ID: 431749
Sample Name:
9n7miZydYC.exe
Cookbook: default.jbs
Time: 08:39:19
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

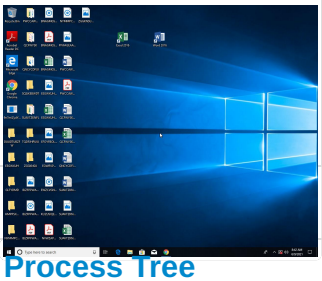
Analysis Report 9n7miZydYC.exe

Overview

General Information

Sample Name:	9n7miZydYC.exe
Analysis ID:	431749
MD5:	61de33a77d34a3..
SHA1:	2690f84adb2c617.
SHA256:	9037afbf6a54684..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

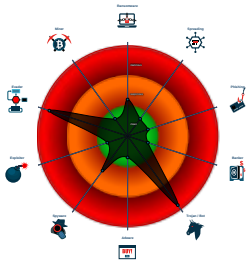
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains method …
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- 9n7miZydYC.exe (PID: 780 cmdline: 'C:\Users\user\Desktop\9n7miZydYC.exe' MD5: 61DE33A77D34A313DF07DC2BDD28140A)
  - 9n7miZydYC.exe (PID: 1736 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
    - schtasks.exe (PID: 4560 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpC2C1.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 4356 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpC67B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 3660 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 9n7miZydYC.exe (PID: 4716 cmdline: C:\Users\user\Desktop\9n7miZydYC.exe 0 MD5: 61DE33A77D34A313DF07DC2BDD28140A)
  - 9n7miZydYC.exe (PID: 3040 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
  - 9n7miZydYC.exe (PID: 4280 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
  - 9n7miZydYC.exe (PID: 5752 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
- dhcpmon.exe (PID: 5508 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 61DE33A77D34A313DF07DC2BDD28140A)
  - dhcpmon.exe (PID: 2148 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
- dhcpmon.exe (PID: 5668 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 61DE33A77D34A313DF07DC2BDD28140A)
  - dhcpmon.exe (PID: 3504 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f9198f9a-66a7-4bba-ab1c-dff8091c",
  "Group": "Default",
  "Domain1": "tzitziklishop.ddns.net",
  "Domain2": "tzitziklishop.ddns.net",
  "Port": 1665,
  "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": "",
  "BackupDNSServer": "37.235.1.177",
  "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 Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001F.00000000.383519060.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001F.00000000.383519060.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001F.00000000.383519060.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000001E.00000002.392510114.00000000042C9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000001E.00000002.392510114.00000000042C9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x435a5:$a: NanoCore • 0x435fe:$a: NanoCore • 0x4363b:$a: NanoCore • 0x436b4:$a: NanoCore • 0x56d5f:$a: NanoCore • 0x56d74:$a: NanoCore • 0x56da9:$a: NanoCore • 0x6fd63:$a: NanoCore • 0x6fd78:$a: NanoCore • 0x6fdad:$a: NanoCore • 0x43607:$b: ClientPlugin • 0x43644:$b: ClientPlugin • 0x43f42:$b: ClientPlugin • 0x43f4f:$b: ClientPlugin • 0x56b1b:$b: ClientPlugin • 0x56b36:$b: ClientPlugin • 0x56b66:$b: ClientPlugin • 0x56d7d:$b: ClientPlugin • 0x56db2:$b: ClientPlugin • 0x6fb1f:$b: ClientPlugin • 0x6fb3a:$b: ClientPlugin
Click to see the 99 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
31.0.dhcpmon.exe.400000.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
31.0.dhcpmon.exe.400000.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
31.0.dhcpmon.exe.400000.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
31.0.dhcpmon.exe.400000.3.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
31.2.dhcpmon.exe.3c505fc.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x287b1:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x287de:$x2: IClientNetworkHost
Click to see the 116 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
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 method to dynamically call methods (often used by packers)
.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:

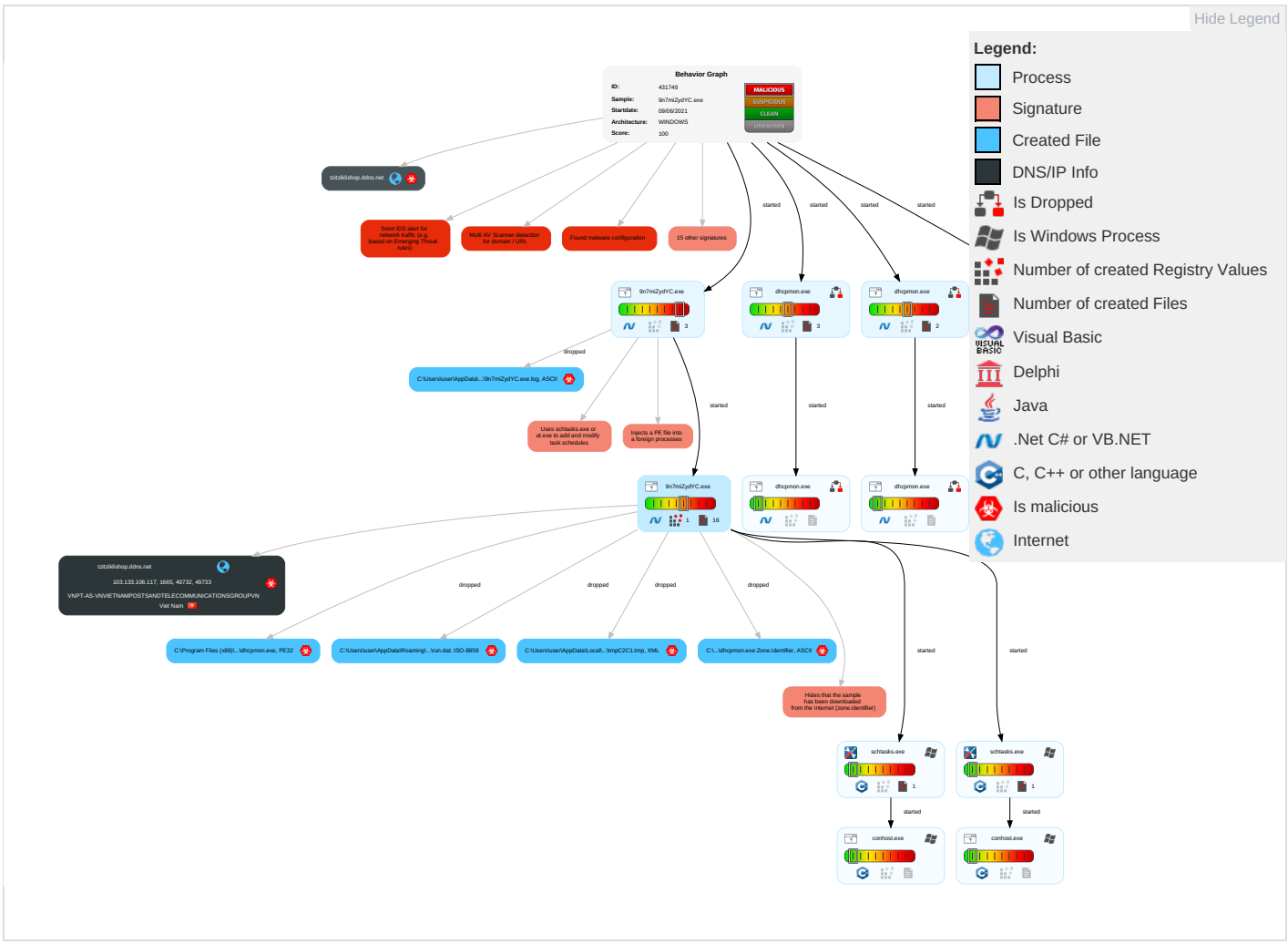
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 1	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

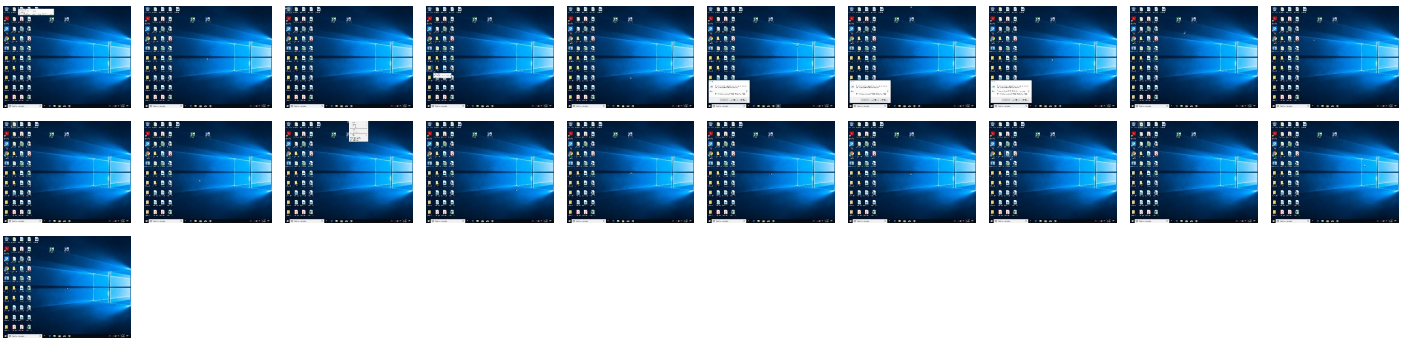
Behavior Graph



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
9n7miZydYC.exe	48%	Virustotal		Browse
9n7miZydYC.exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
9n7miZydYC.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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
31.0.dhcpmon.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
31.0.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.9n7miZydYC.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
30.0.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
29.0.9n7miZydYC.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.9n7miZydYC.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
30.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.9n7miZydYC.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
30.0.dhcpmon.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
29.2.9n7miZydYC.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
29.0.9n7miZydYC.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
31.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
tzitziklishop.ddns.net	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
tzitziklishop.ddns.net	9%	Virustotal		Browse
tzitziklishop.ddns.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/A	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ue	0%	Avira URL Cloud	safe	
http://www.tiro.com	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.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.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.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.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/6	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/6	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/6	0%	URL Reputation	safe	
http://www.fontbureau.comlicd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/e	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/S	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/$	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/$	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/$	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.fontbureau.comA	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comF-	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/oiJ	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/S	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/S	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	0%	URL Reputation	safe	
http://www.fontbureau.comde	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/T	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.com.TTFJ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/w	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/w	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/w	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/va	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/$	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsoS	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tzitziklishop.ddns.net	103.133.106.117	true	true	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
tzitziklishop.ddns.net	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.133.106.117	tzitziklishop.ddns.net	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431749
Start date:	09.06.2021
Start time:	08:39:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9n7miZydYC.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@22/12@12/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 75% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:40:45	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\9n7miZydYC.exe" s>$(Arg0)
08:40:45	API Interceptor	694x Sleep call for process: 9n7miZydYC.exe modified
08:40:45	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
08:40:47	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.133.106.117	NEW ORDER Ref PO-298721.doc	Get hash	malicious	Browse	
	NEW ORDER (Ref PO-298721).exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tzitziklishop.ddns.net	NEW ORDER Ref PO-298721.doc	Get hash	malicious	Browse	• 103.133.106.117
	NEW ORDER (Ref PO-298721).exe	Get hash	malicious	Browse	• 103.133.106.117
	plf.exe	Get hash	malicious	Browse	• 103.89.90.73
	365d37e0_by_Libranalysis.exe	Get hash	malicious	Browse	• 103.89.90.73
	SWIFT COPY.xlsx	Get hash	malicious	Browse	• 103.89.90.73

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	NEW ORDER Ref PO-298721.doc	Get hash	malicious	Browse	• 103.133.106.117
	2-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	3-1.exe	Get hash	malicious	Browse	• 103.114.107.28
	2-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	3-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	3-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	7-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	7-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	9-1.exe	Get hash	malicious	Browse	• 103.114.107.28
	9-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	9-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	11-1.exe	Get hash	malicious	Browse	• 103.114.107.28
	11-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	13-1.exe	Get hash	malicious	Browse	• 103.114.107.28
	13-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	13-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	15-1.exe	Get hash	malicious	Browse	• 103.114.107.28
	15-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	15-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	17-1.exe	Get hash	malicious	Browse	• 103.114.107.28

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	NEW ORDER Ref PO-298721.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\9n7miZydYC.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	736256
Entropy (8bit):	7.59865760202799
Encrypted:	false
SSDEEP:	6144:x2j8F5ve0At+vWlrOXMRzyeYlDW6PzaIm8MI8x39qflzAQnT6kygum2OMidd8P99:sj8FU9qXKueqZPeLhI8N0MQn5zdd8ld
MD5:	61DE33A77D34A313DF07DC2BDD28140A
SHA1:	2690F84ADB2C6174AAB432A61737CA892AF2D206
SHA-256:	9037AFBF6A54684A77A6D0B204DAA0A843555E01A9BD600545D8AE252B88FAD7
SHA-512:	9AAD4399FB37F78D1E658006EFDFE218607F51D630496CE7FBC1766BDD78B8F360657C8A661CF48602105F5C7D7A9C772180D5307BC3B9D5E2D2DE2CDB24E4(
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Joe Sandbox View:	• Filename: NEW ORDER Ref PO-298721.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.`.....0..2.....Q... ...`....@.. ....@.....pQ..O...`.....8P..... ..... ..H.....text....1... ...2..... ..`.rsrc.....`.....4.....@..@.rel oc.....:.....@..B.....Q.....H.....k....x.....r...p}.....}.....(.....(.....*..0..?.....{....o....r[..p(....-\.{....o....r[..p(....-E.{....o....r[..p(....-..{....o....r[..p(....-..{....o....r[..p(....+.....,..r]..p(....&8.....{....s.....=...%.ry..p.%..{....o.....%.r...p.%..{....o.....%.r...p.%..{....o.....%.r...p.%..{....o.....%.r...p.%...{....o.....%..r...p.(.....s.....o.....o.....r...p(....&**...(.....*..*....0..+.....,..{.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\9n7miZydYC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\9n7miZydYC.exe.log	
Process:	C:\Users\user\Desktop\9n7miZydYC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmpC2C1.tmp	
Process:	C:\Users\user\Desktop\9n7miZydYC.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.118944582901851
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0j/xtn:cbk4oL600QydbQxIYODOLedq30j
MD5:	A9BA54AEEE57957F8C82B492D8C5097B
SHA1:	768E15E065FCA4DF27F898AA6E2DFCBB3EBAAC21
SHA-256:	6F19738FFCBFB6AC48E387D6E9DF6941EAD5DACF9D56A6510EDA963CF1A18814
SHA-512:	E8C5005D1ECD66BA35C122C34FF8EE043A6101EFC1E5144C7708C2A1E8E023F956BC8F38AB96FAC3675382CC255A5F5A91830F6DC4D56635AF70D4C8F92475(
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpC67B.tmp	
Process:	C:\Users\user\Desktop\9n7miZydYC.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
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\9n7miZydYC.exe
File Type:	data
Category:	dropped
Size (bytes):	2320
Entropy (8bit):	7.089541637477408

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhDjhDjhL
MD5:	2CC2E05CB39A76B255530F61BA4AA2E3
SHA1:	76BD6001B1922B2B3FB2F618740FA74A6C532A7F
SHA-256:	FBF89196FF1A9FC33EE6C42DC0A959DAA89E2322F3417C77534C9968C0885271
SHA-512:	2EACD3A81456781803A9C14F7471DBBDB126BBE7AEC3105B1A49AB115A8BB831EA0D1DF48BAB00EB8231B114EAE5A03DF73A7A60B45BA03CB2F92382CF4DB B38
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?. ..A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH }..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f. ..p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\9n7miZydYC.exe
File Type:	ISO-8859 text
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:GL8tn:GL8n
MD5:	BDFAE484F0490CA439A3B3B99266C3D7
SHA1:	DE3458EAE36DEB1F38BF5166C041F88423D2F8A8
SHA-256:	FDDDA7C9DE87079CC5EACD239E0C4320D8A9B594C01EF48E6E5B9BC319BEE5E1
SHA-512:	5E3AD9DBE4001CAA46506169E0B94167DB95480190B6FF39BB1BDDC3E05F76F54899A9C148C821DC01C51E0BE90ADE6BE1E0E641CFB07832977E3632E5AB505 4
Malicious:	**true**
Preview:	..0.\+.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\9n7miZydYC.exe
File Type:	data
Category:	modified
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F 97
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\9n7miZydYC.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1:RzWDIfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A 6
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\9n7miZydYC.exe

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wl8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3A
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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_..&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC.....O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$...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\9n7miZydYC.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.486348298002912
Encrypted:	false
SSDEEP:	3:oNWXp5vcvn:oNWXpFcv
MD5:	A11591BB060207647B8D2E30A04C3307
SHA1:	78498F3EBB7B68111B258017412B2BEDC9D2F4CE
SHA-256:	6272B883FBAFE98ABC0CAD713CDA4B705B9A99C3E70C43C982C2FBB06297AF49
SHA-512:	EA14B14522B3B6DDD2FB42DF80792305DBBEF1DE11D3FD1BB52B7A6E0CBACC6846930082D9377276F7C2293C3FB221D1D6D555F914D67006CC8F8B6DDD3C45F
Malicious:	false
Preview:	C:\Users\user\Desktop\9n7miZydYC.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.59865760202799
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	9n7miZydYC.exe
File size:	736256
MD5:	61de33a77d34a313df07dc2bdd28140a
SHA1:	2690f84adb2c6174aab432a61737ca892af2d206
SHA256:	9037afbf6a54684a77a6d0b204daa0a843555e01a9bd60545d8ae252b88fad7
SHA512:	9aad4399fb37f78d1e658006efdfe218607f51d630496ce7fbc1766bdd78b8f360657c8a661cf48602105f5c7d7a9c772180d5307bc3b9d5e2d2de2cdb24e4c1
SSDEEP:	6144:x2j8F5ve0At+vWlrOXMRzyeYlDW6PzaIm8MI8x39qflzAQnT6kygum2OMidd8P99:sj8FU9qXKueqZPeLhI8N0MQn5zdd8ld
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.`.....0..2.....Q... ..`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b51c2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60BF6ABB [Tue Jun 8 13:03:55 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb31c8	0xb3200	False	0.666222795272	data	7.60711640242	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x5dc	0x600	False	0.4296875	data	4.16106067239	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/09/21-08:40:48.822269	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	1665	192.168.2.3	103.133.106.117
06/09/21-08:40:55.835305	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	1665	192.168.2.3	103.133.106.117
06/09/21-08:41:03.048739	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	1665	192.168.2.3	103.133.106.117
06/09/21-08:41:10.295361	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60633	37.235.1.174	192.168.2.3
06/09/21-08:41:10.574958	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	1665	192.168.2.3	103.133.106.117

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/09/21-08:41:19.210772	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	1665	192.168.2.3	103.133.106.117
06/09/21-08:41:27.172287	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	1665	192.168.2.3	103.133.106.117
06/09/21-08:41:35.865210	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	1665	192.168.2.3	103.133.106.117
06/09/21-08:41:42.698348	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	1665	192.168.2.3	103.133.106.117
06/09/21-08:41:49.419836	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	1665	192.168.2.3	103.133.106.117
06/09/21-08:41:55.865614	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	1665	192.168.2.3	103.133.106.117
06/09/21-08:42:02.784457	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	1665	192.168.2.3	103.133.106.117
06/09/21-08:42:10.089038	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	1665	192.168.2.3	103.133.106.117

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 08:40:48.458422899 CEST	192.168.2.3	37.235.1.174	0x4990	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:40:55.365665913 CEST	192.168.2.3	37.235.1.174	0x703b	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:02.682830095 CEST	192.168.2.3	37.235.1.174	0x78af	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:10.142401934 CEST	192.168.2.3	37.235.1.174	0xb2d8	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:18.862062931 CEST	192.168.2.3	37.235.1.174	0x94e9	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:26.709872961 CEST	192.168.2.3	37.235.1.174	0x8506	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:35.439858913 CEST	192.168.2.3	37.235.1.174	0x3e1c	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:42.327558041 CEST	192.168.2.3	37.235.1.174	0x9324	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:49.047765017 CEST	192.168.2.3	37.235.1.174	0x10b5	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:55.503642082 CEST	192.168.2.3	37.235.1.174	0x4c5d	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:42:02.421720028 CEST	192.168.2.3	37.235.1.174	0xf02e	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:42:09.465266943 CEST	192.168.2.3	37.235.1.174	0xa72f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 08:40:48.512447119 CEST	37.235.1.174	192.168.2.3	0x4990	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 08:40:55.548255920 CEST	37.235.1.174	192.168.2.3	0x703b	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:02.745002985 CEST	37.235.1.174	192.168.2.3	0x78af	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:10.295361042 CEST	37.235.1.174	192.168.2.3	0xb2d8	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 08:41:18.916666031 CEST	37.235.1.174	192.168.2.3	0x94e9	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:26.865480900 CEST	37.235.1.174	192.168.2.3	0x8506	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:35.556212902 CEST	37.235.1.174	192.168.2.3	0x3e1c	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:42.385374069 CEST	37.235.1.174	192.168.2.3	0x9324	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:49.103404045 CEST	37.235.1.174	192.168.2.3	0x10b5	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 08:41:55.559006929 CEST	37.235.1.174	192.168.2.3	0x4c5d	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 08:42:02.476983070 CEST	37.235.1.174	192.168.2.3	0xf02e	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 08:42:09.803811073 CEST	37.235.1.174	192.168.2.3	0xa72f	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 9n7miZydYC.exe PID: 780 Parent PID: 5780

General

Start time:	08:40:03
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\9n7miZydYC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\9n7miZydYC.exe'
Imagebase:	0xef0000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.281977110.0000000004495000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.281977110.0000000004495000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.281977110.0000000004495000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.279167689.0000000003334000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.280854533.00000000042E9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.280854533.00000000042E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.280854533.00000000042E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 9n7miZydYC.exe PID: 1736 Parent PID: 780

General

Start time:	08:40:40
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\9n7miZydYC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa20000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
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: 00000007.00000000.277218336.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.277218336.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.277218336.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.463411890.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.463411890.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.463411890.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.277575023.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.277575023.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.277575023.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 4560 Parent PID: 1736

General

Start time:	08:40:43
Start date:	09/06/2021
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\tmpC2C1.tmp'
Imagebase:	0x7ff672e70000
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 — Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4548 Parent PID: 4560

General

Start time:	08:40:44
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 4356 Parent PID: 1736

General

Start time:	08:40:44
Start date:	09/06/2021
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\tmpC67B.tmp'
Imagebase:	0xa0000
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

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 3660 Parent PID: 4356

General

Start time:	08:40:45
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 9n7miZydYC.exe PID: 4716 Parent PID: 528

General

Start time:	08:40:45
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\9n7miZydYC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\9n7miZydYC.exe 0
Imagebase:	0x570000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
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: 0000000F.00000002.375447688.0000000003D35000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.375447688.0000000003D35000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.375447688.0000000003D35000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.374531994.0000000003B89000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.374531994.0000000003B89000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.374531994.0000000003B89000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000F.00000002.372309695.0000000002BD6000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 5508 Parent PID: 528

General

Start time:	08:40:47
Start date:	09/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x6d0000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000013.00000002.372998253.0000000002AD6000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.376242535.0000000003C35000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.376242535.0000000003C35000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.376242535.0000000003C35000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.374908003.0000000003A89000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.374908003.0000000003A89000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.374908003.0000000003A89000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 37%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 5668 Parent PID: 3388

General

Start time:	08:40:54
Start date:	09/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xc0000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
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: 00000015.00000002.391258363.0000000003449000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.391258363.0000000003449000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.391258363.0000000003449000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000015.00000002.388668896.0000000002496000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.392080007.00000000035F5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.392080007.00000000035F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.392080007.00000000035F5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: 9n7miZydYC.exe PID: 3040 Parent PID: 4716

General

Start time:	08:41:21
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\9n7miZydYC.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x350000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 9n7miZydYC.exe PID: 4280 Parent PID: 4716

General

Start time:	08:41:22
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\9n7miZydYC.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3b0000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 9n7miZydYC.exe PID: 5752 Parent PID: 4716

General

Start time:	08:41:23
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\9n7miZydYC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc70000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
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: 0000001D.00000002.388118309.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.388118309.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.388118309.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.390678037.0000000003041000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.390678037.0000000003041000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000000.367378120.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000000.367378120.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000000.367378120.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000000.367856055.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000000.367856055.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000000.367856055.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.391222166.0000000004049000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.391222166.0000000004049000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Reputation:	low

Analysis Process: dhcpmon.exe PID: 2148 Parent PID: 5508

General

Start time:	08:41:23
Start date:	09/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xe20000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.392510114.00000000042C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.392510114.00000000042C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001E.00000000.368666676.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000000.368666676.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000000.368666676.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001E.00000002.388846832.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.388846832.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.388846832.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001E.00000000.368132271.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000000.368132271.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000000.368132271.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.392325016.00000000032C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.392325016.00000000032C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 3504 Parent PID: 5668

General

Start time:	08:41:30
Start date:	09/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7a0000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
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: 0000001F.00000000.383519060.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000000.383519060.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000000.383519060.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001F.00000002.403785027.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000002.403785027.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000002.403785027.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001F.00000000.383969923.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000000.383969923.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000000.383969923.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000002.405159880.0000000002C01000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000002.405159880.0000000002C01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000002.405306863.0000000003C09000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000002.405306863.0000000003C09000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis