



ID: 710454
Sample Name: outstanding statement.exe
Cookbook: default.jbs
Time: 04:37:28
Date: 27/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report outstanding statement.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 6
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 6
AV Detection 6
E-Banking Fraud 6
Persistence and Installation Behavior 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Snort Signatures 7
Joe Sandbox Signatures 9
AV Detection 9
Networking 9
E-Banking Fraud 9
System Summary 9
Data Obfuscation 9
Boot Survival 9
Hooking and other Techniques for Hiding and Protection 9
Malware Analysis System Evasion 10
HIPS / PFW / Operating System Protection Evasion 10
Stealing of Sensitive Information 10
Remote Access Functionality 10
Mitre Att&ck Matrix 10
Behavior Graph 10
Screenshots 11
Thumbnails 11
Antivirus, Machine Learning and Genetic Malware Detection 12
Initial Sample 12
Dropped Files 12
Unpacked PE Files 13
Domains 13
URLs 13
Domains and IPs 13
Contacted Domains 13
URLs from Memory and Binaries 13
World Map of Contacted IPs 16
Public IPs 16
General Information 16
Warnings 17
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASNs 18
JA3 Fingerprints 18
Dropped Files 18
Created / dropped Files 18
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe 18
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier 18
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log 18
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\outstanding statement.exe.log 19
C:\Users\user\AppData\Local\Temp\tmp27F3.tmp 19
C:\Users\user\AppData\Local\Temp\tmp29F7.tmp 19
C:\Users\user\AppData\Local\Temp\tmp6644.tmp 20
C:\Users\user\AppData\Local\Temp\tmp949C.tmp 20
C:\Users\user\AppData\Local\Temp\tmpAB73.tmp 20
C:\Users\user\AppData\Local\Temp\tmpAEBF.tmp 21
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat 21
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 21
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin 22

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat 22
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat 22
C:\Users\user\AppData\Roaming\OIdzpXTWJYUnz.exe 22
Static File Info 23
General 23
File Icon 23
Static PE Info 23
General 23
Entrypoint Preview 24
Data Directories 25
Sections 25
Resources 26
Imports 26
Network Behavior 26
Snort IDS Alerts 26
Network Port Distribution 27
TCP Packets 27
UDP Packets 29
DNS Queries 29
DNS Answers 30
Statistics 30
Behavior 30
System Behavior 31
Analysis Process: outstanding statement.exePID: 5916, Parent PID: 2752 31
General 31
File Activities 31
File Created 31
File Deleted 32
File Written 32
File Read 33
Analysis Process: schtasks.exePID: 5316, Parent PID: 5916 33
General 33
File Activities 34
File Read 34
Analysis Process: conhost.exePID: 5392, Parent PID: 5316 34
General 34
Analysis Process: outstanding statement.exePID: 5468, Parent PID: 5916 34
General 34
File Activities 36
File Created 36
File Deleted 37
File Written 37
File Read 39
Registry Activities 40
Key Value Created 40
Analysis Process: schtasks.exePID: 5700, Parent PID: 5468 40
General 40
File Activities 40
File Read 40
Analysis Process: conhost.exePID: 5776, Parent PID: 5700 40
General 40
Analysis Process: schtasks.exePID: 5436, Parent PID: 5468 41
General 41
File Activities 41
File Read 41
Analysis Process: conhost.exePID: 3132, Parent PID: 5436 41
General 41
Analysis Process: outstanding statement.exePID: 5832, Parent PID: 1064 41
General 41
File Activities 42
File Created 42
File Deleted 42
File Written 42
File Read 42
Analysis Process: dhcpmon.exePID: 3068, Parent PID: 1064 43
General 43
File Activities 43
File Created 43
File Deleted 43
File Written 43
File Read 44
Analysis Process: svchost.exePID: 1276, Parent PID: 576 45
General 45
Analysis Process: dhcpmon.exePID: 5728, Parent PID: 3452 45
General 45
Analysis Process: schtasks.exePID: 3016, Parent PID: 5832 45
General 45
Analysis Process: conhost.exePID: 2208, Parent PID: 3016 46
General 46
Analysis Process: schtasks.exePID: 5788, Parent PID: 3068 46
General 46
Analysis Process: conhost.exePID: 4944, Parent PID: 5788 46
General 46
Analysis Process: outstanding statement.exePID: 5624, Parent PID: 5832 46
General 46
Analysis Process: dhcpmon.exePID: 4456, Parent PID: 3068 47
General 47
Analysis Process: outstanding statement.exePID: 1276, Parent PID: 5832 47
General 47
Analysis Process: dhcpmon.exePID: 2588, Parent PID: 3068 47
General 47

Analysis Process: dhcpmon.exePID: 6076, Parent PID: 3068 48
General 48
Analysis Process: dhcpmon.exePID: 4008, Parent PID: 3068 48
General 48
Analysis Process: schtasks.exePID: 2040, Parent PID: 5728 48
General 48
Analysis Process: conhost.exePID: 3380, Parent PID: 2040 49
General 49
Analysis Process: dhcpmon.exePID: 748, Parent PID: 5728 49
General 49
Disassembly 49

Copyright Joe Security LLC 2022

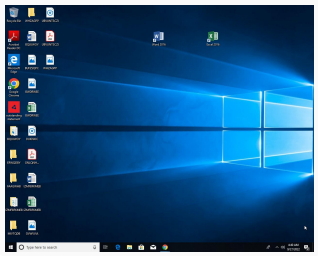
Windows Analysis Report

outstanding statement.exe

Overview

General Information

Sample Name:	outstanding statement.exe
Analysis ID:	710454
MD5:	c83f7860b0c0f1a..
SHA1:	221ba6cf88de4c...
SHA256:	94bcc238e29903..
Tags:	exe NanoCore
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

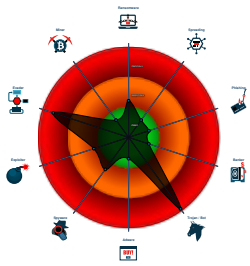
Nanocore

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- outstanding statement.exe (PID: 5916 cmdline: "C:\Users\user\Desktop\outstanding statement.exe" MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
  - schtasks.exe (PID: 5316 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\OldzpXTWJYUnz" /XML "C:\Users\user\AppData\Local\Temp\tmp949C.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - outstanding statement.exe (PID: 5468 cmdline: {path} MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
    - schtasks.exe (PID: 5700 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpAB73.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5436 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmpAEBF.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 3132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- outstanding statement.exe (PID: 5832 cmdline: "C:\Users\user\Desktop\outstanding statement.exe" 0 MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
  - svchost.exe (PID: 1276 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - schtasks.exe (PID: 3016 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\OldzpXTWJYUnz" /XML "C:\Users\user\AppData\Local\Temp\tmp27F3.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2208 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - outstanding statement.exe (PID: 5624 cmdline: {path} MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
  - outstanding statement.exe (PID: 1276 cmdline: {path} MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
- dhcpmon.exe (PID: 3068 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
  - schtasks.exe (PID: 5788 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\OldzpXTWJYUnz" /XML "C:\Users\user\AppData\Local\Temp\tmp29F7.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 4456 cmdline: {path} MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
  - dhcpmon.exe (PID: 2588 cmdline: {path} MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
  - dhcpmon.exe (PID: 6076 cmdline: {path} MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
  - dhcpmon.exe (PID: 4008 cmdline: {path} MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
- dhcpmon.exe (PID: 5728 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
  - schtasks.exe (PID: 2040 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\OldzpXTWJYUnz" /XML "C:\Users\user\AppData\Local\Temp\tmp6644.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 748 cmdline: {path} MD5: C83F7860B0C0F1AD76D8CA65C6BAD689)
- **cleanup**

Copyright Joe Security LLC 2022

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.303794652.0000000007101000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x227c:$a1: NanoCore.ClientPluginHost • 0x2257:$a2: NanoCore.ClientPlugin • 0x226d:$b4: IClientAppHost • 0x675c:$b7: LogClientException • 0x22a6:$b9: IClientLoggingHost
00000003.00000002.553210177.0000000007520000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
00000003.00000002.553210177.0000000007520000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b99:$x2: NanoCore.ClientPluginHost • 0x6bce:$s4: PipeCreated • 0x5b86:$s5: IClientLoggingHost
00000003.00000002.553210177.0000000007520000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x5b70:$x2: NanoCore.ClientPlugin • 0x5b99:$x3: NanoCore.ClientPluginHost • 0x5b61:$i3: IClientNetwork • 0x5b86:$i6: IClientLoggingHost • 0x5bb3:$i7: IClientNetworkHost • 0x59d4:$s1: ClientPlugin • 0x5b79:$s1: ClientPlugin • 0x5e84:$s2: EndPoint • 0x5e8d:$s3: IPAddress • 0x5e97:$s4: IPEndPoint
00000003.00000002.553210177.0000000007520000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x5b99:$a1: NanoCore.ClientPluginHost • 0x5b70:$a2: NanoCore.ClientPlugin • 0x5b86:$b9: IClientLoggingHost

Click to see the 97 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.outstanding statement.exe.40fe5cf.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1a53c:$x1: NanoCore.ClientPluginHost • 0x1a556:$x2: IClientNetworkHost
3.2.outstanding statement.exe.40fe5cf.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1a53c:$x2: NanoCore.ClientPluginHost • 0x1d879:$s4: PipeCreated • 0x1a529:$s5: IClientLoggingHost
3.2.outstanding statement.exe.40fe5cf.5.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x1a513:$x2: NanoCore.ClientPlugin • 0x1a53c:$x3: NanoCore.ClientPluginHost • 0x1a504:$i3: IClientNetwork • 0x1a529:$i6: IClientLoggingHost • 0x1a556:$i7: IClientNetworkHost • 0x1a569:$i8: IClientUIHost • 0x1a273:$s1: ClientPlugin • 0x1a51c:$s1: ClientPlugin
3.2.outstanding statement.exe.40fe5cf.5.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x1a53c:$a1: NanoCore.ClientPluginHost • 0x1a513:$a2: NanoCore.ClientPlugin • 0x1f567:$b7: LogClientException • 0x1a529:$b9: IClientLoggingHost
3.2.outstanding statement.exe.756e8a4.28.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10937:$x1: NanoCore.ClientPluginHost • 0x10951:$x2: IClientNetworkHost

Click to see the 242 entries

Sigma Signatures

AV Detection



Sigma detected: NanoCore

E-Banking Fraud



Sigma detected: NanoCore

Persistence and Installation Behavior



Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information



Sigma detected: NanoCore

Remote Access Functionality



Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194

Timestamp:	192.168.2.6185.216.71.1944972010102816766 09/27/22-04:38:51.977418
SID:	2816766
Source Port:	49720
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.216.71.194 - Destination IP: 192.168.2.6

Timestamp:	185.216.71.194192.168.2.61010497442841753 09/27/22-04:40:41.029927
SID:	2841753
Source Port:	1010
Destination Port:	49744
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194

Timestamp:	192.168.2.6185.216.71.1944972510102816766 09/27/22-04:39:42.842313
SID:	2816766
Source Port:	49725
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194

Timestamp:	192.168.2.6185.216.71.1944972310102816766 09/27/22-04:39:17.707266
SID:	2816766
Source Port:	49723
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194

Timestamp:	192.168.2.6185.216.71.1944972710102816766 09/27/22-04:39:59.267095
SID:	2816766
Source Port:	49727
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.216.71.194 - Destination IP: 192.168.2.6

Timestamp:	185.216.71.194192.168.2.61010497382841753 09/27/22-04:40:20.888739

SID:	2841753
Source Port:	1010
Destination Port:	49738
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194	
Timestamp:	192.168.2.6185.216.71.1944973410102816766 09/27/22-04:40:15.599094
SID:	2816766
Source Port:	49734
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194	
Timestamp:	192.168.2.6185.216.71.1944972610102816766 09/27/22-04:39:50.710998
SID:	2816766
Source Port:	49726
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194	
Timestamp:	192.168.2.6185.216.71.1944972210102816766 09/27/22-04:39:10.006149
SID:	2816766
Source Port:	49722
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194	
Timestamp:	192.168.2.6185.216.71.1944972410102816766 09/27/22-04:39:26.449893
SID:	2816766
Source Port:	49724
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194	
Timestamp:	192.168.2.6185.216.71.1944972410102816718 09/27/22-04:39:26.449893
SID:	2816718
Source Port:	49724
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194	
Timestamp:	192.168.2.6185.216.71.1944972110102816766 09/27/22-04:39:02.212727
SID:	2816766
Source Port:	49721
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194	
Timestamp:	192.168.2.6185.216.71.1944973010102816766 09/27/22-04:40:04.752952
SID:	2816766
Source Port:	49730
Destination Port:	1010
Protocol:	TCP

Copyright Joe Security LLC 2022

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194	
Timestamp:	192.168.2.6185.216.71.194497381010281676 6 09/27/22-04:40:20.889307
SID:	2816766
Source Port:	49738
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 185.216.71.194	
Timestamp:	192.168.2.6185.216.71.194497441010281676 6 09/27/22-04:40:27.214840
SID:	2816766
Source Port:	49744
Destination Port:	1010
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking



Snort IDS alert for network traffic

Uses dynamic DNS services

E-Banking Fraud



Yara detected Nanocore RAT

System Summary



Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation



.NET source code contains potential unpacker

Boot Survival



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

Hooking and other Techniques for Hiding and Protection



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

Malware Analysis System Evasion



Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion



Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected Nanocore RAT

Remote Access Functionality



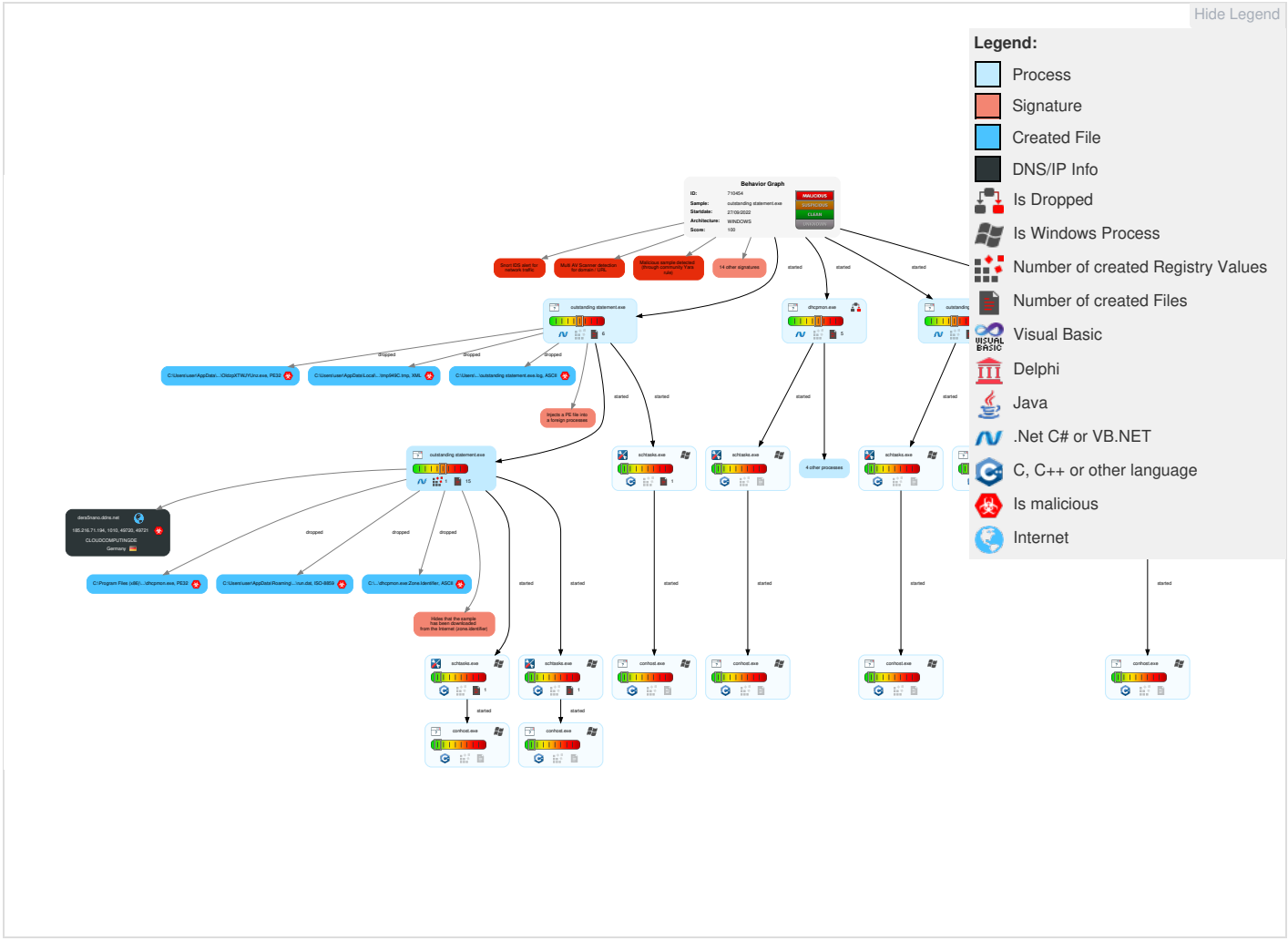
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

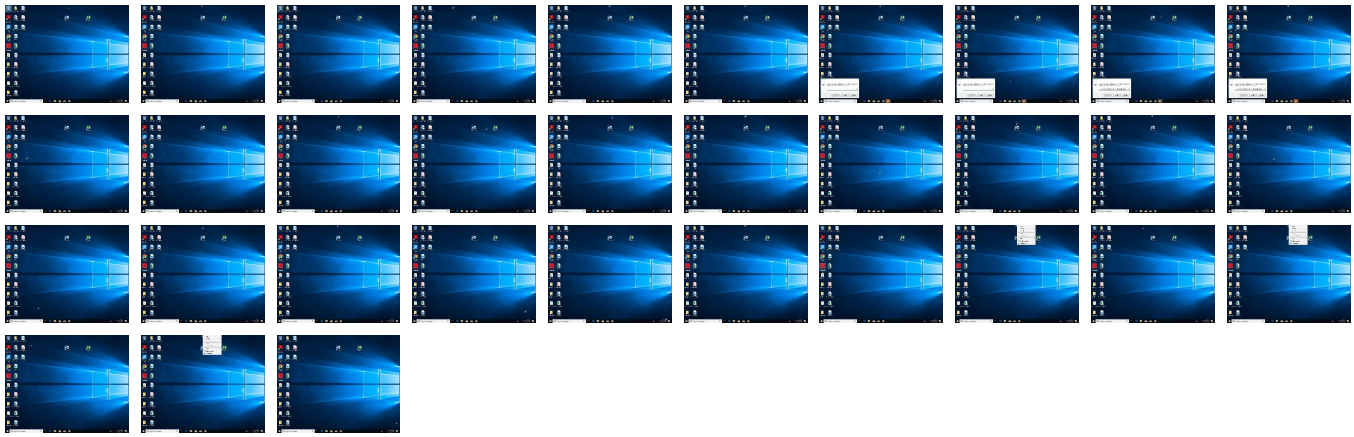
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
outstanding statement.exe	81%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
outstanding statement.exe	36%	Virustotal		Browse
outstanding statement.exe	36%	Metadefender		Browse
outstanding statement.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\OldzpXTWJYUnz.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	81%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	36%	Metadefender		Browse
C:\Users\user\AppData\Roaming\OldzpXTWJYUnz.exe	81%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\OldzpXTWJYUnz.exe	36%	Metadefender		Browse

Copyright Joe Security LLC 2022

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.outstanding statement.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.outstanding statement.exe.5a50000.16.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
dera5nano.ddns.net	14%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://en.w	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.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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cns-m	0%	URL Reputation	safe	
http://www.fontbureau.com2F	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.fonts.comic~	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTFqFV	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/in	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnrin	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnus	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnlQ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dera5nano.ddns.net	185.216.71.194	true	true	• 14%, Virustotal, Browse	unknown

URLs from Memory and Binaries

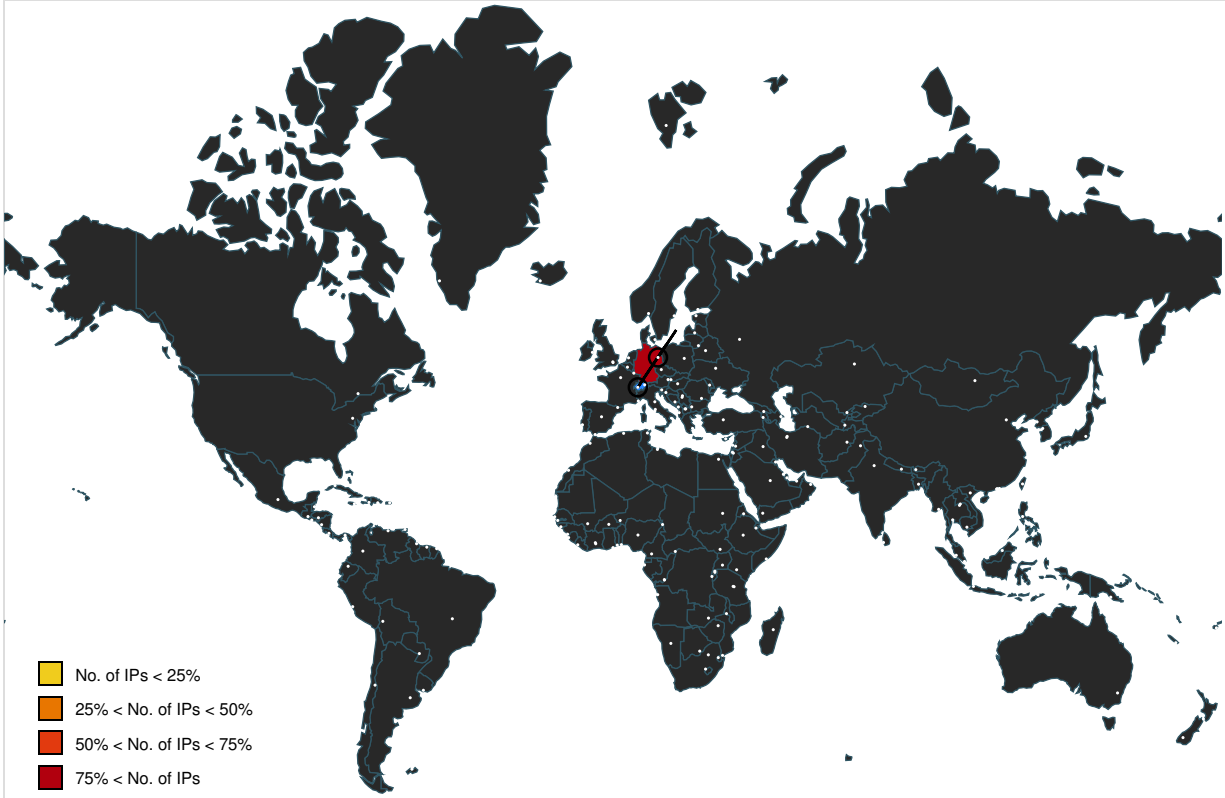
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000000.00000003.250798345.0 000000005983000.00000004.00000800.000200 00.00000000.sdmp	false		high
http://www.fontbureau.com	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com2F	outstanding statement.exe, 00000000.0000 0002.283923620.0000000000E77000.00000004 .00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000000.00000003.246447193.0 000000005981000.00000004.00000800.000200 00.00000000.sdmp, outstanding statement.exe, 00000 000.00000003.246469625.0000000005982000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comic~	outstanding statement.exe, 00000000.0000 0003.245987301.0000000005983000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	outstanding statement.exe, 00000003.0000 0002.540669244.00000000041C0000.00000004 .00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000003.00000002.552972970.0 0000000073C0000.00000004.08000000.000400 00.00000000.sdmp, outstanding statement.exe, 00000 003.00000002.530140440.0000000003149000. 00000004.00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000003.00000002.544 886157.00000000043DE000.00000004.0000080 0.00020000.00000000.sdmp	false		high
http://en.w	outstanding statement.exe, 00000000.0000 0003.251131135.0000000005980000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000000.00000003.248775625.0 000000005983000.00000004.00000800.000200 00.00000000.sdmp, outstanding statement.exe, 00000 000.00000003.249051684.0000000005983000. 00000004.00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000000.00000003.249 356882.000000000596B000.00000004.0000080 0.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comB.TTFqFV	outstanding statement.exe, 00000000.0000 0002.283923620.0000000000E77000.00000004 .00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como	outstanding statement.exe, 00000000.0000 0002.283923620.0000000000E77000.00000004 .00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnrin	outstanding statement.exe, 00000000.0000 0003.248775625.0000000005983000.00000004 .00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000000.00000003.249051684.0 000000005983000.00000004.00000800.000200 00.00000000.sdmp, outstanding statement.exe, 00000 000.00000003.249238521.0000000005984000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000000.00000003.245987301.0 000000005983000.00000004.00000800.000200 00.00000000.sdmp	false		high
http://www.founder.com.cn/cn/in	outstanding statement.exe, 00000000.0000 0003.250157695.0000000005983000.00000004 .00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000000.00000003.250061609.0 000000005983000.00000004.00000800.000200 00.00000000.sdmp, outstanding statement.exe, 00000 000.00000003.249824948.0000000005983000. 00000004.00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000000.00000003.250 228496.0000000005983000.00000004.0000080 0.00020000.00000000.sdmp, outstanding st atement.exe, 00000000.00000003.250441527 .0000000005983000.00000004.00000800.0002 0000.00000000.sdmp, outstanding statement.exe, 000 00000.00000003.249574322.000000000598100 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cns-m	outstanding statement.exe, 00000000.0000 0003.248304884.0000000005969000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	outstanding statement.exe, 00000000.0000 0002.298411409.0000000006C02000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	outstanding statement.exe, 00000000.00000002.284266217.00000000029E1000.00000004.00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000003.00000002.530140440.000000003149000.00000004.00000800.00020000.00000000.sdmp, outstanding statement.exe, 00000010.00000002.370377892.000000000268D000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000011.00000002.379481668.0000000002511000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000015.00000002.421885929.000000000263D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnlQ	outstanding statement.exe, 00000000.00000003.249051684.0000000005983000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	outstanding statement.exe, 00000000.00000002.298411409.000000006C02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnus	outstanding statement.exe, 00000000.00000003.248304884.0000000005969000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnd	outstanding statement.exe, 00000000.00000003.248362376.0000000005966000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.216.71.194	dera5nano.ddns.net	Germany		43659	CLOUDCOMPUTINGDE	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	710454
Start date and time:	2022-09-27 04:37:28 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 23s

Copyright Joe Security LLC 2022

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	outstanding statement.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	42
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@39/16@12/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com, login.live.com, displaycatalog.mp.microsoft.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:38:31	API Interceptor	797x Sleep call for process: outstanding statement.exe modified
04:38:46	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\outstanding statement.exe" s>$(Arg0)
04:38:46	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
04:38:48	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
04:39:05	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\outstanding statement.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	764928
Entropy (8bit):	6.890085708700623
Encrypted:	false
SSDEEP:	12288:PHK2xwKKFbHecmpYAf6GZPVNzBKUcY4oqwlsLhARylQ:/KvHBu1iizgUcGqwlsL+E
MD5:	C83F7860B0C0F1AD76D8CA65C6BAD689
SHA1:	221BA6CF88DE4C688583C69E8892EC9C3804A11E
SHA-256:	94BCC238E29903CC49036DA98144DAE0C7E10526669D6C50E3B87239F8E27262
SHA-512:	B0D67DC5E4F1BFDEFD3785C33088823FABF690107B58B9EFA88C617FE2C1F679B651E7826187106B5F8F4E5B44D4B92FF7D3B9E247A908E1DDC6591FB00C830 7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 81% • Antivirus: Metadefender, Detection: 36%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....+c.....P..... ....@.. ....@.....O.....\|..... ....H.....text...d.... ....`.rsrc...\|.....@..@.reloc..... .....@..B.....H.....d.....8...._...O.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~....o %....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....().....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r/..p~....o-... (.....t$....+..*...0..&.....(....r;..p~....o-...(.....

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

Process:	C:\Users\user\Desktop\outstanding statement.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859

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

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

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

C:\Users\user\AppData\Local\Temp\tmp27F3.tmp

Process:	C:\Users\user\Desktop\outstanding statement.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1658
Entropy (8bit):	5.173145396065913
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3QVtn:cbha7JlNQV/rydbz9I3YODOLNdq3e
MD5:	045EF4AD13327F636AD990FB75EF4745
SHA1:	B3F2D1C045FD1FB74B4CDB696CAA24131608581F
SHA-256:	51451DA82167F1BDA0611EBCCC730E04637D6F4E8EE59723D7C98864561DBD5F
SHA-512:	EB522B1E1307F8AB1650EA237C495CA4467878063D1BA13319E3235553BF5780325566E402FDE1DB38C0D41754AAED91813C7E8C340837E442C8F311DFEA6826
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmp29F7.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1658
Entropy (8bit):	5.173145396065913
Encrypted:	false

SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKB3QVtn:cbha7JlNQV/rydbz9I3YODOLNdq3e
MD5:	045EF4AD13327F636AD990FB75EF4745
SHA1:	B3F2D1C045FD1FB74B4CDB696CAA24131608581F
SHA-256:	51451DA82167F1BDA0611EBCCC730E04637D6F4E8EE59723D7C98864561DBD5F
SHA-512:	EB522B1E1307F8AB1650EA237C495CA4467878063D1BA13319E3235553BF5780325566E402FDE1DB38C0D41754AAED91813C7E8C340837E442C8F311DFEA6826
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmp6644.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1658
Entropy (8bit):	5.173145396065913
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKB3QVtn:cbha7JlNQV/rydbz9I3YODOLNdq3e
MD5:	045EF4AD13327F636AD990FB75EF4745
SHA1:	B3F2D1C045FD1FB74B4CDB696CAA24131608581F
SHA-256:	51451DA82167F1BDA0611EBCCC730E04637D6F4E8EE59723D7C98864561DBD5F
SHA-512:	EB522B1E1307F8AB1650EA237C495CA4467878063D1BA13319E3235553BF5780325566E402FDE1DB38C0D41754AAED91813C7E8C340837E442C8F311DFEA6826
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmp949C.tmp

Process:	C:\Users\user\Desktop\outstanding statement.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1658
Entropy (8bit):	5.173145396065913
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKB3QVtn:cbha7JlNQV/rydbz9I3YODOLNdq3e
MD5:	045EF4AD13327F636AD990FB75EF4745
SHA1:	B3F2D1C045FD1FB74B4CDB696CAA24131608581F
SHA-256:	51451DA82167F1BDA0611EBCCC730E04637D6F4E8EE59723D7C98864561DBD5F
SHA-512:	EB522B1E1307F8AB1650EA237C495CA4467878063D1BA13319E3235553BF5780325566E402FDE1DB38C0D41754AAED91813C7E8C340837E442C8F311DFEA6826
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmpAB73.tmp

Process:	C:\Users\user\Desktop\outstanding statement.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.075456581526247
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0V7llxtn:cbk4oL600QydbQxIYODOLedq3Sj
MD5:	BD86622E7AE294D2E629D0CD70EB4F53
SHA1:	19390333CCBCA863F566D7C7D3C3072660C38639

SHA-256:	68268C47BB1D960EED8A842158FDACEEBD8FDAB2DA338187835483435BC1FAF8
SHA-512:	4D6743EA0AA23A22E694675BC0A4D548B8C4FFE65BC1D22626ED2D2737858CFC35F0875C6D2A7554B8C1CC4599D73B2AFA841E6101D2E8B0764C2178256B21E 0
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\outstanding statement.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733 4
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

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

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

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

Process:	C:\Users\user\Desktop\outstanding statement.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:zFl:L
MD5:	5D4F5C629F89ECD4603E80D69E56497C
SHA1:	F328E21FACD68DE538AB3327B30F245C7028D58D
SHA-256:	BCE23A45323D7F96C8C1424A2C765310C5FA219E1CD9EFCDF2E73AB1B1FBC72F
SHA-512:	FBDC364766F180C157B30C9F024D83BA7CB37E7171717EF173B490BD768CD4ACC166A6C971E5992E6376D6C03FB2C9D9E424FFD70DD5A0760F51B91F305C88 3

Malicious:	**true**
Preview:	..0.|..H

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

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

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

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

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

Process:	C:\Users\user\Desktop\outstanding statement.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	51
Entropy (8bit):	4.000692381850293
Encrypted:	false
SSDEEP:	3:oNN2+WKQNL62duRkAn:oNN2RKg6LRJn
MD5:	51437E707B7C1D7245E6728854ED4C9F
SHA1:	5771D153870F91E112DF11E958231EA1A8B7B9A7
SHA-256:	390D5FF71830498A4FBDA8CAC5C3A8CA0DDB743777C18957172B8BDF0836211E
SHA-512:	76EC1C431A17C0E1B8979A1076FBBDFBA1082D28BB8FDA2C7136997DD863CD3350DB1BFC0F1D7BED4743EDA3D1334011ED04590C9DF1D624223499467488CD
Malicious:	false
Preview:	C:\Users\user\Desktop\outstanding statement.exe

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

Process:	C:\Users\user\Desktop\outstanding statement.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	764928

Entropy (8bit):	6.890085708700623
Encrypted:	false
SSDEEP:	12288:PHK2xwKKFbHecmpYAf6GZPVNzBKUcY4oqwlsLhARylQ:/KvHBu1iizgUcGqwlsL+E
MD5:	C83F7860B0C0F1AD76D8CA65C6BAD689
SHA1:	221BA6CF88DE4C688583C69E8892EC9C3804A11E
SHA-256:	94BCC238E29903CC49036DA98144DAE0C7E10526669D6C50E3B87239F8E27262
SHA-512:	B0D67DC5E4F1BFDEFD3785C33088823FABF690107B58B9EFA88C617FE2C1F679B651E7826187106B5F8F4E5B44D4B92FF7D3B9E247A908E1DDC6591FB00C830 7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 81% • Antivirus: Metadefender, Detection: 36%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....+c.....P..... .....@.. ....@.....O.....\|..... ....H.....text...d.... ....`.rsrc...\|.....@..@.reloc..... .....@..B.....H.....d.....8...._...O.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~....o %....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....().....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*"".....*.0..&.....(....r/..p~....o-... (.....t$....+..*...0..&.....(....r,..p~....o-...(.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.890085708700623
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	outstanding statement.exe
File size:	764928
MD5:	c83f7860b0c0f1ad76d8ca65c6bad689
SHA1:	221ba6cf88de4c688583c69e8892ec9c3804a11e
SHA256:	94bcc238e29903cc49036da98144dae0c7e10526669d6c50e3b87239f8e27262
SHA512:	b0d67dc5e4f1bfdefd3785c33088823fabf690107b58b9efa88c617fe2c1f679b651e7826187106b5f8f4e5b44d4b92ff7d3b9e247a908e1ddc6591fb00c8307
SSDEEP:	12288:PHK2xwKKFbHecmpYAf6GZPVNzBKUcY4oqwlsLhARylQ:/KvHBu1iizgUcGqwlsL+E
TLSH:	F4F42A2425EB521CF4765FE95FC8B8FA499BFE61662AA0F628E073458B33E04CDD1035
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....+c.....P..... .....@.. .....@.....

File Icon



Icon Hash:	0030484e96986000

Static PE Info

General

Entrypoint:	0x4bb01e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x632BD8FA [Thu Sep 22 03:39:38 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0

Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview
Instruction
jmp dword ptr [00402000h]
out 27h, al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
sub eax, 33333340h
xor esi, dword ptr [ebx]
cmp eax, 00000040h
add byte ptr [eax], al
xor byte ptr [edx], 00000040h
xor esi, dword ptr [ebx]
xor esi, dword ptr [ebx]
xor esi, ebx
cmp eax, 00000040h
add byte ptr [eax], al
add byte ptr [edi], ah
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
sub eax, 66666640h
out 29h, al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbafcc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x147c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb9064	0xb9200	False	0.632404994513842	data	6.89608219692869	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x147c	0x1600	False	0.6782670454545454	data	6.473901803583799	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbc100	0xdf0	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xbcf00	0x14	data		
RT_VERSION	0xbcf24	0x358	data		
RT_MANIFEST	0xbd28c	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6185.216.71.19 44972010102816766 09/27/22-04:38:51.977418	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49720	1010	192.168.2.6	185.216.71.194
185.216.71.194192.168.2.61010497442841753 09/27/22-04:40:41.029927	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1010	49744	185.216.71.194	192.168.2.6
192.168.2.6185.216.71.19 44972510102816766 09/27/22-04:39:42.842313	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49725	1010	192.168.2.6	185.216.71.194
192.168.2.6185.216.71.19 44972310102816766 09/27/22-04:39:17.707266	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49723	1010	192.168.2.6	185.216.71.194
192.168.2.6185.216.71.19 44972710102816766 09/27/22-04:39:59.267095	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49727	1010	192.168.2.6	185.216.71.194
185.216.71.194192.168.2.61010497382841753 09/27/22-04:40:20.888739	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1010	49738	185.216.71.194	192.168.2.6
192.168.2.6185.216.71.19 44973410102816766 09/27/22-04:40:15.599094	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49734	1010	192.168.2.6	185.216.71.194
192.168.2.6185.216.71.19 44972610102816766 09/27/22-04:39:50.710998	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49726	1010	192.168.2.6	185.216.71.194
192.168.2.6185.216.71.19 44972210102816766 09/27/22-04:39:10.006149	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49722	1010	192.168.2.6	185.216.71.194

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6185.216.71.19 44972410102816766 09/27/22-04:39:26.449893	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49724	1010	192.168.2.6	185.216.71.194
192.168.2.6185.216.71.19 44972410102816718 09/27/22-04:39:26.449893	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49724	1010	192.168.2.6	185.216.71.194
192.168.2.6185.216.71.19 44972110102816766 09/27/22-04:39:02.212727	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49721	1010	192.168.2.6	185.216.71.194
192.168.2.6185.216.71.19 44973010102816766 09/27/22-04:40:04.752952	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49730	1010	192.168.2.6	185.216.71.194
192.168.2.6185.216.71.19 44973810102816766 09/27/22-04:40:20.889307	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49738	1010	192.168.2.6	185.216.71.194
192.168.2.6185.216.71.19 44974410102816766 09/27/22-04:40:27.214840	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49744	1010	192.168.2.6	185.216.71.194

Network Port Distribution



Total Packets: 48

- 53 (DNS)
- 1010 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 27, 2022 04:38:48.880903006 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:48.909274101 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:48.909415960 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.190139055 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.245604038 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.397131920 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.419725895 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.448052883 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.595479012 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.673928022 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.674000978 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.746371031 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.746431112 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.746457100 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.746478081 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.746567011 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.776268005 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.776321888 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.776361942 CEST	1010	49720	185.216.71.194	192.168.2.6

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 27, 2022 04:38:49.776397943 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.776401997 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.776434898 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.776443005 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.776472092 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.776509047 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.776520967 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.776547909 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.776588917 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.804235935 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804466963 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804524899 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804570913 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804591894 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.804620028 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804639101 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.804667950 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804713964 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804717064 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.804763079 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804805994 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804807901 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.804851055 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804892063 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.804900885 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804944992 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804990053 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.804990053 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.805037975 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.805083036 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.805083990 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.805130959 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.805175066 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.833092928 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833158970 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833205938 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833230019 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.833260059 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833304882 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833306074 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.833349943 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833394051 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833400011 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.833436966 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833477974 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.833479881 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833523989 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833566904 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.833566904 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833612919 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833657026 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833659887 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.833699942 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833741903 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.833744049 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833787918 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833830118 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.833831072 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833874941 CEST	1010	49720	185.216.71.194	192.168.2.6

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 27, 2022 04:38:49.833918095 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833929062 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.833962917 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.833997011 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.834007025 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834052086 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834089041 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.834095001 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834137917 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834197044 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834199905 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.834239960 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834278107 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.834286928 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834331989 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834373951 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.834374905 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834420919 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834461927 CEST	49720	1010	192.168.2.6	185.216.71.194
Sep 27, 2022 04:38:49.834465027 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834510088 CEST	1010	49720	185.216.71.194	192.168.2.6
Sep 27, 2022 04:38:49.834548950 CEST	49720	1010	192.168.2.6	185.216.71.194

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 27, 2022 04:38:48.835799932 CEST	49448	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:38:48.857659101 CEST	53	49448	8.8.8.8	192.168.2.6
Sep 27, 2022 04:39:01.514961958 CEST	59082	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:39:01.534094095 CEST	53	59082	8.8.8.8	192.168.2.6
Sep 27, 2022 04:39:08.802707911 CEST	59504	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:39:08.820116043 CEST	53	59504	8.8.8.8	192.168.2.6
Sep 27, 2022 04:39:15.311350107 CEST	65198	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:39:15.331537962 CEST	53	65198	8.8.8.8	192.168.2.6
Sep 27, 2022 04:39:24.042071104 CEST	62910	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:39:24.061443090 CEST	53	62910	8.8.8.8	192.168.2.6
Sep 27, 2022 04:39:41.273905993 CEST	63863	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:39:41.295010090 CEST	53	63863	8.8.8.8	192.168.2.6
Sep 27, 2022 04:39:48.864797115 CEST	63229	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:39:48.881758928 CEST	53	63229	8.8.8.8	192.168.2.6
Sep 27, 2022 04:39:57.631242990 CEST	62538	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:39:57.653517008 CEST	53	62538	8.8.8.8	192.168.2.6
Sep 27, 2022 04:40:03.645433903 CEST	56122	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:40:03.663759947 CEST	53	56122	8.8.8.8	192.168.2.6
Sep 27, 2022 04:40:11.879111052 CEST	53943	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:40:11.898736000 CEST	53	53943	8.8.8.8	192.168.2.6
Sep 27, 2022 04:40:20.785633087 CEST	58917	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:40:20.802773952 CEST	53	58917	8.8.8.8	192.168.2.6
Sep 27, 2022 04:40:25.943315983 CEST	55629	53	192.168.2.6	8.8.8.8
Sep 27, 2022 04:40:25.964725971 CEST	53	55629	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 27, 2022 04:38:48.835799932 CEST	192.168.2.6	8.8.8.8	0x93fd	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:01.514961958 CEST	192.168.2.6	8.8.8.8	0x42d4	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:08.802707911 CEST	192.168.2.6	8.8.8.8	0xdd4c	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2022

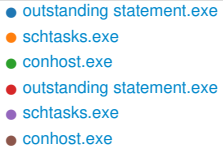
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 27, 2022 04:39:15.311350107 CEST	192.168.2.6	8.8.8.8	0x6ecc	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:24.042071104 CEST	192.168.2.6	8.8.8.8	0x532e	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:41.273905993 CEST	192.168.2.6	8.8.8.8	0xc0cf	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:48.864797115 CEST	192.168.2.6	8.8.8.8	0xa069	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:57.631242990 CEST	192.168.2.6	8.8.8.8	0x95a4	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:40:03.645433903 CEST	192.168.2.6	8.8.8.8	0xbe03	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:40:11.879111052 CEST	192.168.2.6	8.8.8.8	0xc4a3	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:40:20.785633087 CEST	192.168.2.6	8.8.8.8	0x6b77	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:40:25.943315983 CEST	192.168.2.6	8.8.8.8	0x8778	Standard query (0)	dera5nano.ddns.net	A (IP address)	IN (0x0001)	false

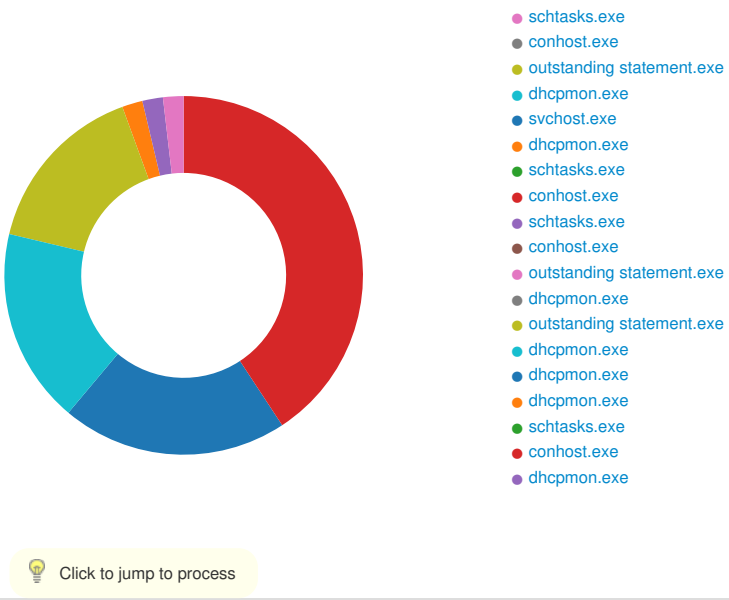
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 27, 2022 04:38:48.857659101 CEST	8.8.8.8	192.168.2.6	0x93fd	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:01.534094095 CEST	8.8.8.8	192.168.2.6	0x42d4	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:08.820116043 CEST	8.8.8.8	192.168.2.6	0xdd4c	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:15.331537962 CEST	8.8.8.8	192.168.2.6	0x6ecc	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:24.061443090 CEST	8.8.8.8	192.168.2.6	0x532e	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:41.295010090 CEST	8.8.8.8	192.168.2.6	0xc0cf	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:48.881758928 CEST	8.8.8.8	192.168.2.6	0xa069	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:39:57.653517008 CEST	8.8.8.8	192.168.2.6	0x95a4	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:40:03.663759947 CEST	8.8.8.8	192.168.2.6	0xbe03	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:40:11.898736000 CEST	8.8.8.8	192.168.2.6	0xc4a3	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:40:20.802773952 CEST	8.8.8.8	192.168.2.6	0x6b77	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false
Sep 27, 2022 04:40:25.964725971 CEST	8.8.8.8	192.168.2.6	0x8778	No error (0)	dera5nano.ddns.net		185.216.71.194	A (IP address)	IN (0x0001)	false

Statistics

Behavior





System Behavior

Analysis Process: outstanding statement.exe PID: **5916**, Parent PID: **2752**

General

Target ID:	0
Start time:	04:38:21
Start date:	27/09/2022
Path:	C:\Users\user\Desktop\outstanding statement.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\outstanding statement.exe"
Imagebase:	0x610000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.290409484.0000000003B17000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.290409484.0000000003B17000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.290409484.0000000003B17000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.290409484.0000000003B17000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D86CF06	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	6D86CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\OldzpXTWJYUnz.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6B1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp949C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C6B7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\outstanding statement.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DB7C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp949C.tmp	success or wait	1	6C6B6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\OldzpXTWJYUnz.exe	0	764928	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\outstanding statement.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DB7C907	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	6D845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D845705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D84CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6B1B4F	ReadFile
C:\Users\user\Desktop\outstanding statement.exe	unknown	764928	success or wait	1	6C6B1B4F	ReadFile

Analysis Process: schtasks.exe PID: **5316**, Parent PID: **5916**

General

Target ID:	1
Start time:	04:38:34
Start date:	27/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\OldzpXTWJYUnz" /XML "C:\Users\user\AppData\Local\Temp\tmp949C.tmp
Imagebase:	0x1220000
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\tmp949C.tmp	unknown	2	success or wait	1	122AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp949C.tmp	unknown	1659	success or wait	1	122ABD9	ReadFile

Analysis Process: conhost.exe PID: **5392**, Parent PID: **5316**

General

Target ID:	2
Start time:	04:38:35
Start date:	27/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: outstanding statement.exe PID: **5468**, Parent PID: **5916**

General

Target ID:	3
Start time:	04:38:35
Start date:	27/09/2022
Path:	C:\Users\user\Desktop\outstanding statement.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xbe0000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000003.303794652.0000000007101000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.553210177.0000000007520000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.553210177.0000000007520000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.553210177.0000000007520000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.553210177.0000000007520000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.552823390.00000000073A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.552823390.00000000073A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.552823390.00000000073A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.552823390.00000000073A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.552462673.0000000007230000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.552462673.0000000007230000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.552462673.0000000007230000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.552462673.0000000007230000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.553773435.0000000007560000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.553773435.0000000007560000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.553773435.0000000007560000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.553773435.0000000007560000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.552108671.0000000007200000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.552108671.0000000007200000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.552108671.0000000007200000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.552108671.0000000007200000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.552972970.00000000073C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.552972970.00000000073C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.552972970.00000000073C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.552972970.00000000073C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.540669244.00000000041C0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.540669244.00000000041C0000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.540669244.00000000041C0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.271120372.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.271120372.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000003.00000000.271120372.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000000.271120372.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.553109432.00000000073D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.553109432.00000000073D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.553109432.00000000073D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.553109432.00000000073D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.552899559.00000000073B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.552899559.00000000073B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.552899559.00000000073B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.552899559.00000000073B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.539716386.00000000040F1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.552699108.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.552699108.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.552699108.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.552699108.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.530140440.0000000003149000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.530140440.0000000003149000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.554089363.0000000007590000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.554089363.0000000007590000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.554089363.0000000007590000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.554089363.0000000007590000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.548985482.0000000005A50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.548985482.0000000005A50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.548985482.0000000005A50000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.548985482.0000000005A50000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen

	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.548985482.0000000005A50000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.550294873.0000000006AA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.550294873.0000000006AA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.550294873.0000000006AA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.550294873.0000000006AA0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.548939987.0000000005A40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.548939987.0000000005A40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.548939987.0000000005A40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.548939987.0000000005A40000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.544886157.00000000043DE000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.544886157.00000000043DE000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.553477471.0000000007540000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.553477471.0000000007540000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.553477471.0000000007540000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.553477471.0000000007540000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D86CF06	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	6D86CF06	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	6C6BBEFF	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	6C6B1E60	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	6C6BBEFF	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	6C6BDD66	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	6C6BDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpAB73.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C6B7038	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	6C6B1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAEBF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C6B7038	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	6C6BBEFF	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	6C6BBEFF	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	10	6C6B1E60	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	6C6B1E60	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	6C6B1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAB73.tmp	success or wait	1	6C6B6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpAEBF.tmp	success or wait	1	6C6B6A95	DeleteFileW
C:\Users\user\Desktop\outstanding statement.exe:Zone.Identifier	success or wait	1	5618B06	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd fd 30 fd 7c fd fd 48	0|H	success or wait	1	6C6B1B4F	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAB73.tmp	0	1314	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	6C6B1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	51	43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 44 65 73 6b 74 6f 70 5c 6f 75 74 73 74 61 6e 64 69 6e 67 20 73 74 61 74 65 6d 65 6e 74 2e 65 78 65	C:\Users\user\Desktop\outstanding statement.exe	success or wait	1	6C6B1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpAEBF.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	6C6B1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	12	6C6B1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327432	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	6C6B1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	6C6B1B4F	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	6D845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D845705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D84CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6B1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D82D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D82D72F	unknown
C:\Users\user\Desktop\outstanding statement.exe	unknown	4096	success or wait	1	6D82D72F	unknown
C:\Users\user\Desktop\outstanding statement.exe	unknown	512	success or wait	1	6D82D72F	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	6C6B646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **5700**, Parent PID: **5468**

General

Target ID:	9
Start time:	04:38:44
Start date:	27/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpAB73.tmp
Imagebase:	0x1220000
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\tmpAB73.tmp	unknown	2	success or wait	1	122AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpAB73.tmp	unknown	1315	success or wait	1	122ABD9	ReadFile

Analysis Process: conhost.exe PID: **5776**, Parent PID: **5700**

General

Target ID:	10
Start time:	04:38:44
Start date:	27/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: schtasks.exe PID: **5436**, Parent PID: **5468**

General

Target ID:	12
Start time:	04:38:45
Start date:	27/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpAEBF.tmp
Imagebase:	0x1220000
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\tmpAEBF.tmp	unknown	2	success or wait	1	122AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpAEBF.tmp	unknown	1311	success or wait	1	122ABD9	ReadFile

Analysis Process: conhost.exe PID: **3132**, Parent PID: **5436**

General

Target ID:	13
Start time:	04:38:45
Start date:	27/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: outstanding statement.exe PID: **5832**, Parent PID: **1064**

General

Target ID:	16
Start time:	04:38:46
Start date:	27/09/2022
Path:	C:\Users\user\Desktop\outstanding statement.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\outstanding statement.exe" 0
Imagebase:	0x110000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689

Copyright Joe Security LLC 2022

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D86CF06	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	6D86CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp27F3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C6B7038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp27F3.tmp	success or wait	1	6C6B6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp27F3.tmp	0	1658	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </Registratio	success or wait	1	6C6B1B4F	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	6D845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D845705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D84CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7A03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6B1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **3068**, Parent PID: **1064**

General

Target ID:	17
Start time:	04:38:47
Start date:	27/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xf0000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 81%, ReversingLabs • Detection: 36%, Metadefender, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D86CF06	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	6D86CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp29F7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C6B7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DB7C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp29F7.tmp	success or wait	1	6C6B6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp29F7.tmp	0	1658	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </Registratio	success or wait	1	6C6B1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DB7C907	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	6D845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D845705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D84CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D845705	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6B1B4F	ReadFile

Analysis Process: svchost.exe PID: **1276**, Parent PID: **576**

General

Target ID:	20
Start time:	04:38:54
Start date:	27/09/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: **5728**, Parent PID: **3452**

General

Target ID:	21
Start time:	04:38:56
Start date:	27/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x250000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: schtasks.exe PID: **3016**, Parent PID: **5832**

General

Target ID:	23
Start time:	04:39:12
Start date:	27/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\OldzpXTWJYUnz" /XML "C:\Users\user\AppData\Local\Temp\tmp27F3.tmp
Imagebase:	0x1220000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **2208**, Parent PID: **3016**

General	
Target ID:	24
Start time:	04:39:13
Start date:	27/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5788**, Parent PID: **3068**

General	
Target ID:	25
Start time:	04:39:13
Start date:	27/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\OldzpXTWJYUnz" /XML "C:\Users\user\AppData\Local\Temp\tmp29F7.tmp
Imagebase:	0x1220000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4944**, Parent PID: **5788**

General	
Target ID:	26
Start time:	04:39:13
Start date:	27/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: outstanding statement.exe PID: **5624**, Parent PID: **5832**

General	
Target ID:	27
Start time:	04:39:14
Start date:	27/09/2022
Path:	C:\Users\user\Desktop\outstanding statement.exe

Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x410000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **4456**, Parent PID: **3068**

General	
Target ID:	28
Start time:	04:39:16
Start date:	27/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x300000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: outstanding statement.exe PID: **1276**, Parent PID: **5832**

General	
Target ID:	29
Start time:	04:39:17
Start date:	27/09/2022
Path:	C:\Users\user\Desktop\outstanding statement.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd10000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.426017926.0000000004109000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.426017926.0000000004109000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001D.00000002.426017926.0000000004109000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.420196088.0000000003101000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.420196088.0000000003101000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001D.00000002.420196088.0000000003101000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: dhcpmon.exe PID: **2588**, Parent PID: **3068**

General	
Target ID:	30
Start time:	04:39:17
Start date:	27/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x1c0000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **6076**, Parent PID: **3068**

General

Target ID:	31
Start time:	04:39:18
Start date:	27/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x2f0000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **4008**, Parent PID: **3068**

General

Target ID:	32
Start time:	04:39:19
Start date:	27/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb20000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.443941283.0000000002E71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.443941283.0000000002E71000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000020.00000002.443941283.0000000002E71000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: schtasks.exe PID: **2040**, Parent PID: **5728**

General

Target ID:	34
Start time:	04:39:29
Start date:	27/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\OldzpXTWJYUnz" /XML "C:\Users\user\AppData\Local\Temp\tmp6644.tmp
Imagebase:	0x1220000

File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3380**, Parent PID: **2040**

General

Target ID:	35
Start time:	04:39:30
Start date:	27/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **748**, Parent PID: **5728**

General

Target ID:	36
Start time:	04:39:36
Start date:	27/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x820000
File size:	764928 bytes
MD5 hash:	C83F7860B0C0F1AD76D8CA65C6BAD689
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Disassembly

No disassembly

Copyright Joe Security LLC 2022