



ID: 708238
Sample Name: remittance.exe
Cookbook: default.jbs
Time: 07:54:52
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report remittance.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Threatname: NanoCore 6
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
AV Detection 7
E-Banking Fraud 7
Persistence and Installation Behavior 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Snort Signatures 7
Joe Sandbox Signatures 9
AV Detection 10
Networking 10
E-Banking Fraud 10
System Summary 10
Data Obfuscation 10
Boot Survival 10
Hooking and other Techniques for Hiding and Protection 10
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 11
Behavior Graph 11
Screenshots 12
Thumbnails 12
Antivirus, Machine Learning and Genetic Malware Detection 13
Initial Sample 13
Dropped Files 13
Unpacked PE Files 13
Domains 13
URLs 14
Domains and IPs 15
Contacted Domains 15
Contacted URLs 15
URLs from Memory and Binaries 15
World Map of Contacted IPs 21
Public IPs 22
General Information 22
Warnings 23
Simulations 23
Behavior and APIs 23
Joe Sandbox View / Context 23
IPs 23
Domains 23
ASNs 23
JA3 Fingerprints 23
Dropped Files 23
Created / dropped Files 23
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe 23
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier 24
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log 24
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\remittance.exe.log 24
C:\Users\user\AppData\Local\Temp\tmp264C.tmp 25
C:\Users\user\AppData\Local\Temp\tmp4136.tmp 25
C:\Users\user\AppData\Local\Temp\tmp5403.tmp 25
C:\Users\user\AppData\Local\Temp\tmpAD34.tmp 26
C:\Users\user\AppData\Local\Temp\tmpB828.tmp 26
C:\Users\user\AppData\Local\Temp\tmpC057.tmp 26
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat 27
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 27
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak 27
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin 27
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat 28

Copyright Joe Security LLC 2022

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat 28
C:\Users\user\AppData\Roaming\QgSBwlYTdt.exe 28
Static File Info 29
General 29
File Icon 29
Static PE Info 29
General 29
Entrypoint Preview 29
Data Directories 31
Sections 31
Resources 32
Imports 32
Network Behavior 32
Snort IDS Alerts 32
Network Port Distribution 33
TCP Packets 33
UDP Packets 35
DNS Queries 36
DNS Answers 36
Statistics 37
Behavior 37
System Behavior 37
Analysis Process: remittance.exePID: 5568, Parent PID: 5484 37
General 37
File Activities 38
File Created 38
File Deleted 38
File Written 38
File Read 40
Analysis Process: schtasks.exePID: 5292, Parent PID: 5568 40
General 40
File Activities 41
File Read 41
Analysis Process: conhost.exePID: 5264, Parent PID: 5292 41
General 41
Analysis Process: remittance.exePID: 5320, Parent PID: 5568 41
General 41
File Activities 43
File Created 43
File Deleted 44
File Written 44
File Read 47
Registry Activities 47
Key Value Created 47
Analysis Process: schtasks.exePID: 4656, Parent PID: 5320 47
General 47
File Activities 48
File Read 48
Analysis Process: conhost.exePID: 1396, Parent PID: 4656 48
General 48
Analysis Process: schtasks.exePID: 2800, Parent PID: 5320 48
General 48
File Activities 48
File Read 48
Analysis Process: remittance.exePID: 5408, Parent PID: 1100 49
General 49
File Activities 49
File Created 49
File Deleted 49
File Written 49
File Read 50
Analysis Process: conhost.exePID: 424, Parent PID: 2800 50
General 50
Analysis Process: dhcpmon.exePID: 3636, Parent PID: 1100 51
General 51
File Activities 51
File Created 51
File Deleted 51
File Written 51
File Read 52
Analysis Process: dhcpmon.exePID: 1368, Parent PID: 3320 52
General 52
Analysis Process: schtasks.exePID: 4176, Parent PID: 5408 53
General 53
Analysis Process: conhost.exePID: 2880, Parent PID: 4176 53
General 53
Analysis Process: remittance.exePID: 4656, Parent PID: 5408 53
General 53
Analysis Process: schtasks.exePID: 5176, Parent PID: 3636 54
General 54
Analysis Process: conhost.exePID: 5268, Parent PID: 5176 54
General 54
Analysis Process: dhcpmon.exePID: 5040, Parent PID: 3636 54
General 54
Analysis Process: schtasks.exePID: 2248, Parent PID: 1368 55
General 55
Analysis Process: dhcpmon.exePID: 4712, Parent PID: 3636 55
General 55
Analysis Process: conhost.exePID: 3992, Parent PID: 2248 55
General 55
Analysis Process: dhcpmon.exePID: 5640, Parent PID: 3636 55

General 55
Analysis Process: dhcpmon.exePID: 4688, Parent PID: 1368 56
General 56
Analysis Process: dhcpmon.exePID: 6020, Parent PID: 3636 56
General 56
Disassembly 56

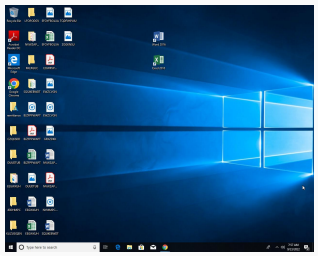
Windows Analysis Report

remittance.exe

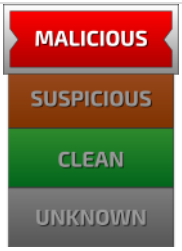
Overview

General Information

Sample Name:	remittance.exe
Analysis ID:	708238
MD5:	31c5c19e5cbf09…
SHA1:	3f39dd3802f34e7.
SHA256:	b9b9fa184afcfe0..
Tags:	exe NanoCore RAT
Infos:	



Detection



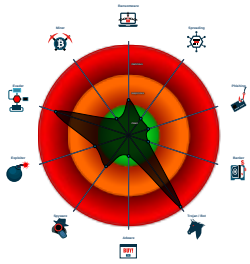
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- 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**
- remittance.exe (PID: 5568 cmdline: "C:\Users\user\Desktop\remittance.exe" MD5: 31C5C19E5CBF0993BAEEF892E8F73ADA)
  - schtasks.exe (PID: 5292 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QgSBwlYTdt" /XML "C:\Users\user\AppData\Local\Temp\tmpAD34.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - remittance.exe (PID: 5320 cmdline: {path} MD5: 31C5C19E5CBF0993BAEEF892E8F73ADA)
    - schtasks.exe (PID: 4656 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpB828.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 2800 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpC057.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- remittance.exe (PID: 5408 cmdline: C:\Users\user\Desktop\remittance.exe 0 MD5: 31C5C19E5CBF0993BAEEF892E8F73ADA)
  - schtasks.exe (PID: 4176 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QgSBwlYTdt" /XML "C:\Users\user\AppData\Local\Temp\tmp264C.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - remittance.exe (PID: 4656 cmdline: {path} MD5: 31C5C19E5CBF0993BAEEF892E8F73ADA)
- dhcpmon.exe (PID: 3636 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 31C5C19E5CBF0993BAEEF892E8F73ADA)
  - schtasks.exe (PID: 5176 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QgSBwlYTdt" /XML "C:\Users\user\AppData\Local\Temp\tmp4136.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 5040 cmdline: {path} MD5: 31C5C19E5CBF0993BAEEF892E8F73ADA)
  - dhcpmon.exe (PID: 4712 cmdline: {path} MD5: 31C5C19E5CBF0993BAEEF892E8F73ADA)
  - dhcpmon.exe (PID: 5640 cmdline: {path} MD5: 31C5C19E5CBF0993BAEEF892E8F73ADA)
  - dhcpmon.exe (PID: 6020 cmdline: {path} MD5: 31C5C19E5CBF0993BAEEF892E8F73ADA)
- dhcpmon.exe (PID: 1368 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 31C5C19E5CBF0993BAEEF892E8F73ADA)
  - schtasks.exe (PID: 2248 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QgSBwlYTdt" /XML "C:\Users\user\AppData\Local\Temp\tmp5403.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 4688 cmdline: {path} MD5: 31C5C19E5CBF0993BAEEF892E8F73ADA)
- **cleanup**

Malware Configuration

Copyright Joe Security LLC 2022

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "fba1bbc6-2cc8-4c94-b6c0-dda5a12f",
  "Group": "Default",
  "Domain1": "brightnano1.ddns.net",
  "Domain2": "",
  "Port": 1989,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.547330853.0000000005F00000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
00000004.00000002.547330853.0000000005F00000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b99:$x2: NanoCore.ClientPluginHost • 0x6bce:$s4: PipeCreated • 0x5b86:$s5: IClientLoggingHost
00000004.00000002.547330853.0000000005F00000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x5b70:$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:$s4: IPEndPoint
00000004.00000002.547330853.0000000005F00000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x5b99:$a1: NanoCore.ClientPluginHost • 0x5b70:$a2: NanoCore.ClientPlugin • 0x5b86:$b9: IClientLoggingHost
00000004.00000003.322686052.00000000063EB000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x1ad4:$a1: NanoCore.ClientPluginHost • 0x1aaf:$a2: NanoCore.ClientPlugin • 0x1ac5:$b4: IClientAppHost • 0x5fb4:$b7: LogClientException • 0x1afe:$b9: IClientLoggingHost

Click to see the 105 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.remittance.exe.2b4689c.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
4.2.remittance.exe.2b4689c.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
4.2.remittance.exe.2b4689c.1.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x2d96:$x2: NanoCore.ClientPlugin • 0x2dbb:$x3: NanoCore.ClientPluginHost • 0x2d87:$i3: IClientNetwork • 0x2dac:$i4: IClientAppHost • 0x2dd5:$i5: IClientDataHost • 0x2de5:$i7: IClientNetworkHost • 0x2df8:$i9: IClientNameObjectCollection • 0x2e1d:$i10: IClientReadOnlyNameObjectCollection • 0x2bce:$s1: ClientPlugin • 0x2d9f:$s1: ClientPlugin
4.2.remittance.exe.2b4689c.1.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x2dbb:$a1: NanoCore.ClientPluginHost • 0x2d96:$a2: NanoCore.ClientPlugin • 0x6758:$b1: get_BuilderSettings • 0x2dac:$b4: IClientAppHost
4.2.remittance.exe.5f20000.22.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
Click to see the 268 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 Keepalive Response 1 - Source IP: 171.22.30.97 - Destination IP: 192.168.2.7 −

Timestamp:	171.22.30.97192.168.2.71989497052810290 09/23/22-07:56:53.827103
SID:	2810290
Source Port:	1989
Destination Port:	49705
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.97 −

Timestamp:	192.168.2.7171.22.30.974971119892816766 09/23/22-07:57:41.247890
SID:	2816766
Source Port:	49711

Copyright Joe Security LLC 2022

Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.97	
Timestamp:	192.168.2.7171.22.30.97497061989281676 6 09/23/22-07:57:06.725139
SID:	2816766
Source Port:	49706
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 171.22.30.97 - Destination IP: 192.168.2.7	
Timestamp:	171.22.30.97192.168.2.71989497132841753 09/23/22-07:58:14.093577
SID:	2841753
Source Port:	1989
Destination Port:	49713
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 171.22.30.97 - Destination IP: 192.168.2.7	
Timestamp:	171.22.30.97192.168.2.71989497052841753 09/23/22-07:56:53.710839
SID:	2841753
Source Port:	1989
Destination Port:	49705
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.97	
Timestamp:	192.168.2.7171.22.30.97497081989281676 6 09/23/22-07:57:20.810472
SID:	2816766
Source Port:	49708
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 171.22.30.97 - Destination IP: 192.168.2.7	
Timestamp:	171.22.30.97192.168.2.71989497092841753 09/23/22-07:57:29.506018
SID:	2841753
Source Port:	1989
Destination Port:	49709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.97	
Timestamp:	192.168.2.7171.22.30.97497041989281676 6 09/23/22-07:56:47.366861
SID:	2816766
Source Port:	49704
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.97	
Timestamp:	192.168.2.7171.22.30.97497021989281676 6 09/23/22-07:56:26.749349
SID:	2816766
Source Port:	49702
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.97	
Timestamp:	192.168.2.7171.22.30.974970719892816766 09/23/22-07:57:12.636515
SID:	2816766
Source Port:	49707
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.97	
Timestamp:	192.168.2.7171.22.30.974971019892816766 09/23/22-07:57:35.334869
SID:	2816766
Source Port:	49710
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.97	
Timestamp:	192.168.2.7171.22.30.974971219892816766 09/23/22-07:57:47.430003
SID:	2816766
Source Port:	49712
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 171.22.30.97 - Destination IP: 192.168.2.7	
Timestamp:	171.22.30.97192.168.2.71989497112841753 09/23/22-07:57:41.521548
SID:	2841753
Source Port:	1989
Destination Port:	49711
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 171.22.30.97 - Destination IP: 192.168.2.7	
Timestamp:	171.22.30.97192.168.2.71989497102841753 09/23/22-07:57:35.595884
SID:	2841753
Source Port:	1989
Destination Port:	49710
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.7 - Destination IP: 171.22.30.97	
Timestamp:	192.168.2.7171.22.30.974970819892816718 09/23/22-07:57:19.224935
SID:	2816718
Source Port:	49708
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 171.22.30.97	
Timestamp:	192.168.2.7171.22.30.974970319892816766 09/23/22-07:56:33.758479
SID:	2816766
Source Port:	49703
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking



Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud



Yara detected Nanocore RAT

System Summary



Malicious sample detected (through community Yara rule)

.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



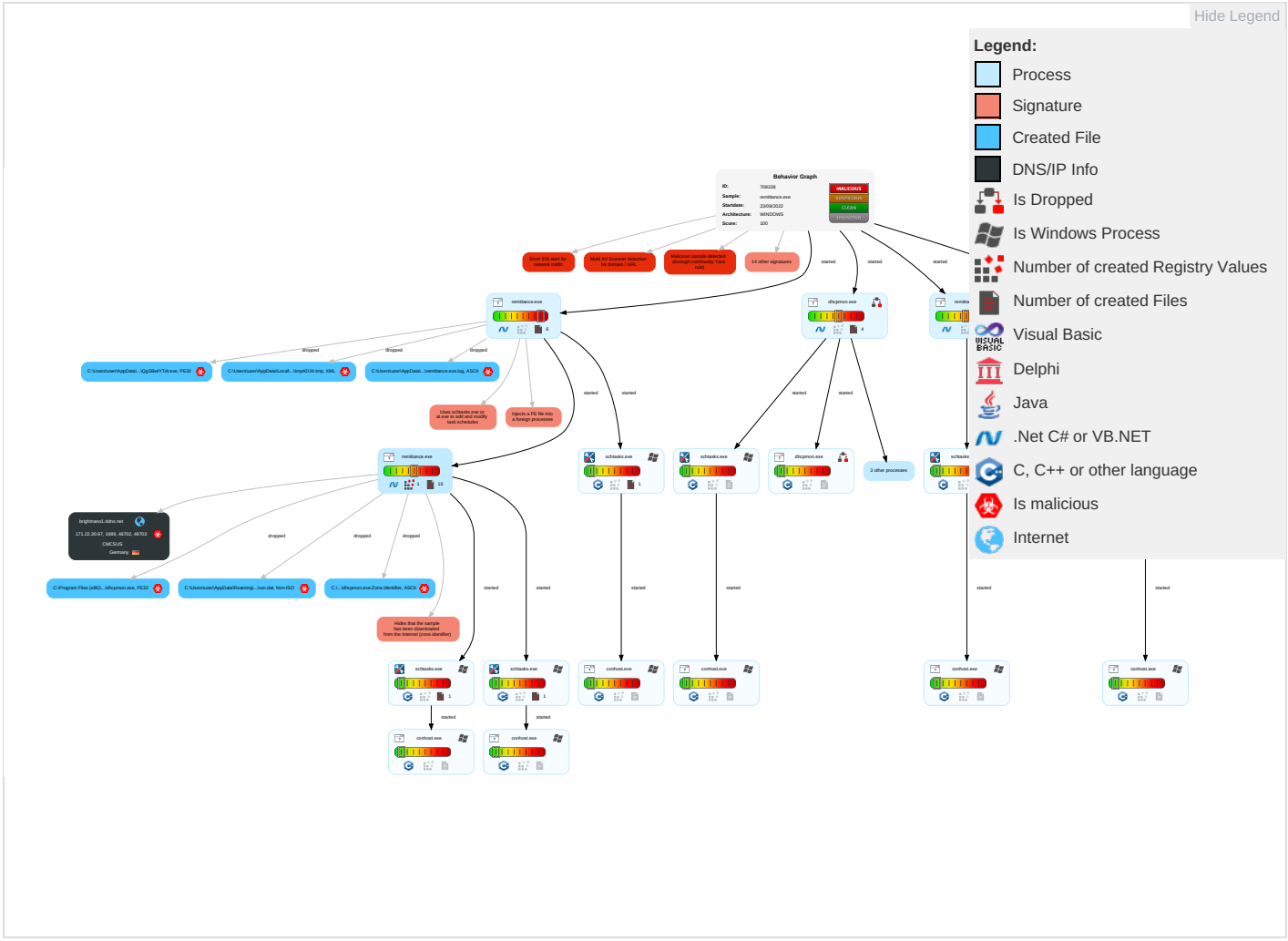
Detected Nanocore Rat

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

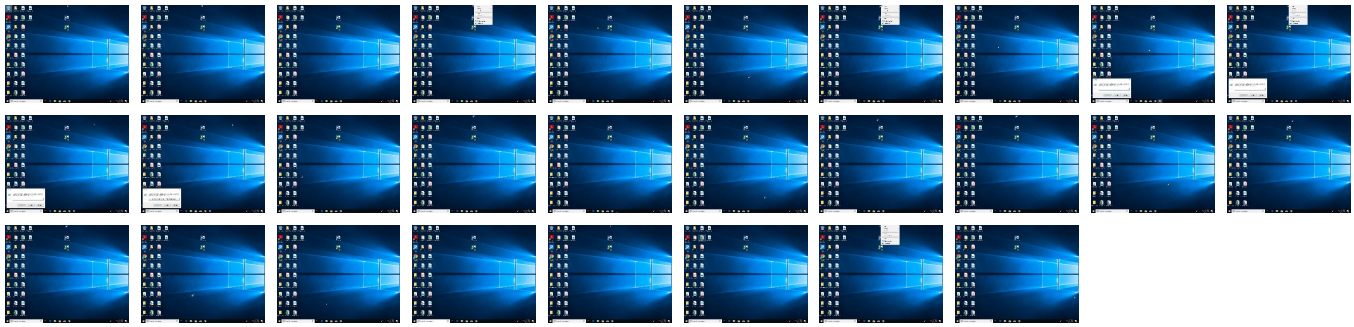
Behavior Graph



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
remittance.exe	8%	ReversingLabs		
remittance.exe	26%	Virustotal		Browse
remittance.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\QgSBwlYTdt.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.remittance.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.remittance.exe.6180000.24.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
brightnano1.ddns.net	11%	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.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.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.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/6	0%	URL Reputation	safe	
http://www.carterandcone.comue	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/#	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	0%	URL Reputation	safe	
http://www.fontbureau.comld	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/es-e	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
	0%	Avira URL Cloud	safe	
http://www.carterandcone.coms0%;	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Kurs	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0lk	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krt-it-h	0%	Avira URL Cloud	safe	
http://www.urwpp.deom	0%	Avira URL Cloud	safe	
http://www.carterandcone.comNS	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krmk	0%	Avira URL Cloud	safe	
http://www.sakkal.comP	0%	Avira URL Cloud	safe	
http://www.sakkal.comd	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://www.fonts.comion	0%	Avira URL Cloud	safe	
brightnano1.ddns.net	100%	Avira URL Cloud	malware	
http://en.wikipedia(	0%	Avira URL Cloud	safe	
http://www.sakkal.com0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/el	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsivaO	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cncom	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnT	0%	Avira URL Cloud	safe	
http://www.tiro.com~Z	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kro.krcr	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
brightnano1.ddns.net	171.22.30.97	true	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
brightnano1.ddns.net	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coms0%;	remittance.exe, 00000000.00000003.255212778.0000000005951000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.255284729.0000000005951000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.255421189.0000000005951000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comNS	remittance.exe, 00000000.00000003.255212778.0000000005951000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0lk	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://google.com	remittance.exe, 00000004.00000002.540559764.0000000003DAE000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000004.00000002.536603069.0000000003B91000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000004.00000002.539191821.0000000003D0A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000004.00000002.524449336.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000004.00000002.547117878.0000000005EE0000.00000004.08000000.00040000.00000000.sdmp	false		high
http://www.carterandcone.com	remittance.exe, 00000000.00000003.255212778.0000000005951000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.255284729.0000000005951000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.255421189.0000000005951000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/:	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256614790.000000000592A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.255721208.0000000005923000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256659668.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256395891.0000000005925000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256068123.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deom	remittance.exe, 00000000.00000003.260046920.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Kurs	remittance.exe, 00000000.00000003.257020488.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256614790.000000000592A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256659668.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256827860.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256774420.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/6	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.255721208.0000000005923000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256068123.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krt-it-h	remittance.exe, 00000000.00000003.253346124.000000000592E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comue	remittance.exe, 00000000.00000003.255212778.0000000005951000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.255284729.0000000005951000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.255421189.0000000005951000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256614790.000000000592A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256659668.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256395891.0000000005925000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/(	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256614790.000000000592A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256659668.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256395891.0000000005925000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	remittance.exe, 00000000.00000003.251831584.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.251901759.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254537231.000000000594F000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.252868092.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254144082.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.252443291.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.252376366.000000000594F000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.251866759.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.252685408.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.252259158.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.253977771.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254109489.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.252232497.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.252389352.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.251996989.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.251682033.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.253103524.0000000005955000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.252176157.0000000005955000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	remittance.exe, 00000000.00000003.253346124.000000000592E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.krl	remittance.exe, 00000000.00000003.253346124.000000000592E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/#	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256614790.000000000592A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256659668.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256395891.0000000005925000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.comd	remittance.exe, 00000000.00000003.256774420.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	remittance.exe, 00000000.00000002.305506569.000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	remittance.exe, 00000000.00000003.260046920.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	remittance.exe, 00000000.00000003.254920591.0000000005952000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254844773.0000000005950000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254910360.000000000594F000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	remittance.exe, 00000000.00000002.295989192.00000000029A1000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000004.00000002.523139135.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000010.00000002.377885898.00000000032AD000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000012.00000002.410525725.0000000002AC8000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000013.00000002.404695909.0000000002A11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.como.	remittance.exe, 00000000.00000003.255421189.0000000005951000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	remittance.exe, 00000000.00000002.305506569.000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	remittance.exe, 00000000.00000003.260376505.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.260046920.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comion	remittance.exe, 00000000.00000003.251840471.000000000106C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y	remittance.exe, 00000000.00000003.256068123.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.krmk	remittance.exe, 00000000.00000003.253346124.000000000592E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	remittance.exe, 00000000.00000002.305506569.000000006B32000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254757127.000000000594F000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	remittance.exe, 00000000.00000003.260376505.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.260046920.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.comP	remittance.exe, 00000000.00000003.256774420.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comF	remittance.exe, 00000000.00000003.260376505.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.260046920.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comTC	remittance.exe, 00000000.00000003.255212778.0000000005951000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/P	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256614790.000000000592A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256659668.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256395891.0000000005925000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256068123.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.wikipedia(	remittance.exe, 00000000.00000003.254099244.000000000594D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254127821.000000000594D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/F	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.257020488.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256614790.000000000592A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256659668.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256827860.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256395891.0000000005925000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.257090388.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256774420.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.257020488.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256614790.000000000592A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256659668.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256827860.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256774420.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	remittance.exe, 00000000.00000003.293674688.0000000005920000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	remittance.exe, 00000000.00000003.254920591.0000000005952000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254537231.000000000594F000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254844773.0000000005950000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254376366.000000000594F000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254910360.000000000594F000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254757127.000000000594F000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.253346124.000000000592E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/el	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256068123.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com0	remittance.exe, 00000000.00000003.256774420.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comsivaO	remittance.exe, 00000000.00000003.260376505.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.260046920.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/u	remittance.exe, 00000000.00000003.257020488.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256614790.000000000592A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256659668.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256827860.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256774420.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cncom	remittance.exe, 00000000.00000003.253900998.000000000594D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.253988482.000000000594D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comld	remittance.exe, 00000000.00000003.293674688.0000000005920000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.257020488.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256614790.000000000592A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.255721208.0000000005923000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256659668.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256827860.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256395891.0000000005925000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256068123.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256774420.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kro.krcr	remittance.exe, 00000000.00000003.253346124.000000000592E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/k	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256614790.000000000592A000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256659668.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256395891.0000000005925000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/es-e	remittance.exe, 00000000.00000003.256131310.000000000592D000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256188885.0000000005927000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.256395891.0000000005925000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	remittance.exe, 00000000.00000003.254910360.000000000594F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	remittance.exe, 00000000.00000002.305506569.0000000006B32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comalic	remittance.exe, 00000000.00000003.260376505.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.260572463.0000000005932000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.260046920.0000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnT	remittance.exe, 00000000.00000003.254920591.0000000005952000.00000004.00000800.00020000.00000000.sdmp, remittance.exe, 00000000.00000003.254910360.000000000594F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com~Z	remittance.exe, 00000000.00000003.254563663.000000000106C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
171.22.30.97	brightnano1.ddns.net	Germany		33657	CMCSUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708238
Start date and time:	2022-09-23 07:54:52 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	remittance.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:	34
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@36/17@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

Copyright Joe Security LLC 2022

Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- 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
07:56:00	API Interceptor	735x Sleep call for process: remittance.exe modified
07:56:16	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
07:56:17	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\remittance.exe" s>$(Arg0)
07:56:20	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
07:56:35	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\remittance.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1066496
Entropy (8bit):	6.704936269736051

Encrypted:	false
SSDEEP:	12288:BGVMmLXxPgZ8Uqcozk9h5uRsOLNoJ86aA/qoUmdaee/QCaCNqGVM9d4dIw8:B1mRgZjqco49hKssoJ8tydLC/VIdkIt
MD5:	31C5C19E5CBF0993BAEEF892E8F73ADA
SHA1:	3F39DD3802F34E7F0B8D307A5AA31DAAC779C3C8
SHA-256:	B9B9FA184AFCFE0808C76A42A44A22E960D0283CF763C120BE371122D0DE8174
SHA-512:	083B584A585FC100EE3619AD31042D0B9188E2BF81EC3F178FB2E89A2854AF30D57ADEF2E59E46E48F0A6ABFD951706D5DEE52D9479F4C12317DD0FDF2E4FE6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!-c.....P..V.....^u.. .....@.. .....@.....u..O.....H.....>..T..... ....H.....text...dU... ...V..... ..`.rsrc...H.....X.....@..@.reloc.....D.....@..B.....@u.....H.....h...._.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(...+..*.0..<.....~.....().....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r9..p~....o-...(.....t$....+..*...0..&.....(....rE..p~....o-...(.....

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

Process:	C:\Users\user\Desktop\remittance.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\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:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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

Process:	C:\Users\user\Desktop\remittance.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\tmp264C.tmp

Process:	C:\Users\user\Desktop\remittance.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1659
Entropy (8bit):	5.1742056536028755
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBZtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3F
MD5:	90E0DD9D30D70B9B789776727D6CD3BB
SHA1:	80F98DE3F9D4F88E0CAEB3C5D774695B9572AEAE
SHA-256:	4C804D823977F1DD3714ECF01D3C8E4A7B36F863C5A0D04E7AFB0B00FB846F47
SHA-512:	633938024CF9453D6ABD6C376340607AF4C343835984D20DD4F59B740EB70C1B9C936FC2CE96028A71EE6DDA384AA0BA7B00837083764E656B65B56F308BB50(
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>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmp4136.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):	1659
Entropy (8bit):	5.1742056536028755
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBZtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3F
MD5:	90E0DD9D30D70B9B789776727D6CD3BB
SHA1:	80F98DE3F9D4F88E0CAEB3C5D774695B9572AEAE
SHA-256:	4C804D823977F1DD3714ECF01D3C8E4A7B36F863C5A0D04E7AFB0B00FB846F47
SHA-512:	633938024CF9453D6ABD6C376340607AF4C343835984D20DD4F59B740EB70C1B9C936FC2CE96028A71EE6DDA384AA0BA7B00837083764E656B65B56F308BB50(
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>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmp5403.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):	1659
Entropy (8bit):	5.1742056536028755
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBZtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3F
MD5:	90E0DD9D30D70B9B789776727D6CD3BB
SHA1:	80F98DE3F9D4F88E0CAEB3C5D774695B9572AEAE
SHA-256:	4C804D823977F1DD3714ECF01D3C8E4A7B36F863C5A0D04E7AFB0B00FB846F47
SHA-512:	633938024CF9453D6ABD6C376340607AF4C343835984D20DD4F59B740EB70C1B9C936FC2CE96028A71EE6DDA384AA0BA7B00837083764E656B65B56F308BB50(

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>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmpAD34.tmp

Process:	C:\Users\user\Desktop\remittance.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1659
Entropy (8bit):	5.1742056536028755
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBZtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3F
MD5:	90E0DD9D30D70B9B789776727D6CD3BB
SHA1:	80F98DE3F9D4F88E0CAEB3C5D774695B9572AEAE
SHA-256:	4C804D823977F1DD3714ECF01D3C8E4A7B36F863C5A0D04E7AFB0B00FB846F47
SHA-512:	633938024CF9453D6ABD6C376340607AF4C343835984D20DD4F59B740EB70C1B9C936FC2CE96028A71EE6DDA384AA0BA7B00837083764E656B65B56F308BB50(
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>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmpB828.tmp

Process:	C:\Users\user\Desktop\remittance.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	5.083908227241512
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Txtn:cbk4oL600QydbQxIYODOLedq3Mj
MD5:	0461E5417F7B83DC1D8DEB0CF8D35762
SHA1:	B86B8833F25C91B15B67038FA3CD5D0F8CD9F3C9
SHA-256:	D371A16053407C3AB323FDBF050C8E2339B4DF8348BBBA61703DD7B2A4F4C642
SHA-512:	09CDBAFE7417BF21837AEE68270DD8238753021B6EF83B96CF0DE3F6B5372D0A97EECA7CE63586B99700EFB4347F7F1EB0614309247EE06331DC11BC090FAC(E
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpC057.tmp

Process:	C:\Users\user\Desktop\remittance.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\remittance.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

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

Process:	C:\Users\user\Desktop\remittance.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:tyt:k
MD5:	CF0DBE61CCFB385B907254B94C4E3430
SHA1:	34F2828C4166EEABAB2FFFFE71A163393A0118A9
SHA-256:	8382A9087BC0D1D0F5C29EE2FF5609E2AF54853E4707D8064F61FB5BEFD1B556
SHA-512:	EC523B28FB7EE959392CE491E9C484F3FED1831DE5E27497FEB70C2C41B56A5C62DA7D7F0873D31FDC1238D66935D6FB56987A1DD7AB43ABAA387AFB6B1946FF
Malicious:	**true**
Preview:	6..s..H

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

Process:	C:\Users\user\Desktop\remittance.exe
File Type:	data
Category:	modified
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

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

Process:	C:\Users\user\Desktop\remittance.exe
File Type:	data
Category:	dropped

Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

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

Process:	C:\Users\user\Desktop\remittance.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\remittance.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.030567322750604
Encrypted:	false
SSDEEP:	3:oN0naRRXeELXJ:oNcSRuETJ
MD5:	DE35DDE4CA7722A94CBC9BB3B13D04F5
SHA1:	B73A406E9E5A4CEB6EFC6BC758272EF1810EC9AE
SHA-256:	F99CE96A413109B65B60981759201A90948616BC5C616ABA9011286930471874
SHA-512:	FA152B76392F9F6D427730428F1F764F061FD4DB29FB8C73246E5C61524241089C3C08922AD31CD27836084DAE455D37ABEFB4B92E2CDF13A97DB3C7EFF29DE
Malicious:	false
Preview:	C:\Users\user\Desktop\remittance.exe

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

Process:	C:\Users\user\Desktop\remittance.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1066496
Entropy (8bit):	6.704936269736051
Encrypted:	false
SSDEEP:	12288:BGVMmLXxPgZ8Uqcozk9h5uRsOLNoJ86aA/qoUmdaee/QCaCNqGVM9d4dlw8:B1mRgZjqco49hKssoJ8tydLC/VIdkIt
MD5:	31C5C19E5CBF0993BAEEF892E8F73ADA
SHA1:	3F39DD3802F34E7F0B8D307A5AA31DAAC779C3C8
SHA-256:	B9B9FA184AFCFE0808C76A42A44A22E960D0283CF763C120BE371122D0DE8174
SHA-512:	083B584A585FC100EE3619AD31042D0B9188E2BF81EC3F178FB2E89A2854AF30D57ADEF2E59E46E48F0A6ABFD951706D5DEE52D9479F4C12317DD0FDF2E4FE6
Malicious:	**true**

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!-c.....P..V.....^u... .....@.. ....@.....u..O.....H.....>..T..... ....H.....text...dU... ...V..... ..`.rsrc...H.....X.....@..@.reloc.....D.....@..B.....@u.....H.....h...._.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r9..p~....o-...(.....t$....+..*...0..&.....(....rE..p~....o-...(.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.704936269736051
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:	remittance.exe
File size:	1066496
MD5:	31c5c19e5cbf0993baeef892e8f73ada
SHA1:	3f39dd3802f34e7f0b8d307a5aa31daac779c3c8
SHA256:	b9b9fa184afcfe0808c76a42a44a22e960d0283cf763c120be371122d0de8174
SHA512:	083b584a585fc100ee3619ad31042d0b9188e2bf81ec3f178fb2e89a2854af30d57adef2e59e46e48f0a6abfd951706d5dee52d9479f4c12317dd0fdf2e4fe86
SSDEEP:	12288:BGVMmLXxPgZ8Uqcozk9h5uRsOLNoJ86aA/qoUmdaee/QCaCNqGVM9d4dlw8:B1mRgZjqco49hKssoJ8tydLC/VIdkIt
TLSH:	35353B1022EB577CF47A5BB95BD4B4F64BD6FE615229E1FA28A073494732E00CCE1236
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!-c.....P..V.....^u... .....@.. .....@.....

File Icon



Icon Hash:	b4b4b4747cec9404

Static PE Info

General

Entrypoint:	0x4f755e
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:	0x632D2106 [Fri Sep 23 02:59:18 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]
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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf750c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf8000	0xea48	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x108000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xf3e98	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xf5564	0xf5600	False	0.5823645647605705	data	6.784690132291941	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xf8000	0xea48	0xec00	False	0.3647212658898305	data	4.963894931143003	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x108000	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	0xf81e0	0x2ded	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xfafe0	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xff218	0x25a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x1017d0	0x1a68	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x103248	0x10a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x104300	0x988	data		
RT_ICON	0x104c98	0x6b8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x105360	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1057d8	0x76	data		
RT_VERSION	0x105860	0x3bc	data		
RT_MANIFEST	0x105c2c	0xe15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

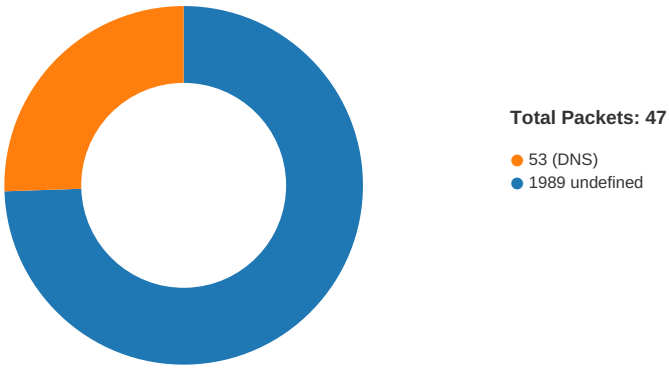
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
171.22.30.97192.168.2.71 989497052810290 09/23/22-07:56:53.827103	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	1989	49705	171.22.30.97	192.168.2.7
192.168.2.7171.22.30.974 971119892816766 09/23/22-07:57:41.247890	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49711	1989	192.168.2.7	171.22.30.97
192.168.2.7171.22.30.974 970619892816766 09/23/22-07:57:06.725139	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49706	1989	192.168.2.7	171.22.30.97
171.22.30.97192.168.2.71 989497132841753 09/23/22-07:58:14.093577	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1989	49713	171.22.30.97	192.168.2.7
171.22.30.97192.168.2.71 989497052841753 09/23/22-07:56:53.710839	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1989	49705	171.22.30.97	192.168.2.7
192.168.2.7171.22.30.974 970819892816766 09/23/22-07:57:20.810472	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	1989	192.168.2.7	171.22.30.97

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
171.22.30.97192.168.2.71 989497092841753 09/23/22-07:57:29.506018	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1989	49709	171.22.30.97	192.168.2.7
192.168.2.7171.22.30.974 970419892816766 09/23/22-07:56:47.366861	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	1989	192.168.2.7	171.22.30.97
192.168.2.7171.22.30.974 970219892816766 09/23/22-07:56:26.749349	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	1989	192.168.2.7	171.22.30.97
192.168.2.7171.22.30.974 970719892816766 09/23/22-07:57:12.636515	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49707	1989	192.168.2.7	171.22.30.97
192.168.2.7171.22.30.974 971019892816766 09/23/22-07:57:35.334869	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49710	1989	192.168.2.7	171.22.30.97
192.168.2.7171.22.30.974 971219892816766 09/23/22-07:57:47.430003	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49712	1989	192.168.2.7	171.22.30.97
171.22.30.97192.168.2.71 989497112841753 09/23/22-07:57:41.521548	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1989	49711	171.22.30.97	192.168.2.7
171.22.30.97192.168.2.71 989497102841753 09/23/22-07:57:35.595884	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1989	49710	171.22.30.97	192.168.2.7
192.168.2.7171.22.30.974 970819892816718 09/23/22-07:57:19.224935	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49708	1989	192.168.2.7	171.22.30.97
192.168.2.7171.22.30.974 970319892816766 09/23/22-07:56:33.758479	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	1989	192.168.2.7	171.22.30.97

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 07:56:21.482043982 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:21.509731054 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:21.510103941 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:22.216409922 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:22.256000996 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:22.324546099 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:22.423261881 CEST	1989	49702	171.22.30.97	192.168.2.7

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 07:56:22.424520016 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:22.452661037 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:22.593451977 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.184242964 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.321696997 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.558301926 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.721668005 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.796843052 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.796885967 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.796962976 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.797007084 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.797070980 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.797106981 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.828367949 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.828425884 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.828466892 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.828504086 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.828546047 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.828577042 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.828577995 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.828619003 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.828659058 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.828725100 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.828782082 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.828788996 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.856030941 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.856092930 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.856134892 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.856170893 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.856209993 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.856252909 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.856290102 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.856328964 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.856367111 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.856370926 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.856406927 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.856420994 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.856427908 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.856434107 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.856458902 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.859765053 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.859795094 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.859818935 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.859842062 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.859858990 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.859874964 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.859915972 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.859960079 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.886225939 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886291981 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886332035 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886368990 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886408091 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886446953 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886486053 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886526108 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886563063 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886600971 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886609077 CEST	49702	1989	192.168.2.7	171.22.30.97

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 07:56:23.886640072 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886660099 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.886667967 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.886672974 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.886677980 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.886678934 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886719942 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886737108 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.886759043 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886799097 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886816025 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.886840105 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886876106 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886890888 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.886915922 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886955976 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.886967897 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.886993885 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.887044907 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.888641119 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.888680935 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.888720036 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.888758898 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.888781071 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.888796091 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.888829947 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.888837099 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.888875961 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.888889074 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.888915062 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.888955116 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.888971090 CEST	49702	1989	192.168.2.7	171.22.30.97
Sep 23, 2022 07:56:23.889004946 CEST	1989	49702	171.22.30.97	192.168.2.7
Sep 23, 2022 07:56:23.889049053 CEST	1989	49702	171.22.30.97	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 07:56:21.361603022 CEST	55752	53	192.168.2.7	8.8.8.8
Sep 23, 2022 07:56:21.383256912 CEST	53	55752	8.8.8.8	192.168.2.7
Sep 23, 2022 07:56:32.793658018 CEST	50330	53	192.168.2.7	8.8.8.8
Sep 23, 2022 07:56:32.813060999 CEST	53	50330	8.8.8.8	192.168.2.7
Sep 23, 2022 07:56:46.083199024 CEST	56588	53	192.168.2.7	8.8.8.8
Sep 23, 2022 07:56:46.104861021 CEST	53	56588	8.8.8.8	192.168.2.7
Sep 23, 2022 07:56:53.618938923 CEST	60326	53	192.168.2.7	8.8.8.8
Sep 23, 2022 07:56:53.638699055 CEST	53	60326	8.8.8.8	192.168.2.7
Sep 23, 2022 07:57:03.385513067 CEST	50835	53	192.168.2.7	8.8.8.8
Sep 23, 2022 07:57:03.408543110 CEST	53	50835	8.8.8.8	192.168.2.7
Sep 23, 2022 07:57:12.039894104 CEST	50505	53	192.168.2.7	8.8.8.8
Sep 23, 2022 07:57:12.063334942 CEST	53	50505	8.8.8.8	192.168.2.7
Sep 23, 2022 07:57:18.231241941 CEST	61178	53	192.168.2.7	8.8.8.8
Sep 23, 2022 07:57:18.250767946 CEST	53	61178	8.8.8.8	192.168.2.7
Sep 23, 2022 07:57:29.180773973 CEST	63926	53	192.168.2.7	8.8.8.8
Sep 23, 2022 07:57:29.203119040 CEST	53	63926	8.8.8.8	192.168.2.7
Sep 23, 2022 07:57:34.402625084 CEST	53336	53	192.168.2.7	8.8.8.8
Sep 23, 2022 07:57:34.421861887 CEST	53	53336	8.8.8.8	192.168.2.7
Sep 23, 2022 07:57:40.466837883 CEST	51007	53	192.168.2.7	8.8.8.8
Sep 23, 2022 07:57:40.484746933 CEST	53	51007	8.8.8.8	192.168.2.7
Sep 23, 2022 07:57:46.221164942 CEST	50513	53	192.168.2.7	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 07:57:46.239267111 CEST	53	50513	8.8.8.8	192.168.2.7
Sep 23, 2022 07:57:52.903994083 CEST	60765	53	192.168.2.7	8.8.8.8
Sep 23, 2022 07:57:52.922050953 CEST	53	60765	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 23, 2022 07:56:21.361603022 CEST	192.168.2.7	8.8.8.8	0x2ac4	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:56:32.793658018 CEST	192.168.2.7	8.8.8.8	0x18c8	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:56:46.083199024 CEST	192.168.2.7	8.8.8.8	0x33fa	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:56:53.618938923 CEST	192.168.2.7	8.8.8.8	0x6943	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:03.385513067 CEST	192.168.2.7	8.8.8.8	0x8c89	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:12.039894104 CEST	192.168.2.7	8.8.8.8	0x5a72	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:18.231241941 CEST	192.168.2.7	8.8.8.8	0x66b5	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:29.180773973 CEST	192.168.2.7	8.8.8.8	0xa5a5	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:34.402625084 CEST	192.168.2.7	8.8.8.8	0x2366	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:40.466837883 CEST	192.168.2.7	8.8.8.8	0x2a0e	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:46.221164942 CEST	192.168.2.7	8.8.8.8	0x7977	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:52.903994083 CEST	192.168.2.7	8.8.8.8	0x5e9	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false

DNS Answers

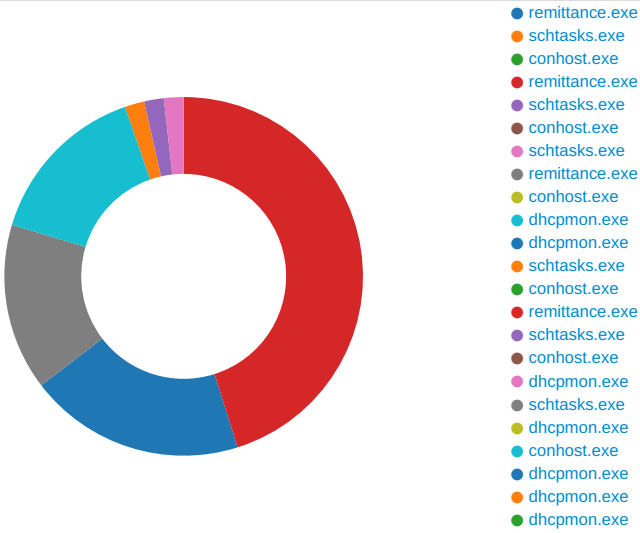
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 23, 2022 07:56:21.383256912 CEST	8.8.8.8	192.168.2.7	0x2ac4	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:56:32.813060999 CEST	8.8.8.8	192.168.2.7	0x18c8	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:56:46.104861021 CEST	8.8.8.8	192.168.2.7	0x33fa	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:56:53.638699055 CEST	8.8.8.8	192.168.2.7	0x6943	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:03.408543110 CEST	8.8.8.8	192.168.2.7	0x8c89	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:12.063334942 CEST	8.8.8.8	192.168.2.7	0x5a72	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:18.250767946 CEST	8.8.8.8	192.168.2.7	0x66b5	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:29.203119040 CEST	8.8.8.8	192.168.2.7	0xa5a5	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:34.421861887 CEST	8.8.8.8	192.168.2.7	0x2366	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:40.484746933 CEST	8.8.8.8	192.168.2.7	0x2a0e	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false
Sep 23, 2022 07:57:46.239267111 CEST	8.8.8.8	192.168.2.7	0x7977	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 23, 2022 07:57:52.922050953 CEST	8.8.8.8	192.168.2.7	0x5e9	No error (0)	brightnano 1.ddns.net		171.22.30.97	A (IP address)	IN (0x0001)	false

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: remittance.exe PID: **5568**, Parent PID: **5484**

General

Target ID:	0
Start time:	07:55:47
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\remittance.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\remittance.exe"
Imagebase:	0x520000
File size:	1066496 bytes
MD5 hash:	31C5C19E5CBF0993BAEEF892E8F73ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.302004595.0000000003C78000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.302004595.0000000003C78000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.302004595.0000000003C78000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.302004595.0000000003C78000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.300781701.0000000003AD7000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.300781701.0000000003AD7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.300781701.0000000003AD7000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.300781701.0000000003AD7000.00000004.00000800.00020000.00000000.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	6D7CCF06	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	6D7CCF06	unknown
C:\Users\user\AppData\Roaming\QgSBwlYTdt.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C611E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpAD34.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C617038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\remittance.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DADC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAD34.tmp	success or wait	1	6C616A95	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\Roaming\QgSBwlYTdt.exe	0	1066496	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\remittance.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	6DADC907	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	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Users\user\Desktop\remittance.exe	unknown	1066496	success or wait	1	6C611B4F	ReadFile

Analysis Process: schtasks.exe PID: **5292**, Parent PID: **5568**

General

Target ID:	1
Start time:	07:56:07
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QgSBwlYTdt" /XML "C:\Users\user\AppData\Local\Temp\tmpAD34.tmp
Imagebase:	0x11f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2022

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\tmpAD34.tmp	unknown	2	success or wait	1	11FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpAD34.tmp	unknown	1660	success or wait	1	11FABD9	ReadFile

Analysis Process: conhost.exe PID: **5264**, Parent PID: **5292**

General

Target ID:	2
Start time:	07:56:08
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: remittance.exe PID: **5320**, Parent PID: **5568**

General

Target ID:	4
Start time:	07:56:09
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\remittance.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x760000
File size:	1066496 bytes
MD5 hash:	31C5C19E5CBF0993BAEEF892E8F73ADA
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: 00000004.00000002.547330853.0000000005F00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.547330853.0000000005F00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.547330853.0000000005F00000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.547330853.0000000005F00000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000003.322686052.00000000063EB000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.536603069.0000000003B91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.536603069.0000000003B91000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.536603069.0000000003B91000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.540559764.0000000003DAE000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.540559764.0000000003DAE000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.551697216.0000000006F40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.551697216.0000000006F40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.551697216.0000000006F40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.551697216.0000000006F40000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.539191821.0000000003D0A000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.539191821.0000000003D0A000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.546662397.00000000055B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.546662397.00000000055B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.546662397.00000000055B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.546662397.00000000055B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.552246512.00000000070D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.552246512.00000000070D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.552246512.00000000070D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.552246512.00000000070D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.523139135.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.523139135.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.524449336.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.524449336.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.547248773.0000000005EF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.547248773.0000000005EF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.547248773.0000000005EF0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.547248773.0000000005EF0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.548156224.0000000006180000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.548156224.0000000006180000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.548156224.0000000006180000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.548156224.0000000006180000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.548156224.0000000006180000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.547117878.0000000005EE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.547117878.0000000005EE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.547117878.0000000005EE0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.547117878.0000000005EE0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.551554712.0000000006F30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.551554712.0000000006F30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.551554712.0000000006F30000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.551554712.0000000006F30000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.290583986.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.290583986.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000000.290583986.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000000.290583986.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.547043213.0000000005ED0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.547043213.0000000005ED0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.547043213.0000000005ED0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.547043213.0000000005ED0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.552056208.0000000006F70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.552056208.0000000006F70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth

	• Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.552056208.0000000006F70000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.552056208.0000000006F70000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.552340856.0000000007160000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.552340856.0000000007160000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.552340856.0000000007160000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.552340856.0000000007160000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.552120650.0000000006F80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.552120650.0000000006F80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.552120650.0000000006F80000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.552120650.0000000006F80000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.547605387.0000000005F20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.547605387.0000000005F20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.547605387.0000000005F20000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.547605387.0000000005F20000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.547869881.0000000005F40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.547869881.0000000005F40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.547869881.0000000005F40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.547869881.0000000005F40000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000004.00000002.535725850.0000000003AC1000.00000004.00000800.00020000.00000000.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	6D7CCF06	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	6D7CCF06	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	6C61BEFF	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	6C611E60	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	6C61BEFF	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	6C61DD66	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	6C61DD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB828.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C617038	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	6C611E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpC057.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C617038	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	6C61BEFF	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	6C61BEFF	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	11	6C611E60	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	6C611E60	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	6C611E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C61DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB828.tmp	success or wait	1	6C616A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpC057.tmp	success or wait	1	6C616A95	DeleteFileW
C:\Users\user\Desktop\remittance.exe:Zone.Identifier	success or wait	1	6C592935	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	success or wait	1	6C616A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	36 fa fd 73 fd fd 48	6sH	success or wait	1	6C611B4F	WriteFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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\tmpC057.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	6C611B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	12	6C611B4F	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	6C611B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	24	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd	9iH}Z4f~a	success or wait	2	6C611B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	0	24	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d fd 4a 22 fd 43 3b 22 61	9iH}Z4fJ"C;"a	success or wait	1	6C61DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D78D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D78D72F	unknown
C:\Users\user\Desktop\remittance.exe	unknown	4096	success or wait	1	6D78D72F	unknown
C:\Users\user\Desktop\remittance.exe	unknown	512	success or wait	1	6D78D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6D78D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6D78D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6D78D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6D78D72F	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	6C61646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **4656**, Parent PID: **5320**

General

Target ID:	13
Start time:	07:56:15
Start date:	23/09/2022
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\tmpB828.tmp
Imagebase:	0x11f0000
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\tmpB828.tmp	unknown	2	success or wait	1	11FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpB828.tmp	unknown	1305	success or wait	1	11FABD9	ReadFile

Analysis Process: conhost.exe PID: **1396**, Parent PID: **4656**

General

Target ID:	14
Start time:	07:56:16
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: **2800**, Parent PID: **5320**

General

Target ID:	15
Start time:	07:56:17
Start date:	23/09/2022
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\tmpC057.tmp
Imagebase:	0x11f0000
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\tmpC057.tmp	unknown	2	success or wait	1	11FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC057.tmp	unknown	1311	success or wait	1	11FABD9	ReadFile

Analysis Process: remittance.exe PID: **5408**, Parent PID: **1100**

General

Target ID:	16
Start time:	07:56:17
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\remittance.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\remittance.exe 0
Imagebase:	0xdd0000
File size:	1066496 bytes
MD5 hash:	31C5C19E5CBF0993BAEEF892E8F73ADA
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	6D7CCF06	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	6D7CCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp264C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C617038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp264C.tmp	success or wait	1	6C616A95	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\tmp264C.tmp	0	1659	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 66 72 6f 6e 74 64 65 73 6b 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	<?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> </Registrati	success or wait	1	6C611B4F	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	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C611B4F	ReadFile

Analysis Process: conhost.exe PID: **424**, Parent PID: **2800**

General

Target ID:	17
Start time:	07:56:18
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: dhcpmon.exe PID: **3636**, Parent PID: **1100**

General

Target ID:	18
Start time:	07:56:20
Start date:	23/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x5a0000
File size:	1066496 bytes
MD5 hash:	31C5C19E5CBF0993BAEEF892E8F73ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	6D7CCF06	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	6D7CCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp4136.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C617038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4136.tmp	success or wait	1	6C616A95	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\tmp4136.tmp	0	1659	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 66 72 6f 6e 74 64 65 73 6b 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	<?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> </Registrati	success or wait	1	6C611B4F	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	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C611B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **1368**, Parent PID: **3320**

General

Target ID:	19
Start time:	07:56:25
Start date:	23/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x540000
File size:	1066496 bytes
MD5 hash:	31C5C19E5CBF0993BAEEF892E8F73ADA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Reputation:	low

Analysis Process: schtasks.exe PID: **4176**, Parent PID: **5408**

General	
Target ID:	20
Start time:	07:56:39
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QgSBwlYTdt" /XML "C:\Users\user\AppData\Local\Temp\tmp264C.tmp
Imagebase:	0x11f0000
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: **2880**, Parent PID: **4176**

General	
Target ID:	21
Start time:	07:56:43
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: remittance.exe PID: **4656**, Parent PID: **5408**

General	
Target ID:	22
Start time:	07:56:45
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\remittance.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xfe0000
File size:	1066496 bytes
MD5 hash:	31C5C19E5CBF0993BAEEF892E8F73ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.417596435.0000000004409000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.417596435.0000000004409000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000016.00000002.417596435.0000000004409000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.414806118.0000000003401000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.414806118.0000000003401000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000016.00000002.414806118.0000000003401000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: schtasks.exe PID: **5176**, Parent PID: **3636**

General	
Target ID:	23
Start time:	07:56:46
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QgSBwlYTdt" /XML "C:\Users\user\AppData\Local\Temp\tmp4136.tmp
Imagebase:	0x11f0000
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: **5268**, Parent PID: **5176**

General	
Target ID:	24
Start time:	07:56:48
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **5040**, Parent PID: **3636**

General	
Target ID:	25
Start time:	07:56:49
Start date:	23/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x2d0000
File size:	1066496 bytes
MD5 hash:	31C5C19E5CBF0993BAEEF892E8F73ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **2248**, Parent PID: **1368**

General	
Target ID:	26
Start time:	07:56:51
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QgSBwlYTdt" /XML "C:\Users\user\AppData\Local\Temp\tmp5403.tmp
Imagebase:	0x11f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **4712**, Parent PID: **3636**

General	
Target ID:	27
Start time:	07:56:51
Start date:	23/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x60000
File size:	1066496 bytes
MD5 hash:	31C5C19E5CBF0993BAEEF892E8F73ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3992**, Parent PID: **2248**

General	
Target ID:	28
Start time:	07:56:52
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: **5640**, Parent PID: **3636**

General	
Target ID:	29
Start time:	07:56:53
Start date:	23/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x170000
File size:	1066496 bytes
MD5 hash:	31C5C19E5CBF0993BAEEF892E8F73ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **4688**, Parent PID: **1368**

General	
Target ID:	30
Start time:	07:56:54
Start date:	23/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xbd0000
File size:	1066496 bytes
MD5 hash:	31C5C19E5CBF0993BAEEF892E8F73ADA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.446559269.0000000003141000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.446559269.0000000003141000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001E.00000002.446559269.0000000003141000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: dhcpmon.exe PID: **6020**, Parent PID: **3636**

General	
Target ID:	31
Start time:	07:56:54
Start date:	23/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x550000
File size:	1066496 bytes
MD5 hash:	31C5C19E5CBF0993BAEEF892E8F73ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

No disassembly