ID: 627817
Sample Name: PO #50251_House Building Project.exe
Cookbook: default.jbs
Time: 21:24:13
Date: 16/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

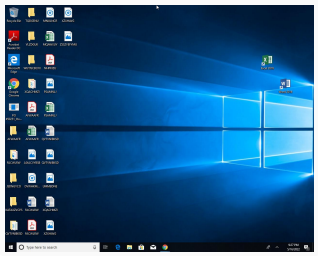
Windows Analysis Report

PO #50251_House Building Project.exe

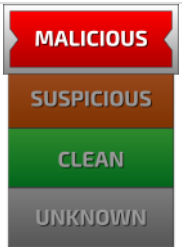
Overview

General Information

Sample Name:	PO #50251_House Building Project.exe
Analysis ID:	627817
MD5:	08c261ade5c2d3..
SHA1:	2a18a2cefe110c...
SHA256:	17952248625aaa.
Tags:	exe nanocore
Infos:	



Detection



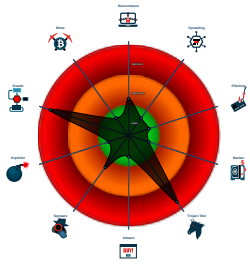
Nanocore

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

Signatures

- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- 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...
- Injects a PE file into a foreign proce...
- Yara detected Generic Downloader

Classification



Process Tree

- **System is w10x64**
- PO #50251_House Building Project.exe (PID: 6996 cmdline: "C:\Users\user\Desktop\PO #50251_House Building Project.exe" MD5: 08C261ADE5C2D31437DA373D90A2F6D0)
  - PO #50251_House Building Project.exe (PID: 3968 cmdline: C:\Users\user\Desktop\PO #50251_House Building Project.exe MD5: 08C261ADE5C2D31437DA373D90A2F6D0)
  - PO #50251_House Building Project.exe (PID: 4780 cmdline: C:\Users\user\Desktop\PO #50251_House Building Project.exe MD5: 08C261ADE5C2D31437DA373D90A2F6D0)
    - schtasks.exe (PID: 6520 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpCD7F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 4448 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpD6B8.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- PO #50251_House Building Project.exe (PID: 5844 cmdline: "C:\Users\user\Desktop\PO #50251_House Building Project.exe" 0 MD5: 08C261ADE5C2D31437DA373D90A2F6D0)
  - PO #50251_House Building Project.exe (PID: 6824 cmdline: C:\Users\user\Desktop\PO #50251_House Building Project.exe MD5: 08C261ADE5C2D31437DA373D90A2F6D0)
- dhcpmon.exe (PID: 3960 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 08C261ADE5C2D31437DA373D90A2F6D0)
  - dhcpmon.exe (PID: 4356 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 08C261ADE5C2D31437DA373D90A2F6D0)
  - dhcpmon.exe (PID: 5996 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 08C261ADE5C2D31437DA373D90A2F6D0)
- dhcpmon.exe (PID: 6696 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 08C261ADE5C2D31437DA373D90A2F6D0)
  - dhcpmon.exe (PID: 5696 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 08C261ADE5C2D31437DA373D90A2F6D0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.703804511.0000000006A00000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
00000003.00000002.703804511.0000000006A00000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost
00000003.00000002.703804511.0000000006A00000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x227f:$x2: NanoCore.ClientPlugin • 0x2205:$x3: NanoCore.ClientPluginHost • 0x2295:$i3: IClientNetwork • 0x221f:$i6: IClientLoggingHost • 0x223e:$i7: IClientNetworkHost • 0x1f9f:$s1: ClientPlugin • 0x2288:$s1: ClientPlugin
0000000C.00000002.574005491.0000000007630000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x5186f:$s1: file:/// • 0x5177f:$s2: {11111-22222-10009-11112} • 0x517ff:$s3: {11111-22222-50001-00000} • 0x4ec49:$s4: get_Module • 0x4f08f:$s5: Reverse • 0x510ae:$s6: BlockCopy • 0x50ef2:$s7: ReadByte • 0x51881:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...
00000003.00000002.701420993.00000000045D1000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x56297:$a: NanoCore • 0x56381:$a: NanoCore • 0x571f8:$a: NanoCore • 0x603a2:$a: NanoCore • 0x60403:$a: NanoCore • 0x60446:$a: NanoCore • 0x60486:$a: NanoCore • 0x606c2:$a: NanoCore • 0x60762:$a: NanoCore • 0x60f3a:$a: NanoCore • 0x6152d:$a: NanoCore • 0x6167e:$a: NanoCore • 0x624d8:$a: NanoCore • 0x6273f:$a: NanoCore • 0x62754:$a: NanoCore • 0x62773:$a: NanoCore • 0x6b676:$a: NanoCore • 0x6b69f:$a: NanoCore • 0x77418:$a: NanoCore • 0x77441:$a: NanoCore • 0x9c304:$a: NanoCore
Click to see the 168 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.PO #50251_House Building Project.exe.74b0000.32.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
3.2.PO #50251_House Building Project.exe.74b0000.32.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x170b:$x2: NanoCore.ClientPluginHost • 0x34b6:$s4: PipeCreated • 0x16f8:$s5: IClientLoggingHost
3.2.PO #50251_House Building Project.exe.74b0000.32.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x16e2:$x2: NanoCore.ClientPlugin • 0x170b:$x3: NanoCore.ClientPluginHost • 0x16d3:$i3: IClientNetwork • 0x16f8:$i6: IClientLoggingHost • 0x1725:$i7: IClientNetworkHost • 0x154e:$s1: ClientPlugin • 0x16eb:$s1: ClientPlugin
3.2.PO #50251_House Building Project.exe.33243e0.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
3.2.PO #50251_House Building Project.exe.33243e0.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
Click to see the 465 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

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29

Timestamp:	192.168.2.562.197.136.294975069322025019 05/16/22-21:25:52.856033
SID:	2025019
Source Port:	49750
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29

Timestamp:	192.168.2.562.197.136.294980969322816766 05/16/22-21:27:12.964613
SID:	2816766
Source Port:	49809
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29

Timestamp:	192.168.2.562.197.136.294979869322816766 05/16/22-21:26:49.243371
SID:	2816766
Source Port:	49798
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29

Timestamp:	192.168.2.562.197.136.294976869322816766 05/16/22-21:26:11.235768
SID:	2816766
Source Port:	49768
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29

Timestamp:	192.168.2.562.197.136.294975369322025019 05/16/22-21:26:01.935288
SID:	2025019
Source Port:	49753
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29

Timestamp:	192.168.2.562.197.136.294979069322025019 05/16/22-21:26:42.275938

SID:	2025019
Source Port:	49790
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294981569322816766 05/16/22-21:27:26.149799
SID:	2816766
Source Port:	49815
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294980569322816766 05/16/22-21:26:59.008542
SID:	2816766
Source Port:	49805
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294977669322025019 05/16/22-21:26:23.086500
SID:	2025019
Source Port:	49776
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294978669322025019 05/16/22-21:26:35.982915
SID:	2025019
Source Port:	49786
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294977469322816766 05/16/22-21:26:18.016014
SID:	2816766
Source Port:	49774
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294980069322025019 05/16/22-21:26:54.440781
SID:	2025019
Source Port:	49800
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294979069322816766 05/16/22-21:26:43.277475
SID:	2816766
Source Port:	49790
Destination Port:	6932
Protocol:	TCP

Copyright Joe Security LLC 2022

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294978469322816766 05/16/22-21:26:30.844453
SID:	2816766
Source Port:	49784
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294979869322025019 05/16/22-21:26:48.328157
SID:	2025019
Source Port:	49798
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294976869322025019 05/16/22-21:26:09.561629
SID:	2025019
Source Port:	49768
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 62.197.136.29 - Destination IP: 192.168.2.5	
Timestamp:	62.197.136.29192.168.2.56932497742810290 05/16/22-21:26:17.683429
SID:	2810290
Source Port:	6932
Destination Port:	49774
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294975069322816766 05/16/22-21:25:55.185134
SID:	2816766
Source Port:	49750
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 62.197.136.29 - Destination IP: 192.168.2.5	
Timestamp:	62.197.136.29192.168.2.56932498002841753 05/16/22-21:26:54.469135
SID:	2841753
Source Port:	6932
Destination Port:	49800
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294980669322025019 05/16/22-21:27:04.210887
SID:	2025019
Source Port:	49806
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294981669322025019 05/16/22-21:27:31.248386

SID:	2025019
Source Port:	49816
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29

Timestamp:	192.168.2.562.197.136.294978469322025019 05/16/22-21:26:29.259944
SID:	2025019
Source Port:	49784
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 62.197.136.29 - Destination IP: 192.168.2.5

Timestamp:	62.197.136.29192.168.2.56932498052841753 05/16/22-21:26:59.008396
SID:	2841753
Source Port:	6932
Destination Port:	49805
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 62.197.136.29 - Destination IP: 192.168.2.5

Timestamp:	62.197.136.29192.168.2.56932498062841753 05/16/22-21:27:04.245424
SID:	2841753
Source Port:	6932
Destination Port:	49806
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29

Timestamp:	192.168.2.562.197.136.294978469322816718 05/16/22-21:26:30.844453
SID:	2816718
Source Port:	49784
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29

Timestamp:	192.168.2.562.197.136.294980569322025019 05/16/22-21:26:58.969128
SID:	2025019
Source Port:	49805
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29

Timestamp:	192.168.2.562.197.136.294977469322025019 05/16/22-21:26:16.240472
SID:	2025019
Source Port:	49774
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29

Timestamp:	192.168.2.562.197.136.294981169322816766 05/16/22-21:27:20.077754
SID:	2816766
Source Port:	49811
Destination Port:	6932
Protocol:	TCP

Copyright Joe Security LLC 2022

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 62.197.136.29 - Destination IP: 192.168.2.5	
Timestamp:	62.197.136.29192.168.2.56932498162841753 05/16/22-21:27:46.318090
SID:	2841753
Source Port:	6932
Destination Port:	49816
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294977669322816766 05/16/22-21:26:24.262881
SID:	2816766
Source Port:	49776
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294981169322025019 05/16/22-21:27:18.270244
SID:	2025019
Source Port:	49811
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294975369322816766 05/16/22-21:26:04.278239
SID:	2816766
Source Port:	49753
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294980969322025019 05/16/22-21:27:09.797979
SID:	2025019
Source Port:	49809
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294981569322025019 05/16/22-21:27:25.175574
SID:	2025019
Source Port:	49815
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 62.197.136.29	
Timestamp:	192.168.2.562.197.136.294978669322816766 05/16/22-21:26:37.260257
SID:	2816766
Source Port:	49786
Destination Port:	6932
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted 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

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

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

Yara detected Nanocore RAT

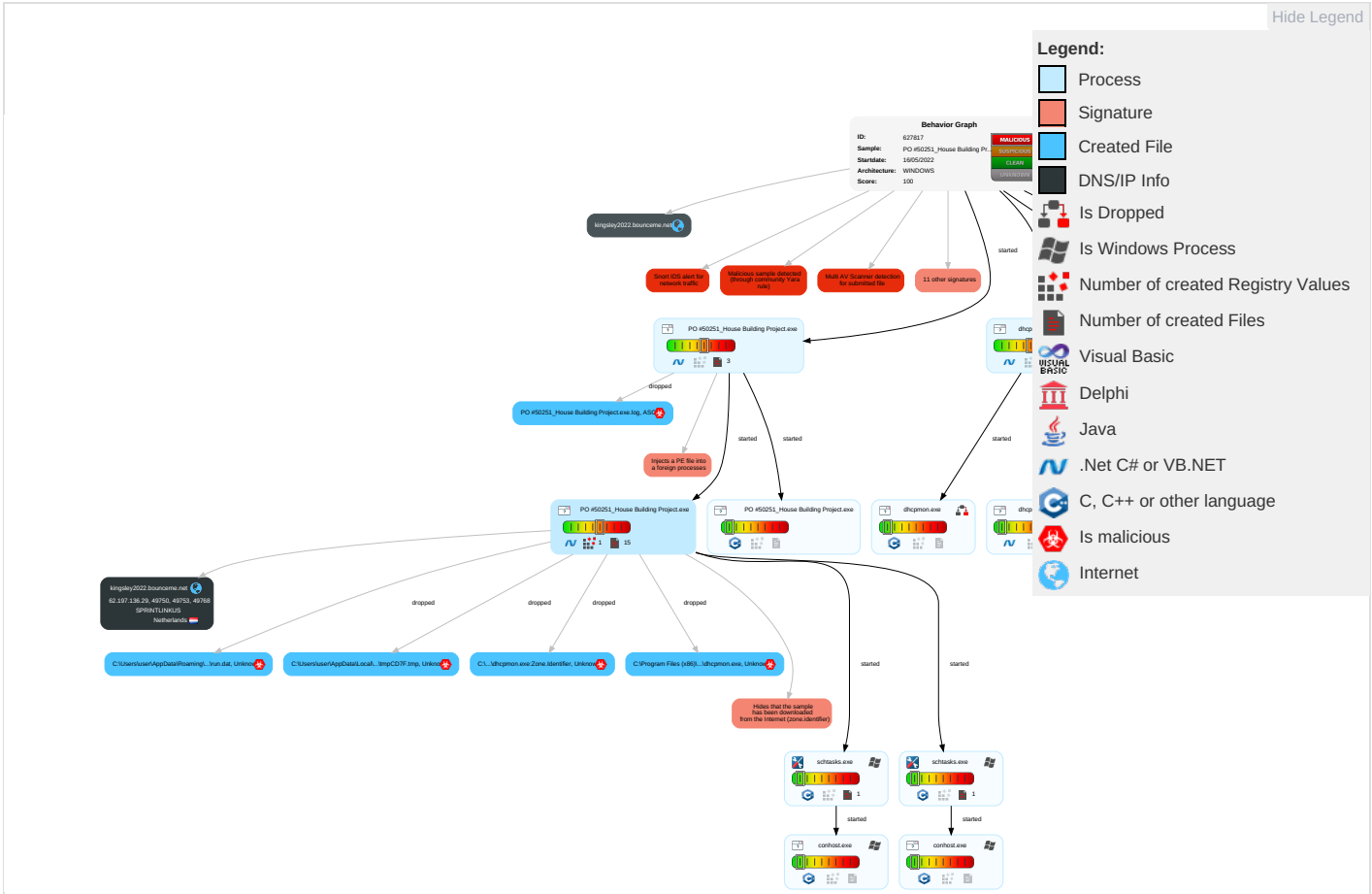
Copyright Joe Security LLC 2022

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 Disable or Modify Tools	LSASS Memory	1 1 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	1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	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

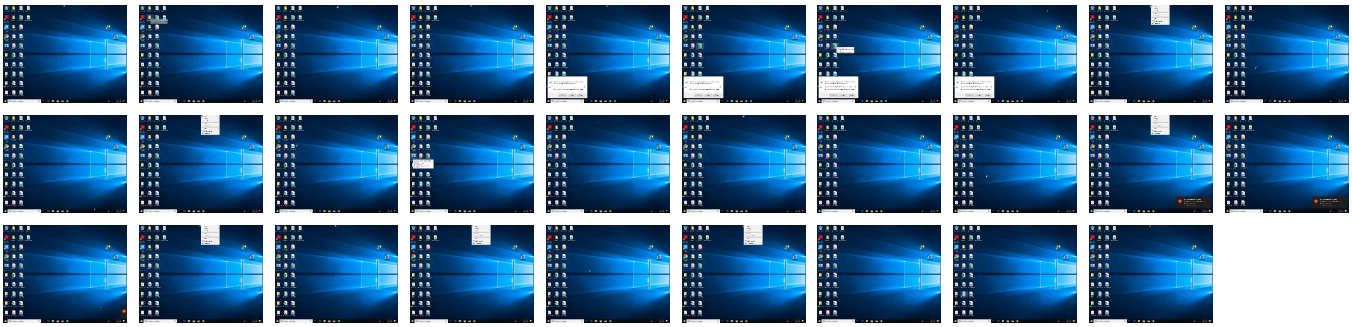
Copyright Joe Security LLC 2022



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
PO #50251_House Building Project.exe	29%	Virustotal		Browse
PO #50251_House Building Project.exe	34%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
PO #50251_House Building Project.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.PO #50251_House Building Project.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.PO #50251_House Building Project.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.PO #50251_House Building Project.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
3.0.PO #50251_House Building Project.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.PO #50251_House Building Project.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.PO #50251_House Building Project.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.PO #50251_House Building Project.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.PO #50251_House Building Project.exe.5ce0000.25.unpack	100%	Avira	TR/NanoCore.fadte		Download File
16.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.PO #50251_House Building Project.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.PO #50251_House Building Project.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.PO #50251_House Building Project.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.PO #50251_House Building Project.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.PO #50251_House Building Project.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

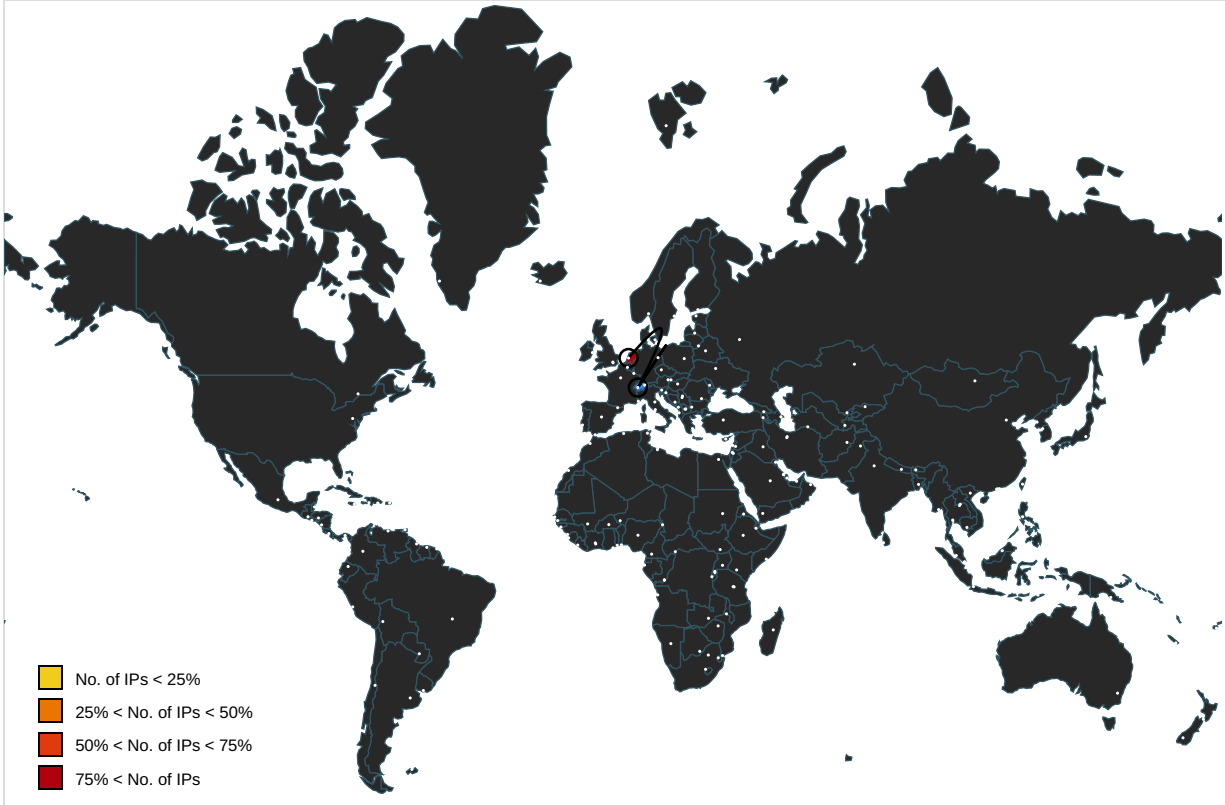
Name	IP	Active	Malicious	Antivirus Detection	Reputation
kingsley2022.bounceme.net	62.197.136.29	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	PO #50251_House Building Project.exe, 00000003.00000002.701420993.00000000045D1000.00000004.00000800.00020000.00000000.sdmp, PO #50251_House Building Project.exe, 00000003.00000002.701249536.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, PO #50251_House Building Project.exe, 00000003.00000002.699082789.0000000003360000.00000004.00000800.00020000.00000000.sdmp, PO #50251_House Building Project.exe, 00000003.00000002.704185578.0000000007470000.00000004.08000000.00040000.00000000.sdmp	false		high
http://www.carterandcone.coml	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	PO #50251_House Building Project.exe, 00000000.00000002.474662454.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
62.197.136.29	kingsley2022.bounceme.net	Netherlands		1239	SPRINTLINKUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	627817

Start date and time: 16/05/202221:24:13	2022-05-16 21:24:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO #50251_House Building Project.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@22/11@16/1
EGA Information:	• Successful, ratio: 75%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • 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): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target PO #50251_House Building Project.exe, PID 3968 because there are no executed function
- 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.

Simulations

Behavior and APIs

Time	Type	Description
21:25:37	API Interceptor	763x Sleep call for process: PO #50251_House Building Project.exe modified
21:25:48	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\PO #50251_House Building Project.exe" s>$(Arg0)
21:25:51	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
21:25:53	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
21:26:02	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
File Type:	Unknown
Category:	dropped
Size (bytes):	565248
Entropy (8bit):	7.967142777272689
Encrypted:	false
SSDEEP:	6144:2OQIHT3dvRwms8jDkJuapaQWaR0eyrcBsW03AUWH33Z/h/aZnAqAFtz8PX2c+Vbs:2ApfjDktaiqePiR4B5aGvFtzrDcxbd
MD5:	08C261ADE5C2D31437DA373D90A2F6D0
SHA1:	2A18A2CEFE110CFEE786AFABAED53DB3AF3B0E4B
SHA-256:	17952248625AAA9C25208DC4AB2D7849AA39D2C189AAC5B26FE2F3D130301E1A
SHA-512:	289A9E40729F319C5E080706A3DBD4423E1D87C8BDA54625F928ACE1DA72DD69CA835833D53B968E9ABE0DCDF14D46E1DDDBE90A1DF3D95042F280DE2337220
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...4R.b.....0..... .....@.. ....@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....M..(-.....:...z...;.....(.....}.....{....o.....}.....}.....s....}....*...0..O.....{....o....#.....6..{....o/.....+.....s;..... {.....o.....+...+..*^.(.....}.....}....*..0.....{.....+..*.0.....{.....+..*".(.....*B.(.....}....*B...{.....X}....*..0.....{.....+..*.0.....(.....s....}.....s....}.....+...{.....ss....o.....X .....-...+...{.....cs....o.....X.....

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

Process:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
File Type:	Unknown
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\PO #50251_House Building Project.exe.log

Process:	C:\Users\user\Desktop\PO #50251_House Building Project.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:	**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\Temp\tmpCD7F.tmp

Process:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
File Type:	Unknown
Category:	dropped
Size (bytes):	1323
Entropy (8bit):	5.119615855451204
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0PZxtn:cbk4oL600QydbQxIYODOLedq3SZj
MD5:	74773A6FF5024880B8BAA78ABAAF16A7
SHA1:	87D9F2169952088916627AD2D7348974BCE69EC0
SHA-256:	964634EC39313B451538C04B52347B091171ADA097F1E30168ED8F79AEC4F13D
SHA-512:	B5F196A9C8A04E91D7121FEF3AA3AFBE6409BAEE8894058308AE6B90A8A00D3F8B99412EB51EE08DBC231531FD026C9D2F4F2BF33D1F0134C1CA45B462B4788E
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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpD6B8.tmp

Process:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
File Type:	Unknown
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
File Type:	Unknown
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\PO #50251_House Building Project.exe
File Type:	Unknown
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:qd:qd
MD5:	4C8DAD00841C3792A8BC07DA38C3625C
SHA1:	C5376437D3FDEEF526B94FCC3AC60C55DA1C52A1
SHA-256:	C72AA4D77A277E88DB04406BF419074CF455D74898B9AEF0519F5F357F34219C
SHA-512:	2D594148650E2C651E757C66E626D0C196171FCA4BF459345512CED8B5C6291FBBD4682AA2F76B399CB60C06DF8BD67A90D3FC64D4CBEA1EDD4249480A30CFBA
Malicious:	**true**
Reputation:	unknown

Preview:	{..O.7.H

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

Process:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
File Type:	Unknown
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

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

Process:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
File Type:	Unknown
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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...l.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV...,...0.... ....n.w6PMl.......v.'".v.......#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*l..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.Ql..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<..._[.69@.2..m..l..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

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

Process:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
File Type:	Unknown
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.8423188792597305
Encrypted:	false
SSDEEP:	3:oNUWJRW1qB9QlnQdWEeC:oNNJAgBNV
MD5:	195F5555DE114E5B83BBA9BCBBC53678
SHA1:	AC0E62FCC55F0FF36B90CC08E3944B400BCFA26B
SHA-256:	E23C2315A4F50FE82D28626A9833AE751AC52D4C9175B022A59F831A171132EA
SHA-512:	99ABBB1103177D363288700E8307DF136B270741838E844E93C825CA52589ED157B1C28BB8799010CE371983326FCEA328BDE217749D96E140411019E7E253E6
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\PO #50251_House Building Project.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.967142777272689
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PO #50251_House Building Project.exe
File size:	565248
MD5:	08c261ade5c2d31437da373d90a2f6d0
SHA1:	2a18a2cefe110cfee786afabaed53db3af3b0e4b
SHA256:	17952248625aaa9c25208dc4ab2d7849aa39d2c189aac5b26fe2f3d130301e1a
SHA512:	289a9e40729f319c5e080706a3dbd4423e1d87c8bda54625f928ace1da72dd69ca835833d53b968e9abe0dcdf14d46e1dddbe90a1df3d95042f280de23372f20
SSDEEP:	6144:2OQIHT3dvRwms8jDkJuapaQWaR0eyrcBsW03AUWH33Z/h/aZnAqAFtz8PX2c+Vbs:2ApfjDktaiqePiR4B5aGvFtzrDcxbd
TLSH:	2BC423582DF8DB31CAAA03BF62359924DB7A30556C71DE972DE240D82712BD18CF1E27
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...4R.b.....0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48b712
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:	0x62825234 [Mon May 16 13:31:32 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]
call far B999h : 99999999h
aas
mov eax, 51EB851Eh
mov eax, 5C293FBEh
pop edx
cmc
sub ah, cl
aas
mov eax, 51EB851Eh
mov eax, 147B3FCEh
scasb
inc edi

Instruction
loope 00007FA388AFE43Ch
aam 3Fh
salc
aas
call far D999h : 99999999h
aas
int CCh
int3
int3
int3
int3
fdivr qword ptr [edi]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
loopne 00007FA388AFE401h
movsb
jo 00007FA388AFE3FFh
or dl, bh
mov dword ptr [999A3FE0h], eax
cdq
cdq
cdq
cdq
mov ecx, 851EB83Fh
jmp 00007FA388AFE413h
mov eax, 5C293FBEh
pop edx
cmc
sub ah, cl
aas
mov eax, 51EB851Eh
mov eax, 147B3FCEh
scasb
inc edi
loope 00007FA388AFE43Ch
aam 3Fh
salc
aas
scasb
inc edi
loope 00007FA388AFE43Ch
adc al, AEh
xlatb
aas
add dword ptr [eax], eax
add byte ptr [eax], al
xor eax, 2C000025h
xchg eax, edi
add byte ptr [eax], al
inc esp
inc edx
add dword ptr [eax], eax
cmp al, 67h
add al, byte ptr [eax]
inc eax
or eax, D0900003h
add eax, dword ptr [eax]
and byte ptr [ecx-7B7FFFF9h], ah

Instruction
push ds
add byte ptr [eax+01009896h], al
add byte ptr [eax], al
add ah, ah
and eax, 9A330000h
add byte ptr [eax], al
call 00007FA35DAFE50Dh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8b6c0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8c000	0x3e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x897e8	0x89800	False	0.972807173295	data	7.97320023522	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8c000	0x3e0	0x400	False	0.408203125	data	3.1221458638	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x8c058	0x384	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	2021 Razer Inc. All rights reserved.
Assembly Version	1.0.0.0
InternalName	YieldAwaita.exe
FileVersion	1.0.0.0
CompanyName	HP Legion
LegalTrademarks	
Comments	
ProductName	GameManager Service
ProductVersion	1.0.0.0

Copyright Joe Security LLC 2022

Description	Data
FileDescription	GameManager Service
OriginalFilename	YieldAwaita.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.562.197.136.29 4975069322025019 05/16/22-21:25:52.856033	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4980969322816766 05/16/22-21:27:12.964613	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49809	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4979869322816766 05/16/22-21:26:49.243371	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49798	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4976869322816766 05/16/22-21:26:11.235768	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49768	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4975369322025019 05/16/22-21:26:01.935288	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4979069322025019 05/16/22-21:26:42.275938	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49790	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4981569322816766 05/16/22-21:27:26.149799	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49815	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4980569322816766 05/16/22-21:26:59.008542	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49805	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4977669322025019 05/16/22-21:26:23.086500	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4978669322025019 05/16/22-21:26:35.982915	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4977469322816766 05/16/22-21:26:18.016014	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49774	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4980069322025019 05/16/22-21:26:54.440781	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49800	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4979069322816766 05/16/22-21:26:43.277475	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49790	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4978469322816766 05/16/22-21:26:30.844453	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49784	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4979869322025019 05/16/22-21:26:48.328157	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49798	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.29 4976869322025019 05/16/22-21:26:09.561629	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	6932	192.168.2.5	62.197.136.29

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
62.197.136.29192.168.2.56932497742810290 05/16/22-21:26:17.683429	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	6932	49774	62.197.136.29	192.168.2.5
192.168.2.562.197.136.294975069322816766 05/16/22-21:25:55.185134	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49750	6932	192.168.2.5	62.197.136.29
62.197.136.29192.168.2.56932498002841753 05/16/22-21:26:54.469135	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6932	49800	62.197.136.29	192.168.2.5
192.168.2.562.197.136.294980669322025019 05/16/22-21:27:04.210887	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49806	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.294981669322025019 05/16/22-21:27:31.248386	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.294978469322025019 05/16/22-21:26:29.259944	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	6932	192.168.2.5	62.197.136.29
62.197.136.29192.168.2.56932498052841753 05/16/22-21:26:59.008396	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6932	49805	62.197.136.29	192.168.2.5
62.197.136.29192.168.2.56932498062841753 05/16/22-21:27:04.245424	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6932	49806	62.197.136.29	192.168.2.5
192.168.2.562.197.136.294978469322816718 05/16/22-21:26:30.844453	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49784	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.294980569322025019 05/16/22-21:26:58.969128	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49805	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.294977469322025019 05/16/22-21:26:16.240472	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49774	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.294981169322816766 05/16/22-21:27:20.077754	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49811	6932	192.168.2.5	62.197.136.29
62.197.136.29192.168.2.56932498162841753 05/16/22-21:27:46.318090	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6932	49816	62.197.136.29	192.168.2.5
192.168.2.562.197.136.294977669322816766 05/16/22-21:26:24.262881	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49776	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.294981169322025019 05/16/22-21:27:18.270244	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49811	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.294975369322816766 05/16/22-21:26:04.278239	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49753	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.294980969322025019 05/16/22-21:27:09.797979	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49809	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.294981569322025019 05/16/22-21:27:25.175574	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	6932	192.168.2.5	62.197.136.29
192.168.2.562.197.136.294978669322816766 05/16/22-21:26:37.260257	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49786	6932	192.168.2.5	62.197.136.29

Network Port Distribution

Total Packets: 46

- 53 (DNS)
- 6932 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 16, 2022 21:25:52.749424934 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:52.782857895 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:52.783004045 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:52.856033087 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:52.930124044 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:52.945125103 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:52.974734068 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:53.076452971 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:53.808614016 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:53.896286964 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.154181004 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.246649027 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.404290915 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.404349089 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.404373884 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.404400110 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.404541969 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.404587030 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.454766989 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.454813957 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.454838991 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.454924107 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.454950094 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.454973936 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.454977036 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.454999924 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.454999924 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.455023050 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.455027103 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.455075979 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.481057882 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481098890 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481123924 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481147051 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481172085 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481198072 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481223106 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481247902 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481271029 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481293917 CEST	6932	49750	62.197.136.29	192.168.2.5

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 16, 2022 21:25:54.481302977 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.481319904 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481333971 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.481343031 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481368065 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.481369972 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481393099 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.481395006 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481421947 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481447935 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.481465101 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.481507063 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.507662058 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.507752895 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.507778883 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.507798910 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.507817984 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.507842064 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.507864952 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.507890940 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.507915020 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.507946014 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.507966042 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.507989883 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508013964 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508023977 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.508038044 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508057117 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.508065939 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508090973 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508093119 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.508116961 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508141041 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508150101 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.508167982 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508188009 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508214951 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508224964 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.508241892 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508266926 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508280039 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.508294106 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508318901 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508322954 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.508344889 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508354902 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.508372068 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508397102 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508409023 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.508424997 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508452892 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.508452892 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.508498907 CEST	49750	6932	192.168.2.5	62.197.136.29
May 16, 2022 21:25:54.508511066 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.544588089 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.544626951 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.544651985 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.544676065 CEST	6932	49750	62.197.136.29	192.168.2.5

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 16, 2022 21:25:54.544701099 CEST	6932	49750	62.197.136.29	192.168.2.5
May 16, 2022 21:25:54.544724941 CEST	6932	49750	62.197.136.29	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 16, 2022 21:25:52.718883991 CEST	53757	53	192.168.2.5	8.8.8.8
May 16, 2022 21:25:52.739039898 CEST	53	53757	8.8.8.8	192.168.2.5
May 16, 2022 21:26:01.874166012 CEST	54322	53	192.168.2.5	8.8.8.8
May 16, 2022 21:26:01.892497063 CEST	53	54322	8.8.8.8	192.168.2.5
May 16, 2022 21:26:09.506463051 CEST	62466	53	192.168.2.5	8.8.8.8
May 16, 2022 21:26:09.524383068 CEST	53	62466	8.8.8.8	192.168.2.5
May 16, 2022 21:26:16.193361998 CEST	61941	53	192.168.2.5	8.8.8.8
May 16, 2022 21:26:16.211782932 CEST	53	61941	8.8.8.8	192.168.2.5
May 16, 2022 21:26:23.019675970 CEST	57352	53	192.168.2.5	8.8.8.8
May 16, 2022 21:26:23.039601088 CEST	53	57352	8.8.8.8	192.168.2.5
May 16, 2022 21:26:29.188756943 CEST	63538	53	192.168.2.5	8.8.8.8
May 16, 2022 21:26:29.209069967 CEST	53	63538	8.8.8.8	192.168.2.5
May 16, 2022 21:26:35.936079979 CEST	61478	53	192.168.2.5	8.8.8.8
May 16, 2022 21:26:35.954624891 CEST	53	61478	8.8.8.8	192.168.2.5
May 16, 2022 21:26:42.222913980 CEST	57809	53	192.168.2.5	8.8.8.8
May 16, 2022 21:26:42.239293098 CEST	53	57809	8.8.8.8	192.168.2.5
May 16, 2022 21:26:48.281331062 CEST	49407	53	192.168.2.5	8.8.8.8
May 16, 2022 21:26:48.297589064 CEST	53	49407	8.8.8.8	192.168.2.5
May 16, 2022 21:26:54.390856028 CEST	49912	53	192.168.2.5	8.8.8.8
May 16, 2022 21:26:54.407196045 CEST	53	49912	8.8.8.8	192.168.2.5
May 16, 2022 21:26:58.918062925 CEST	63488	53	192.168.2.5	8.8.8.8
May 16, 2022 21:26:58.936566114 CEST	53	63488	8.8.8.8	192.168.2.5
May 16, 2022 21:27:04.165057898 CEST	57990	53	192.168.2.5	8.8.8.8
May 16, 2022 21:27:04.181545019 CEST	53	57990	8.8.8.8	192.168.2.5
May 16, 2022 21:27:09.603466988 CEST	54463	53	192.168.2.5	8.8.8.8
May 16, 2022 21:27:09.621463060 CEST	53	54463	8.8.8.8	192.168.2.5
May 16, 2022 21:27:18.219963074 CEST	49416	53	192.168.2.5	8.8.8.8
May 16, 2022 21:27:18.238219976 CEST	53	49416	8.8.8.8	192.168.2.5
May 16, 2022 21:27:25.108907938 CEST	54152	53	192.168.2.5	8.8.8.8
May 16, 2022 21:27:25.128952980 CEST	53	54152	8.8.8.8	192.168.2.5
May 16, 2022 21:27:31.198779106 CEST	54258	53	192.168.2.5	8.8.8.8
May 16, 2022 21:27:31.219415903 CEST	53	54258	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 16, 2022 21:25:52.718883991 CEST	192.168.2.5	8.8.8.8	0x9aa3	Standard query (0)	kingsley2022.bouncme.net	A (IP address)	IN (0x0001)
May 16, 2022 21:26:01.874166012 CEST	192.168.2.5	8.8.8.8	0x998b	Standard query (0)	kingsley2022.bouncme.net	A (IP address)	IN (0x0001)
May 16, 2022 21:26:09.506463051 CEST	192.168.2.5	8.8.8.8	0x5f35	Standard query (0)	kingsley2022.bouncme.net	A (IP address)	IN (0x0001)
May 16, 2022 21:26:16.193361998 CEST	192.168.2.5	8.8.8.8	0x3467	Standard query (0)	kingsley2022.bouncme.net	A (IP address)	IN (0x0001)
May 16, 2022 21:26:23.019675970 CEST	192.168.2.5	8.8.8.8	0xccf3	Standard query (0)	kingsley2022.bouncme.net	A (IP address)	IN (0x0001)
May 16, 2022 21:26:29.188756943 CEST	192.168.2.5	8.8.8.8	0x652	Standard query (0)	kingsley2022.bouncme.net	A (IP address)	IN (0x0001)
May 16, 2022 21:26:35.936079979 CEST	192.168.2.5	8.8.8.8	0x633a	Standard query (0)	kingsley2022.bouncme.net	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 16, 2022 21:26:42.222913980 CEST	192.168.2.5	8.8.8.8	0x1870	Standard query (0)	kingsley2022.bouncemee.net	A (IP address)	IN (0x0001)
May 16, 2022 21:26:48.281331062 CEST	192.168.2.5	8.8.8.8	0x273	Standard query (0)	kingsley2022.bouncemee.net	A (IP address)	IN (0x0001)
May 16, 2022 21:26:54.390856028 CEST	192.168.2.5	8.8.8.8	0x9ab3	Standard query (0)	kingsley2022.bouncemee.net	A (IP address)	IN (0x0001)
May 16, 2022 21:26:58.918062925 CEST	192.168.2.5	8.8.8.8	0x14ee	Standard query (0)	kingsley2022.bouncemee.net	A (IP address)	IN (0x0001)
May 16, 2022 21:27:04.165057898 CEST	192.168.2.5	8.8.8.8	0x8644	Standard query (0)	kingsley2022.bouncemee.net	A (IP address)	IN (0x0001)
May 16, 2022 21:27:09.603466988 CEST	192.168.2.5	8.8.8.8	0x5128	Standard query (0)	kingsley2022.bouncemee.net	A (IP address)	IN (0x0001)
May 16, 2022 21:27:18.219963074 CEST	192.168.2.5	8.8.8.8	0x1539	Standard query (0)	kingsley2022.bouncemee.net	A (IP address)	IN (0x0001)
May 16, 2022 21:27:25.108907938 CEST	192.168.2.5	8.8.8.8	0x698	Standard query (0)	kingsley2022.bouncemee.net	A (IP address)	IN (0x0001)
May 16, 2022 21:27:31.198779106 CEST	192.168.2.5	8.8.8.8	0x18ba	Standard query (0)	kingsley2022.bouncemee.net	A (IP address)	IN (0x0001)

DNS Answers

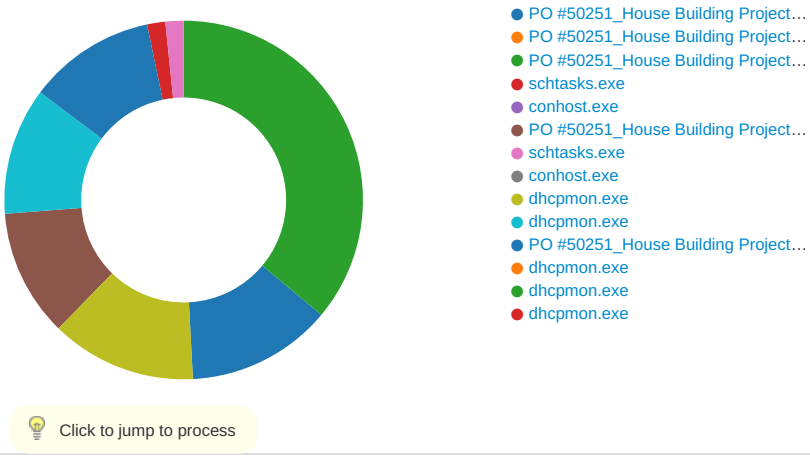
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 16, 2022 21:25:52.739039898 CEST	8.8.8.8	192.168.2.5	0x9aa3	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:26:01.892497063 CEST	8.8.8.8	192.168.2.5	0x998b	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:26:09.524383068 CEST	8.8.8.8	192.168.2.5	0x5f35	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:26:16.211782932 CEST	8.8.8.8	192.168.2.5	0x3467	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:26:23.039601088 CEST	8.8.8.8	192.168.2.5	0xccf3	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:26:29.209069967 CEST	8.8.8.8	192.168.2.5	0x652	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:26:35.954624891 CEST	8.8.8.8	192.168.2.5	0x633a	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:26:42.239293098 CEST	8.8.8.8	192.168.2.5	0x1870	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:26:48.297589064 CEST	8.8.8.8	192.168.2.5	0x273	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:26:54.407196045 CEST	8.8.8.8	192.168.2.5	0x9ab3	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:26:58.936566114 CEST	8.8.8.8	192.168.2.5	0x14ee	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:27:04.181545019 CEST	8.8.8.8	192.168.2.5	0x8644	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:27:09.621463060 CEST	8.8.8.8	192.168.2.5	0x5128	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:27:18.238219976 CEST	8.8.8.8	192.168.2.5	0x1539	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 16, 2022 21:27:25.128952980 CEST	8.8.8.8	192.168.2.5	0x698	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)
May 16, 2022 21:27:31.219415903 CEST	8.8.8.8	192.168.2.5	0x18ba	No error (0)	kingsley2022.bouncemee.net		62.197.136.29	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: PO #50251_House Building Project.exe PID: 6996, Parent PID: 5952

General

Target ID:	0
Start time:	21:25:24
Start date:	16/05/2022
Path:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO #50251_House Building Project.exe"
Imagebase:	0x820000
File size:	565248 bytes
MD5 hash:	08C261ADE5C2D31437DA373D90A2F6D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.471924697.0000000002E88000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.475865884.00000000073B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.471237534.0000000002BF3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.472184715.0000000003C98000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.472184715.0000000003C98000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.472184715.0000000003C98000.00000004.00000800.00020000.00000000.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	6E45CF06	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	6E45CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO #50251_House Building Project.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E76C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO #50251_House Building Project.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	6E76C907	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	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E435705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E43CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2A1B4F	ReadFile

Analysis Process: PO #50251_House Building Project.exe PID: **3968**, Parent PID: **6996**

General

Target ID:	2
Start time:	21:25:40
Start date:	16/05/2022
Path:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
Imagebase:	0x70000
File size:	565248 bytes
MD5 hash:	08C261ADE5C2D31437DA373D90A2F6D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PO #50251_House Building Project.exe PID: **4780**, Parent PID: **6996**

General

Target ID:	3
Start time:	21:25:41
Start date:	16/05/2022
Path:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
Imagebase:	0xdf0000
File size:	565248 bytes
MD5 hash:	08C261ADE5C2D31437DA373D90A2F6D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.703804511.0000000006A00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.703804511.0000000006A00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.703804511.0000000006A00000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.701420993.00000000045D1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.692313822.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.692313822.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.692313822.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.703829522.0000000006A10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.703829522.0000000006A10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.703829522.0000000006A10000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.703147351.0000000005BD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.703147351.0000000005BD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.703147351.0000000005BD0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.465095050.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.465095050.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.465095050.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.464706750.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.464706750.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.464706750.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source:

00000003.00000002.703450714.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.703450714.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.703450714.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.703450714.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.704203855.0000000007480000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.704203855.0000000007480000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.704203855.0000000007480000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.704263668.00000000074B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.704263668.00000000074B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.704263668.00000000074B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.700746857.0000000004331000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.704338683.0000000007500000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.704338683.0000000007500000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.704338683.0000000007500000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.703360663.0000000005C50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.703360663.0000000005C50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.703360663.0000000005C50000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.465505967.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.465505967.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000003.00000000.465505967.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.701249536.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.701249536.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.702930041.0000000005A10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.702930041.0000000005A10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.702930041.0000000005A10000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.704283187.00000000074C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.704283187.00000000074C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.704283187.00000000074C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.703292909.0000000005C20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.703292909.0000000005C20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.703292909.0000000005C20000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.703777042.00000000069F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.703777042.00000000069F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.703777042.00000000069F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.699082789.0000000003360000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.704222309.0000000007490000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.704222309.0000000007490000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.704222309.0000000007490000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.704185578.0000000007470000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.704185578.0000000007470000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.704185578.0000000007470000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.464221648.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.464221648.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000003.00000000.464221648.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.698957935.00000000032E1000.00000004.00000800.00020000.00000000.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	6E45CF06	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	6E45CF06	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	6D2ABEFF	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	6D2A1E60	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	6D2ABEFF	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	6D2ADD66	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	6D2ADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpCD7F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D2A7038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D2A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpD6B8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D2A7038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D2ABEFF	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	6D2ABEFF	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	12	6D2A1E60	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	6D2A1E60	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	6D2A1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCD7F.tmp	success or wait	1	6D2A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpD6B8.tmp	success or wait	1	6D2A6A95	DeleteFileW
C:\Users\user\Desktop\PO #50251_House Building Project.exe:Zone.Identifier	success or wait	1	6D222935	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	7b 1a fd 4f fd 37 fd 48	{O7H	success or wait	1	6D2A1B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 34 52 fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 08 00 00 06 00 00 00 00 00 00 12 fd 08 00 00 20 00 00 00 fd 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 09 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL4Rb0 @ @	success or wait	3	6D2ADD66	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	6D2ADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpCD7F.tmp	0	1323	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" x mlns="http://schemas.mic rosoft .com/windows/2004/02/m it/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <Logon Type>InteractiveToken</ LogonType>	success or wait	1	6D2A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	60	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 50 4f 20 23 35 30 32 35 31 5f 48 6f 75 73 65 20 42 75 69 6c 64 69 6e 67 20 50 72 6f 6a 65 63 74 2e 65 78 65	C:\Users\user\Desktop\PO #50251_House Building Project.exe	success or wait	1	6D2A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpD6B8.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	6D2A1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	11	6D2A1B4F	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	6D2A1B4F	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 fd 16 fd fd 20 38 fd 6a fd fd fd fd 7c fd 26 58 fd fd 65 fd 46 fd 2a fd	9iH}Z4f 8j|&XeF*	success or wait	1	6D2A1B4F	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	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E435705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E43CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2A1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E41D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E41D72F	unknown
C:\Users\user\Desktop\PO #50251_House Building Project.exe	unknown	4096	success or wait	1	6E41D72F	unknown
C:\Users\user\Desktop\PO #50251_House Building Project.exe	unknown	512	success or wait	1	6E41D72F	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	6D2A646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **6520**, Parent PID: **4780**

General	
Target ID:	4
Start time:	21:25:47
Start date:	16/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpCD7F.tmp
Imagebase:	0x3b0000
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\tmpCD7F.tmp	unknown	2	success or wait	1	3BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCD7F.tmp	unknown	1324	success or wait	1	3BABD9	ReadFile

Analysis Process: conhost.exe PID: **6504**, Parent PID: **6520**

General	
Target ID:	5
Start time:	21:25:47
Start date:	16/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: PO #50251_House Building Project.exe PID: **5844**, Parent PID: **1040**

General	
Target ID:	6
Start time:	21:25:48
Start date:	16/05/2022
Path:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO #50251_House Building Project.exe" 0
Imagebase:	0x970000
File size:	565248 bytes
MD5 hash:	08C261ADE5C2D31437DA373D90A2F6D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.528918008.0000000003128000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000006.00000002.539423206.0000000007120000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.530909891.0000000003F38000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.530909891.0000000003F38000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.530909891.0000000003F38000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.527589844.0000000002E93000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E45CF06	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	6E45CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E435705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E43CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2A1B4F	ReadFile

Analysis Process: schtasks.exe PID: **4448**, Parent PID: **4780**

General

Target ID:	7
Start time:	21:25:49
Start date:	16/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpD6B8.tmp
Imagebase:	0x3b0000
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\tmpD6B8.tmp	unknown	2	success or wait	1	3BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD6B8.tmp	unknown	1311	success or wait	1	3BABD9	ReadFile

Analysis Process: conhost.exe PID: **1320**, Parent PID: **4448**

General

Target ID:	8
Start time:	21:25:50
Start date:	16/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **3960**, Parent PID: **1040**

General

Target ID:	10
Start time:	21:25:53
Start date:	16/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x780000
File size:	565248 bytes
MD5 hash:	08C261ADE5C2D31437DA373D90A2F6D0
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: 0000000A.00000002.543087362.0000000002C43000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 0000000A.00000002.557629085.0000000006D50000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.546348410.0000000003CE8000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.546348410.0000000003CE8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.546348410.0000000003CE8000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.544519531.0000000002ED8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	6E45CF06	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	6E45CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E76C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	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	6E76C907	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	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E435705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E43CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2A1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **6696**, Parent PID: **684**

Copyright Joe Security LLC 2022

General	
Target ID:	12
Start time:	21:26:00
Start date:	16/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xe70000
File size:	565248 bytes
MD5 hash:	08C261ADE5C2D31437DA373D90A2F6D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 0000000C.00000002.574005491.0000000007630000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.561626893.0000000004378000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.561626893.0000000004378000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.561626893.0000000004378000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000C.00000002.555382708.00000000032D3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000C.00000002.560657971.0000000003568000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E45CF06	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	6E45CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E435705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E43CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2A1B4F	ReadFile

Analysis Process: PO #50251_House Building Project.exe PID: 6824, Parent PID: 5844

General

Target ID:	13
Start time:	21:26:02
Start date:	16/05/2022
Path:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO #50251_House Building Project.exe
Imagebase:	0xc90000
File size:	565248 bytes
MD5 hash:	08C261ADE5C2D31437DA373D90A2F6D0
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: 0000000D.00000000.517190067.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.517190067.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.517190067.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.544585450.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.544585450.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.544585450.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.516442509.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.516442509.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.516442509.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.514937741.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.514937741.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.514937741.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.551950556.0000000004149000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.551950556.0000000004149000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.518826428.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.518826428.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.518826428.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.550459008.0000000003141000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.550459008.0000000003141000.00000004.00000800.00020000.00000000.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	6E45CF06	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	6E45CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E435705	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E43CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E435705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2A1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **4356**, Parent PID: **3960**

General

Target ID:	15
Start time:	21:26:08
Start date:	16/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x2f0000
File size:	565248 bytes
MD5 hash:	08C261ADE5C2D31437DA373D90A2F6D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: **5996**, Parent PID: **3960**

General

Target ID:	16
Start time:	21:26:11
Start date:	16/05/2022
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:	565248 bytes
MD5 hash:	08C261ADE5C2D31437DA373D90A2F6D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.577659438.0000000003DE9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.577659438.0000000003DE9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.573309326.0000000002DE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.573309326.0000000002DE1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.537506951.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.537506951.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.537506951.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.564816059.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.564816059.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.564816059.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.538397447.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.538397447.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.538397447.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.536899320.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.536899320.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.536899320.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.535757135.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.535757135.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.535757135.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: **5696**, Parent PID: **6696**

General

Target ID:	17
Start time:	21:26:14
Start date:	16/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x7e0000
File size:	565248 bytes
MD5 hash:	08C261ADE5C2D31437DA373D90A2F6D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.544772648.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.544772648.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.544772648.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.577502934.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.577502934.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.577502934.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.580453884.0000000003C69000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.580453884.0000000003C69000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.580254552.0000000002C61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.580254552.0000000002C61000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.544206014.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.544206014.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.544206014.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.542909394.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.542909394.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.542909394.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.541210561.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.541210561.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.541210561.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Disassembly

No disassembly