185988.0000000000E60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.495924977.0000000000E30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.495924977.0000000000E30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.495924977.0000000000E30000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.501709617.0000000005260000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.501709617.0000000005260000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.501709617.0000000005260000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.274867582.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.274867582.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000008.00000000.274867582.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.496097202.0000000000E50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.496097202.0000000000E50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.496097202.0000000000E50000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.495050243.0000000000B40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.495050243.0000000000B40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.495050243.0000000000B40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: NanoCore, Description: unknown, Source: 00000008.00000002.496960213.000000000296C000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.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	6D94CF06	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	6D94CF06	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	6C79BEFF	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	6C791E60	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	6C79BEFF	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	6C79DD66	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	6C79DD66	CopyFileW
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	6C79BEFF	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	6C79BEFF	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	13	6C791E60	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	6C791E60	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	6C791E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Bank Details.exe:Zone.Identifier	success or wait	1	6C712935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	06 60 fd fd fd 33 fd 48	`3H	success or wait	1	6C791B4F	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 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 34 63 7c 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 60 08 00 00 40 00 00 00 00 00 00 fd 73 08 00 00 20 00 00 00 fd 08 00 00 00 40 00 00 20 00 00 00 20 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 08 00 00 20 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.$PEL4c|b0`@s @ @	success or wait	3	6C79DD66	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	6C79DD66	CopyFileW
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(1PPcLTAb4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F}EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	13	6C791B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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"30tRDn_4dEi~|fX_Xfp^>a$e6:7d(aA=)*{B[y%*iQ<xtXHHF7gI*3{nLy;is-(5iJ5b7}fKHV	success or wait	1	6C791B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	6C791B4F	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	6D925705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D925705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D92CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D925705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D925705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C791B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D90D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D90D72F	unknown
C:\Users\user\Desktop\Bank Details.exe	unknown	4096	success or wait	1	6D90D72F	unknown
C:\Users\user\Desktop\Bank Details.exe	unknown	512	success or wait	1	6D90D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6D90D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6D90D72F	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	6C79646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **6400**, Parent PID: **3616**

General

Target ID:	20
Start time:	04:18:42
Start date:	12/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xa70000
File size:	573440 bytes
MD5 hash:	E62E3496DEB3EE2C512CA61CF2642A0D
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: 00000014.00000002.343046224.0000000002F43000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.344353611.000000000400F000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.344353611.000000000400F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.344353611.000000000400F000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.342911345.0000000002EB1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 12%, ReversingLabs
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	6D94CF06	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	6D94CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp5C9D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C797038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC5C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5C9D.tmp	success or wait	1	6C796A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5C9D.tmp	0	1598	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 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 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo>	success or wait	1	6C791B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	1308	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	6DC5C907	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	6D925705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D925705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D92CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D925705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D925705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C791B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C791B4F	ReadFile

Analysis Process: powershell.exe PID: **6572**, Parent PID: **6400**

General

Target ID:	23
Start time:	04:18:50
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nOcstjdWFAT.exe
Imagebase:	0xd50000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: **6580**, Parent PID: **6572**

General

Target ID:	24
Start time:	04:18:50
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: **6588**, Parent PID: **6400**

General

Target ID:	25
Start time:	04:18:50
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nOcstjdWFAT" /XML "C:\Users\user\AppData\Local\Temp\tmp5C9D.tmp
Imagebase:	0x1060000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **6680**, Parent PID: **6588**

General	
Target ID:	26
Start time:	04:18:51
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: **6784**, Parent PID: **6400**

General	
Target ID:	27
Start time:	04:18:54
Start date:	12/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x960000
File size:	573440 bytes
MD5 hash:	E62E3496DEB3EE2C512CA61CF2642A0D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.333597791.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.333597791.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.333597791.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.331990399.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.331990399.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.331990399.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000002.358941413.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.358941413.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.358941413.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.360814812.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.360814812.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.360570995.0000000002DB1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.360570995.0000000002DB1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.334288082.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.334288082.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.334288082.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.332881554.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.332881554.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.332881554.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Disassembly

No disassembly