ID: 321402
Sample Name:
Package_details.exe
Cookbook: default.jbs
Time: 15:28:10
Date: 21/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

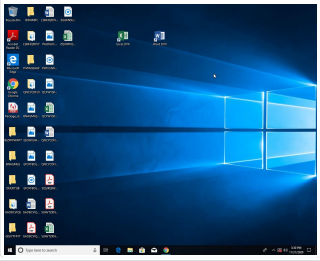
Analysis Report Package_details.exe

Overview

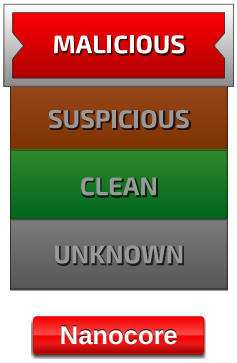
General Information

Sample Name:	Package_details.exe
Analysis ID:	321402
MD5:	ce3c5367fb067a4..
SHA1:	9d0f4d746747a6f..
SHA256:	e4fc20492ed4f47..
Tags:	NanoCore

Most interesting Screenshot:



Detection

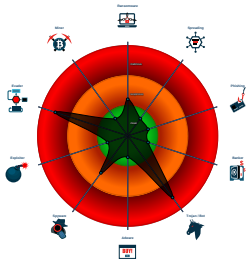


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Detected unpacking (creates a PE fi…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Connects to many ports of the same…
- Hides that the sample has been dow…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- Package_details.exe (PID: 1092 cmdline: 'C:\Users\user\Desktop\Package_details.exe' MD5: CE3C5367FB067A45F5FA10C35CA23A28)
  - cmd.exe (PID: 4092 cmdline: cmd /c schtasks /Create /TN fonts /XML 'C:\Users\user\AppData\Local\Temp\3b53dd4f8dbc40fcb4ebf67bcf9e21d3.xml' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 2296 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5464 cmdline: schtasks /Create /TN fonts /XML 'C:\Users\user\AppData\Local\Temp\3b53dd4f8dbc40fcb4ebf67bcf9e21d3.xml' MD5: 15FF7D8324231381BAD48A052F85DF04)
  - Package_details.exe (PID: 4156 cmdline: C:\Users\user\Desktop\Package_details.exe MD5: CE3C5367FB067A45F5FA10C35CA23A28)
    - schtasks.exe (PID: 5592 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp30A7.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5108 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp33C5.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Package_details.exe (PID: 5804 cmdline: C:\Users\user\Desktop\Package_details.exe 0 MD5: CE3C5367FB067A45F5FA10C35CA23A28)
  - Package_details.exe (PID: 4168 cmdline: C:\Users\user\Desktop\Package_details.exe MD5: CE3C5367FB067A45F5FA10C35CA23A28)
  - Package_details.exe (PID: 2140 cmdline: C:\Users\user\Desktop\Package_details.exe MD5: CE3C5367FB067A45F5FA10C35CA23A28)
    - Package_details.exe (PID: 6304 cmdline: C:\Users\user\Desktop\Package_details.exe MD5: CE3C5367FB067A45F5FA10C35CA23A28)
- dhcpmon.exe (PID: 4112 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: CE3C5367FB067A45F5FA10C35CA23A28)
  - dhcpmon.exe (PID: 5712 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: CE3C5367FB067A45F5FA10C35CA23A28)
- dhcpmon.exe (PID: 4604 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: CE3C5367FB067A45F5FA10C35CA23A28)
  - dhcpmon.exe (PID: 6236 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: CE3C5367FB067A45F5FA10C35CA23A28)
  - dhcpmon.exe (PID: 6296 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: CE3C5367FB067A45F5FA10C35CA23A28)
    - dhcpmon.exe (PID: 6532 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: CE3C5367FB067A45F5FA10C35CA23A28)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.254234385.000000000400000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x251e5:$x1: NanoCore.ClientPluginHost • 0x25222:$x2: IClientNetworkHost • 0x28d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000002.254234385.000000000400000.00000040.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x24f5d:$x1: NanoCore Client.exe • 0x251e5:$x2: NanoCore.ClientPluginHost • 0x2681e:$s1: PluginCommand • 0x26812:$s2: FileCommand • 0x276c3:$s3: PipeExists • 0x2d47a:$s4: PipeCreated • 0x2520f:$s5: IClientLoggingHost
0000000C.00000002.254234385.000000000400000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000002.254234385.000000000400000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x24f4d:$a: NanoCore • 0x24f5d:$a: NanoCore • 0x25191:$a: NanoCore • 0x251a5:$a: NanoCore • 0x251e5:$a: NanoCore • 0x24fac:$b: ClientPlugin • 0x251ae:$b: ClientPlugin • 0x251ee:$b: ClientPlugin • 0x250d3:$c: ProjectData • 0x25ada:$d: DESCrypto • 0x2d4a6:$e: KeepAlive • 0x2b494:$g: LogClientMessage • 0x2768f:$i: get_Connected • 0x25e10:$j: #=q • 0x25e40:$j: #=q • 0x25e5c:$j: #=q • 0x25e8c:$j: #=q • 0x25ea8:$j: #=q • 0x25ec4:$j: #=q • 0x25ef4:$j: #=q • 0x25f10:$j: #=q
00000015.00000002.279047270.0000000002F10000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 96 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.dhcpmon.exe.5760000.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
12.2.dhcpmon.exe.5760000.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
12.2.dhcpmon.exe.5760000.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
12.2.dhcpmon.exe.5760000.2.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
19.2.Package_details.exe.2970000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 103 entries				

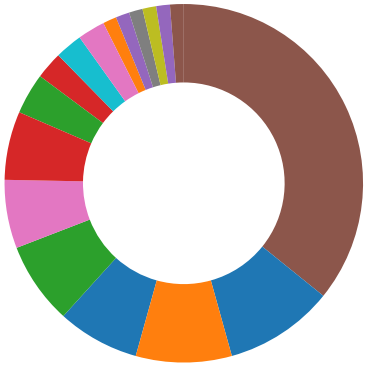
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

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)

Connects to many ports of the same IP (likely port scanning)

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (creates a PE file in dynamic memory)

.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)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

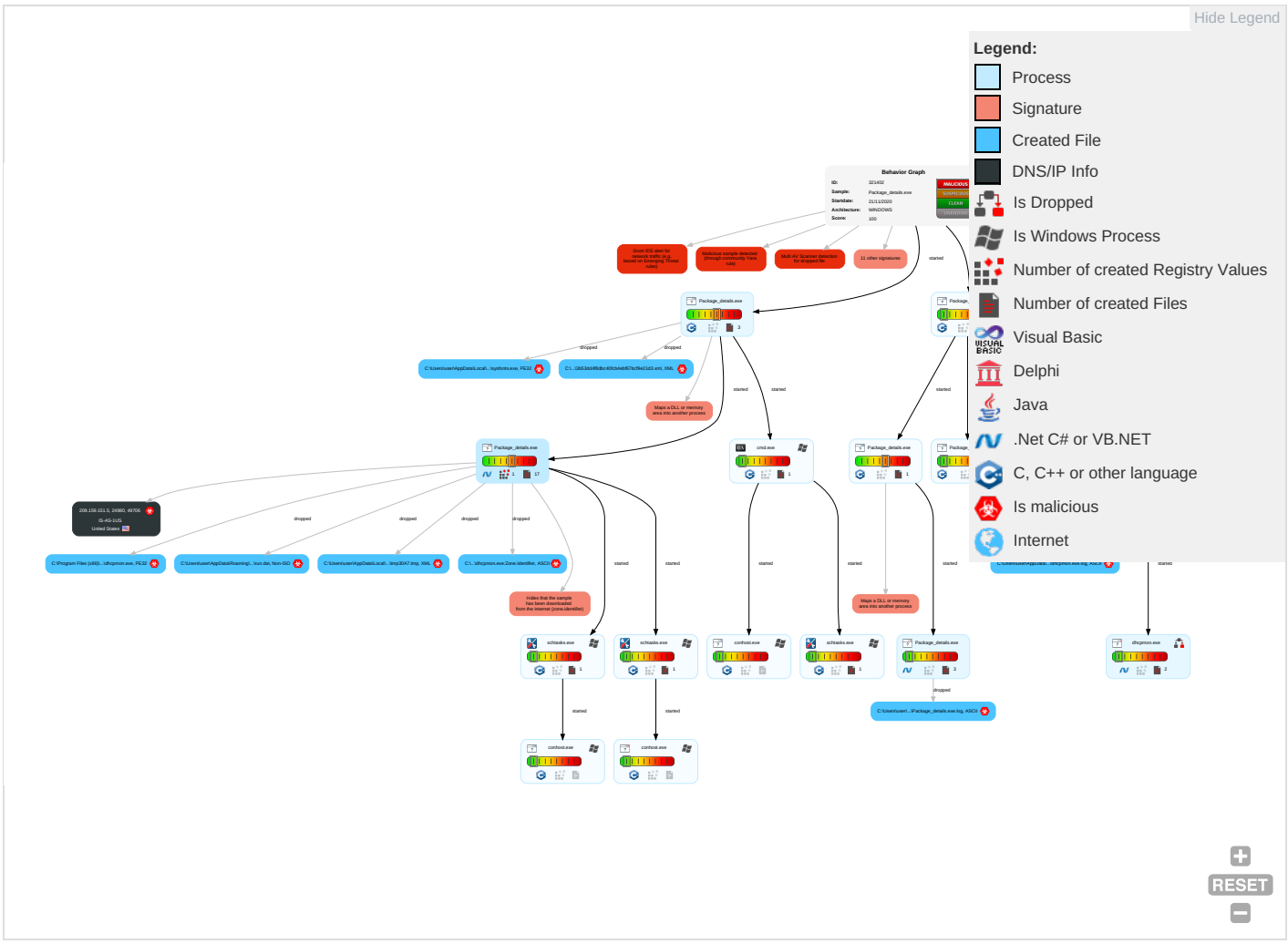
Detected Nanocore Rat

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 2	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	Command and Scripting Interpreter 3	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 1	NTDS	System Information Discovery 2 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Security Software Discovery 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 2	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	Hidden Files and Directories 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

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
Package_details.exe	25%	ReversingLabs		
Package_details.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AppData\sysfonts.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	35%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	25%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Package_details.exe.3160000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.2.dhcpmon.exe.2420000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.2.Package_details.exe.25c0000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
21.2.dhcpmon.exe.5470000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.Package_details.exe.1910000.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.2.Package_details.exe.2fb0000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.2.dhcpmon.exe.df0000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
14.2.Package_details.exe.2db0000.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.2.Package_details.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
18.2.dhcpmon.exe.2a40000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.2.dhcpmon.exe.2600000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.2.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.dhcpmon.exe.57b0000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.Package_details.exe.d10000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.2.dhcpmon.exe.2ae0000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
21.2.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
18.2.dhcpmon.exe.1040000.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.2.Package_details.exe.2ad0000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

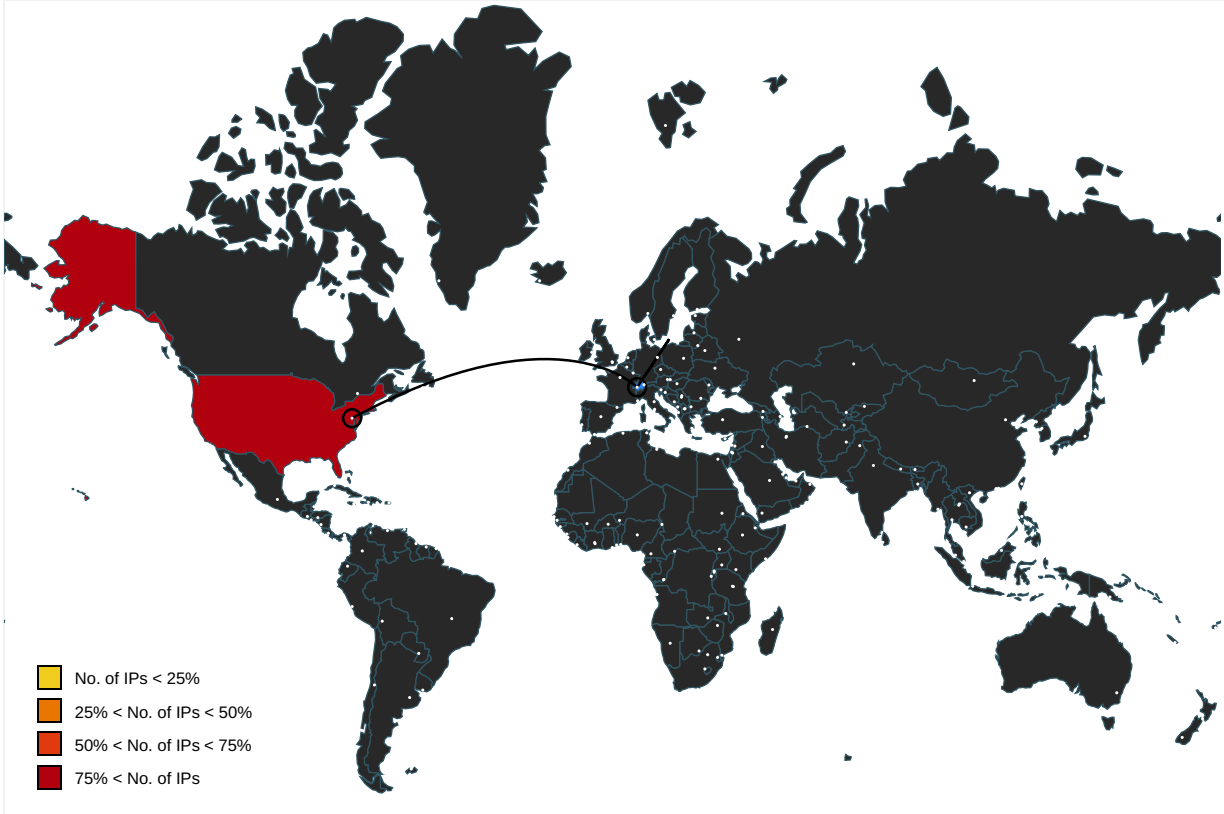
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.159.151.5	unknown	United States		19318	IS-AS-1US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321402
Start date:	21.11.2020
Start time:	15:28:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Package_details.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	38
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@31/13@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 76.6% (good quality ratio 72.5%) • Quality average: 80.7% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 82% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • 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 exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:29:05	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
15:29:06	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Package_details.exe" s>$(Arg0)
15:29:06	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
15:29:06	API Interceptor	964x Sleep call for process: Package_details.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IS-AS-1US	http://https://bakrisoil.com/wp-content/cd.php?e=gjeffries@hughesellard.com	Get hash	malicious	Browse	• 104.218.51.229
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 66.45.248.130
	http://https://encrypt.poweradz.net/	Get hash	malicious	Browse	• 209.159.158.130
	http://encrypt.poweradz.net	Get hash	malicious	Browse	• 209.159.158.130
	eLaaw7SqMi.exe	Get hash	malicious	Browse	• 104.37.188.231
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 66.45.248.130
	Invoice_334654_168522_from_Inc.xlsm	Get hash	malicious	Browse	• 216.219.81.3
	Invoice_403372_917428_from_Inc.xlsm	Get hash	malicious	Browse	• 216.219.81.3
	IQtvZjIdhN.exe	Get hash	malicious	Browse	• 66.45.248.130
	Req-87086782-8575.htm	Get hash	malicious	Browse	• 66.45.228.57
	148wWoi8vI.exe	Get hash	malicious	Browse	• 66.45.248.130
	wZ6ARBLKPj.exe	Get hash	malicious	Browse	• 69.10.42.234
	Attachments_240369 475265.doc	Get hash	malicious	Browse	• 216.219.81.50
	AGENT APPOINTMENT.xlsm	Get hash	malicious	Browse	• 216.158.225.211
	isb777amx.exe	Get hash	malicious	Browse	• 66.23.227.135
	http://https://venushome-my.sharepoint.com/:b:/g/personal/nsh_venushomeappliances_com/EX5FneZcfnZMndmJcDSa_toBsLtKOV-PlkwfYKs_6Hf8sA?e=I7myHO	Get hash	malicious	Browse	• 206.72.203.52
	test9.exe	Get hash	malicious	Browse	• 66.45.228.160
	http://https://firebasestorage.googleapis.com/v0/b/iouyfgjkgh.appspot.com/o/WEBMAIL.html?alt=media&token=f21ff97e-0c97-456a-9a4b-10962301f5d2#salim.mamlouk@holding-kamph.com	Get hash	malicious	Browse	• 64.20.38.219
	http://https://firebasestorage.googleapis.com/v0/b/nnajnr.appspot.com/o/WEBMAIL.html?alt=media&token=de90d2b5-b8b1-4623-87f1-c5411b10395b#asegura@talgo.com	Get hash	malicious	Browse	• 64.20.38.219
	http://https://firebasestorage.googleapis.com/v0/b/nnajnr.appspot.com/o/WEBMAIL.html?alt=media&token=de90d2b5-b8b1-4623-87f1-c5411b10395b#ialcalde@talgo.com	Get hash	malicious	Browse	• 64.20.38.219

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Package_details.exe

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	508416
Entropy (8bit):	7.553173588079667
Encrypted:	false
SSDEEP:	12288:VYuE3woImTkWfHrqWWBKZ8r/VkZhRChRr+FDszyNghK:VYuE3woLdHr7WqnA37WNp
MD5:	CE3C5367FB067A45F5FA10C35CA23A28
SHA1:	9D0F4D746747A6FD13A48B1A867EB8D103D9DAEC
SHA-256:	E4FC20492ED4F4750766382F6578D84F38BF680646EB6B5193C5733925941F67
SHA-512:	AE46E93DD82128EFD0C1F8DAB094B7A51716A6BCDE6053A66EFDD8724115E7B6D4A0FAB1CAF0775482F358488EDEFE81BECDD01A2A820FBA9B338C30CB2D8A07
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 35%, Browse • Antivirus: ReversingLabs, Detection: 25%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(k-.I.C.I.C.I.C..|..{.C..|..Z.C..|....C.er..c.C.I.B...C..|..m.C..|..m.C..|..m.C.Richl.C.....PE..L....._.....h.....@.....@.....<.....`.....(.....text..... ..`.rdata..4W.....X.....@..@.data.....P...h...0.....@....rsrc...`.....@..@.reloc...!.....".^.....@..B.....

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

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Package_details.exe.log	
Process:	C:\Users\user\Desktop\Package_details.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_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):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\3b53dd4f8dbc40fcb4ebf67bcf9e21d3.xml	
Process:	C:\Users\user\Desktop\Package_details.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1292
Entropy (8bit):	5.2398518553165365
Encrypted:	false
SSDEEP:	24:2do4+S8TcqdgrnIgFwvXVIrovlgU3ODOiIQRvh7hwZgvw43aVdy7Tbn:c+XBgzgXVIrovl33ODOiLdKZgfoI7/
MD5:	5363971BB4E75D190780EAE4B297A7DC
SHA1:	5A8A8BE876670C7B4502A40EBDB1A91BE55FA164
SHA-256:	4EE8F1603518DCD73AF9B0B1DC170826489587561BB8F35910A2A673AC077395
SHA-512:	7A4AE7E2590494D4B4CCD133453E160594A060AA9B4FD3E1175EDFA6D3B214E62BF3D72E9929A36A210377EF7AEBB75195165AEC57685B7B519656EF19A3996F
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>2015-09-27T14:27:44.8929027</Date > .<Author>549163\user</Author>.</RegistrationInfo>.<Triggers>.<LogonTrigger>.<Enabled>true</Enabled>.<UserId>549163\user</UserId>.</LogonTrigger>.<RegistrationTrigger>.<Enabled>false</Enabled>.</RegistrationTrigger>.</Triggers>.<Principals>.<Principal id="Author">.<UserId>549163\user</UserId>.<LogonType>InteractiveToken</LogonType>.<RunLevel>LeastPrivilege</RunLevel>.</Principal>.</Principals>.<Settings>.<MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.<AllowHardTerminate>false</AllowHardTerminate>.<StartWhenAvailable>true</StartWhenAvailable>.<RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.<IdleSettings>.<StopOnIdleEnd>true</StopOnIdleEnd>.<RestartOnIdle>false</RestartOnIdle>.</IdleSettings>.<AllowStartOnDemand>true</AllowStartOnDemand>.<Enabled>true</Enabled>.<Hidden>fals

C:\Users\user\AppData\Local\Temp\AppData\sysfonts.exe	
Process:	C:\Users\user\Desktop\Package_details.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	508426
Entropy (8bit):	7.5530920458361335
Encrypted:	false
SSDEEP:	12288:VYuE3woImTkWfHrqWWBKZ8r/VkZhRChRr+FDszyNgh:VYuE3woLdHr7WqnA37WN
MD5:	AC793C4CE42F9F1FA9158ECD6B234DDE
SHA1:	C336CDC682DF1BCE80AFEFB202E048BDA3762725
SHA-256:	51B557C38973A019AD7B894AA7A0B4ACA9696D4AD3523447CCE6181ABEB3938C
SHA-512:	90068F8729CC3D9A3A94A0BCF37843F0BFB0AEB471CE92BB5BB403F3F93D4223C962ABBA821839E53AA70E7AFB97C4FEA84C6A2A6FE7EC3A8DA56AFA6D4E021F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(k-.I.C.I.C.I.C..|..{.C..|..Z.C..|....C.er..c.C.I.B...C..|..m.C..|..m.C..|..m.C.Richl.C.....PE..L....._.....h.....@.....@.....<.....`.....(.....text..... ..`.rdata..4W.....X.....@..@.data.....P...h...0.....@....rsrc...`.....@..@.reloc...!....."...^.....@..B.....

C:\Users\user\AppData\Local\Temp\tmp30A7.tmp	
Process:	C:\Users\user\Desktop\Package_details.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1305
Entropy (8bit):	5.0992916127163666
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0fL3xtn:cbk4oL600QydbQxIYODOLedq3czj
MD5:	DE07D5279DEEC6B525C123125016B4C2
SHA1:	FA6EEC4A236E84B2506DD4280A4B24FD9124CC58
SHA-256:	A62ABE7A8B7A3D5F70CABD49CCBF12DE474E0BFBA21A0A8FC46800FCF48E0C52
SHA-512:	098CB099A869046494CDC4B9832A5C9FBE987ED53581D05767C17E5C2BD4A85177F8B7D0CBD879FE61238AD4450E7987FF0E5BF2D11FF024963F606FD78BA9C
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\tmp30A7.tmp	
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\tmp33C5.tmp	
Process:	C:\Users\user\Desktop\Package_details.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\Package_details.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF385 1
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.....[.&

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Package_details.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:An:A
MD5:	8B38108DFF8545452009901160E26753
SHA1:	73D5ED40FA083606029C1CE61B04B0B0D1961CA5
SHA-256:	E07631DD52B828F997192DB13896AC110DC113C01E16C1CE096DAD1B1745D8D4
SHA-512:	4E801BFFD3569125D1D8C2D3AA14F35D85D3103EFFE11C0E03A2299A6158EB9C85DB8C1790CD98D52AA14903B9C4082FB5869581370D239FD6921254BD072EC
Malicious:	**true**
Preview:	.{=<u..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Package_details.exe
File Type:	data
Category:	modified

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
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\Package_details.exe
File Type:	data
Category:	dropped
Size (bytes):	426832
Entropy (8bit):	**7.999527918131335**
Encrypted:	**true**
SSDEEP:	6144:zKfHbamD8WN+JQYrjM7Ei2CsFJjyh9zvgPonV5HqZcPVT4Eb+Z6no3QSzjeMsdF/:zKf137EiDsTjevgArYcPVLoTQS+0iv
MD5:	653DDDCB6C89F6EC51F3DDC0053C5914
SHA1:	4CF7E7D42495CE01C261E4C5C4B8BF6CD76CCEE5
SHA-256:	83B9CAE66800C768887FB270728F6806CBEBDEAD9946FA730F01723847F17FF9
SHA-512:	27A467F2364C21CD1C6C34EF1CA5FFB09B4C3180FC9C025E293374EB807E4382108617BB4B97F8EBBC27581CD6E5988BB5E21276B3CB829C1C0E49A6FC9463A
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.I'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`'].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&... .g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\Package_details.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.26113230362812
Encrypted:	false
SSDEEP:	3:oNWXp5v1E0iIM4A:oNWXpFO0RrA
MD5:	4CACDC973783E93B39FD939846A38F73
SHA1:	8C863E75701DC2F9E1E2233672CDE785603B4E98
SHA-256:	674E347C8427347CBAC62DB1B722FE6D5C03FF9E23A9E9F6891AF918B53D61FD
SHA-512:	E2A0A113661E57571B5F0F3548F12DC51BAD04607D4A223EE9E340B5B394F8DD0D2AB3E5B105AE246CC70AF5676EDAA6A7350607973F8AF07E8F1BE6E63EBD0 5
Malicious:	false
Preview:	C:\Users\user\Desktop\Package_details.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.553173588079667
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Package_details.exe
File size:	508416
MD5:	ce3c5367fb067a45f5fa10c35ca23a28
SHA1:	9d0f4d746747a6fd13a48b1a867eb8d103d9daec

General

SHA256:	e4fc20492ed4f4750766382f6578d84f38bf680646eb6b5193c5733925941f67
SHA512:	ae46e93dd82128efd0c1f8dab094b7a51716a6bcde6053a66efdd8724115e7b6d4a0fab1caf0775482f358488edefe81becdd01a2a820fba9b338c30cb2d8a07
SSDEEP:	12288:VYuE3woImTkWfHrqWWBKZ8r/VkZhRChRr+FDszyNghK:VYuE3woLdHr7WqnA37WNp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(k-.l.C.l.C.l.C..|..{.C..|..Z.C..|....C.er..c.C.l.B...C..|..m.C..|..m.C..|..m.C.Richl.C.....PE..L....._...

File Icon

Icon Hash:	7cf292aecae8e896

Static PE Info

General

Entrypoint:	0x40af68
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB8ACF5 [Sat Nov 21 06:00:21 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fe91cd96af1348223f21fb3d7bcc19bd

Entrypoint Preview

Instruction
call 00007F9BA0A750F2h
jmp 00007F9BA0A6DB4Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
xor ecx, ecx
cmp eax, dword ptr [004253E0h+ecx*8]
je 00007F9BA0A6DCD5h
inc ecx
cmp ecx, 2Dh
jc 00007F9BA0A6DCB3h
lea ecx, dword ptr [eax-13h]
cmp ecx, 11h
jnbe 00007F9BA0A6DCD0h
push 0000000Dh
pop eax
pop ebp
ret
mov eax, dword ptr [004253E4h+ecx*8]
pop ebp
ret
add eax, FFFFFF44h

Instruction
push 0000000Eh
pop ecx
cmp ecx, eax
sbb eax, eax
and eax, ecx
add eax, 08h
pop ebp
ret
call 00007F9BA0A73905h
test eax, eax
jne 00007F9BA0A6DCC8h
mov eax, 00425548h
ret
add eax, 08h
ret
call 00007F9BA0A738F2h
test eax, eax
jne 00007F9BA0A6DCC8h
mov eax, 0042554Ch
ret
add eax, 0Ch
ret
mov edi, edi
push ebp
mov ebp, esp
push esi
call 00007F9BA0A6DCA7h
mov ecx, dword ptr [ebp+08h]
push ecx
mov dword ptr [eax], ecx
call 00007F9BA0A6DC47h
pop ecx
mov esi, eax
call 00007F9BA0A6DC81h
mov dword ptr [eax], esi
pop esi
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 4Ch
mov eax, dword ptr [00425810h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
xor ebx, ebx
push esi
mov esi, dword ptr [ebp+08h]
push edi
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-1Ch], ebx
mov dword ptr [ebp-20h], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-24h], ebx
mov dword ptr [ebp-4Ch], esi
mov dword ptr [ebp-48h], ebx
cmp dword ptr [esi+14h], ebx

Rich Headers

Programming Language:	• [LNK] VS2010 build 30319 • [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [C++] VS2010 build 30319 • [RES] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x23cb0	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2f000	0xc560	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3c000	0x1628	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1f000	0x1c8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1d3d7	0x1d400	False	0.554587339744	data	6.66584733231	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1f000	0x5734	0x5800	False	0.364479758523	data	4.98964076212	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x25000	0x9880	0x6800	False	0.806114783654	data	7.41513673267	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2f000	0xc560	0xc600	False	0.377308238636	data	4.9790039799	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3c000	0x21ac	0x2200	False	0.522977941176	data	5.07781530691	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2f2b0	0x800	data	English	United States
RT_ICON	0x2fab0	0x400	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2291108095, next used block 136	English	United States
RT_ICON	0x2feb0	0x200	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x300b0	0x1000	data	English	United States
RT_ICON	0x310b0	0xa00	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 16119029, next used block 15988220	English	United States
RT_ICON	0x31ab0	0x800	data	English	United States
RT_ICON	0x322b0	0x600	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x328b0	0x4400	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 252, next used block 4294902016	English	United States
RT_ICON	0x36cb0	0x2600	data	English	United States
RT_ICON	0x392b0	0x1200	data	English	United States
RT_ICON	0x3a4b0	0xa00	data	English	United States
RT_ICON	0x3aeb0	0x600	GLS_BINARY_LSB_FIRST	English	United States
RT_GROUP_ICON	0x3b4b0	0xae	data	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	WaitForSingleObject, GetExitCodeProcess, HeapReAlloc, IsValidLocale, EnumSystemLocalesA, GetLocaleInfoA, CreateProcessA, CloseHandle, SetFilePointer, ReadFile, FlushFileBuffers, GetConsoleMode, GetConsoleCP, HeapSize, IsValidCodePage, GetOEMCP, GetACP, GetStringTypeW, WriteConsoleW, SetStdHandle, CompareStringW, SetEnvironmentVariableA, GetUserDefaultLCID, VirtualProtect, WideCharToMultiByte, InterlockedIncrement, InterlockedDecrement, InterlockedExchange, MultiByteToWideChar, EncodePointer, DecodePointer, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, GetLastError, HeapFree, GetProcAddress, GetModuleHandleW, ExitProcess, GetCommandLineW, HeapSetInformation, GetStartupInfoW, GetCPInfo, RaiseException, RtlUnwind, HeapAlloc, LCMapStringW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, TerminateProcess, GetCurrentProcess, IsProcessorFeaturePresent, HeapCreate, GetFileAttributesA, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, SetLastError, GetCurrentThreadId, InitializeCriticalSectionAndSpinCount, LoadLibraryW, GetLocaleInfoW, WriteFile, GetStdHandle, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, CreateFileW
MSVFW32.dll	ICGetInfo, ICSeqCompressFrameStart, ICCompressorChoose, ICSeqCompressFrame
AVIFIL32.dll	AVIMakeStreamFromClipboard, AVIClearClipboard, AVIStreamOpenFromFile, AVIStreamRead
wsnmp32.dll	
SETUPAPI.dll	SetupDiCreateDeviceInterfaceRegKeyA, SetupDiInstallClassExA, SetupDiEnumDriverInfoW, SetupDiBuildDriverInfoList, SetupRenameErrorA, SetupDefaultQueueCallback, SetupInstallFilesFromInfSectionA
SHELL32.dll	SHFileOperationA, ShellHookProc, DragQueryFile
COMDLG32.dll	ReplaceTextW, ReplaceTextA, PrintDlgW, PrintDlgExW, CommDlgExtendedError, PrintDlgExA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/21/20-15:29:06.823457	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	24980	192.168.2.3	209.159.151.5

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 15:29:06.684222937 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:06.788212061 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:06.788661003 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:06.823457003 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:06.939136028 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:06.951705933 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.056266069 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.074459076 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.230221987 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.230542898 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.250165939 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.250224113 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.250262976 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.250302076 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.250344038 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.250395060 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.250433922 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.250441074 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.250469923 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.250483990 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.250524044 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.250535965 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.250566959 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.250606060 CET	49706	24980	192.168.2.3	209.159.151.5

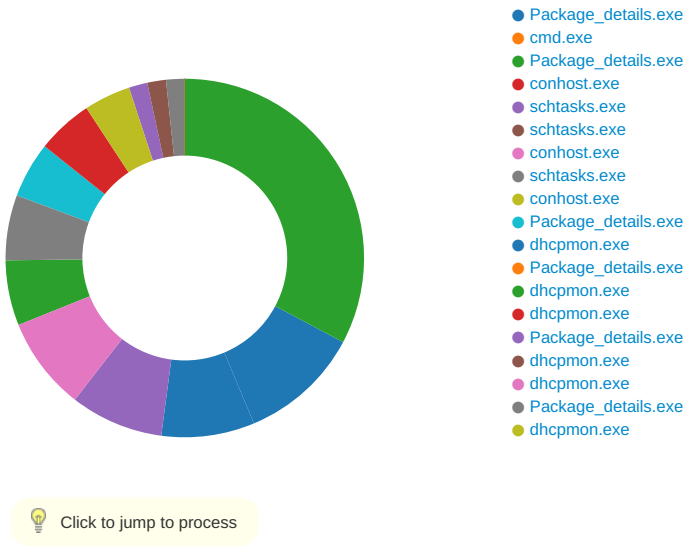
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 15:29:07.250683069 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.354428053 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354495049 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354535103 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354583979 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354629993 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354670048 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354708910 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354720116 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.354751110 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.354751110 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354758024 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.354793072 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354835987 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354846001 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.354876995 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354917049 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.354926109 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.354971886 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.355009079 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.355017900 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.355050087 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.355087042 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.355089903 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.355129004 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.355168104 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.355169058 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.355210066 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.355256081 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.355258942 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.355341911 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.459498882 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.459578991 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.459621906 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.459661007 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.459702969 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.459741116 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.459789991 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.459789991 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.459827900 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.459835052 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.459867954 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.459877014 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.459918976 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.459928036 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.459959030 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.459997892 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460002899 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.460038900 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460078955 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460097075 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.460129023 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460171938 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460200071 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.460211039 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460252047 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460280895 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.460293055 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460330009 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.460335016 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460377932 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460417032 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460465908 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460467100 CET	49706	24980	192.168.2.3	209.159.151.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 15:29:07.460510969 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460550070 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460562944 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.460591078 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460608959 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.460630894 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460668087 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460685015 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.460709095 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460748911 CET	24980	49706	209.159.151.5	192.168.2.3
Nov 21, 2020 15:29:07.460764885 CET	49706	24980	192.168.2.3	209.159.151.5
Nov 21, 2020 15:29:07.460798979 CET	24980	49706	209.159.151.5	192.168.2.3

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Package_details.exe PID: 1092 Parent PID: 5720

General

Start time:	15:28:56
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\Package_details.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Package_details.exe'
Imagebase:	0xd90000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.216025049.0000000001890000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.216025049.0000000001890000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.216025049.0000000001890000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.216025049.0000000001890000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	DB8CB6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\AppData\sysfonts.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DB8BFC	CreateFileW
C:\Users\user\AppData\Local\Temp\3b53dd4f8dbc40fcb4ebf67bcf9e21d3.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DBB16D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AppData\sysfonts.exe	unknown	508426	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 28 6b 2d ba 6c 0a 43 e9 6c 0a 43 e9 6c 0a 43 e9 03 7c dd e9 7b 0a 43 e9 03 7c e8 e9 5a 0a 43 e9 03 7c e9 e9 f9 0a 43 e9 65 72 d0 e9 63 0a 43 e9 6c 0a 42 e9 1d 0a 43 e9 03 7c ec e9 6d 0a 43 e9 03 7c d9 e9 6d 0a 43 e9 03 7c de e9 6d 0a 43 e9 52 69 63 68 6c 0a 43 e9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 f5 ac b8 5f 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode....$.......(k- .l.C.l.C.l.C..|..{. C..|..Z.C..|....C.er..c.C.l.B. ..C..|..m.C..|..m.C..|..m.C.R ichl.C........................ PE..L......_...	success or wait	1	DB8C15	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3b53dd4f8dbc40fcb4ebf67bcf9e21d3.xml	unknown	1292	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 20 3d 20 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 3c 44 61 74 65 3e 32 30 31 35 2d 30 39 2d 32 37 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 20 3e 20 0a 3c 41 75 74 68 6f 72 3e 35 34 39 31 36 33 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0a 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 3c 54 72 69 67 67 65 72 73 3e 0a 3c 4c 6f 67 6f 6e 54	<?xml version="1.0" encoding="UTF-16"?>.<Task version = "1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.<RegistrationInfo>.<Date>2015-09-27T14:27:44.8929027</Date > .<Author>549163\user</Author>.</RegistrationInfo>.<Triggers>.<LogonT	success or wait	1	DBB19C	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Package_details.exe	unknown	508416	success or wait	1	DB8BC2	ReadFile
C:\Users\user\Desktop\Package_details.exe	unknown	508416	success or wait	1	DB8564	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile

Analysis Process: cmd.exe PID: 4092 Parent PID: 1092

General

Start time:	15:29:02
Start date:	21/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c schtasks /Create /TN fonts /XML 'C:\Users\user\AppData\Local\Temp\3b53dd4f8dbc40fcb4ebf67bcf9e21d3.xml'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: Package_details.exe PID: 4156 Parent PID: 1092

General

Start time:	15:29:02
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\Package_details.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Package_details.exe
Imagebase:	0xd90000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000002.00000003.223529798.0000000004BEB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	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	5B70A09	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	5B70B03	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	5B70A09	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	5B70D88	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	5B70D88	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp30A7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5B70F84	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	5B70B03	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp33C5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5B70F84	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	5B70A09	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	5B70A09	CreateDirectoryW
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	72FB60AC	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	72FB60AC	unknown
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	1	5B70B03	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	5B70B03	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	5B70B03	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp30A7.tmp	success or wait	1	5B7030E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp33C5.tmp	success or wait	1	5B7030E	DeleteFileW
C:\Users\user\Desktop\Package_details.exe:Zone.Identifier	success or wait	1	5B713B5	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	de 7b 3d 3c 75 8e d8 48	.{=<u..H	success or wait	1	5B70CBB	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe</td><td>0</td><td>131072</td><td>4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 28 6b 2d ba 6c 0a 43 e9 6c 0a 43 e9 6c 0a 43 e9 03 7c dd e9 7b 0a 43 e9 03 7c e8 e9 5a 0a 43 e9 03 7c e9 e9 f9 0a 43 e9 65 72 d0 e9 63 0a 43 e9 6c 0a 42 e9 1d 0a 43 e9 03 7c ec e9 6d 0a 43 e9 03 7c d9 e9 6d 0a 43 e9 03 7c de e9 6d 0a 43 e9 52 69 63 68 6c 0a 43 e9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 f5 ac b8 5f 00 00 00</td><td>MZ......................@.....
....
............!..L.!This program
cannot be run in DOS
mode....$.......(k-
.l.C.l.C.l.C..|..{.
C..|..Z.C..|....C.er..c.C.l.B.
..C..|..m.C..|..m.C..|..m.C.R
ichl.C........................
PE..L......_...</td><td>success or wait</td><td>4</td><td>5B70D88</td><td>CopyFileW</td></tr>
<tr><td>C:\Program Files (x86)\DHCP Mo
nitor\dhcpmon.exe:Zone.Identifier</td><td>0</td><td>26</td><td>5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30</td><td>[ZoneTransfer]....ZoneId=0</td><td>success or wait</td><td>1</td><td>5B70D88</td><td>CopyFileW</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\tmp30A7.tmp</td><td>unknown</td><td>1305</td><td>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</td><td><?xml version="1.0"
encoding="UTF-16"?>..
<Task version="1.2"
xmlns="http://schemas.mic
roso
ft.com/windows/2004/02/m
it/task">..
<RegistrationInfo />..
<Triggers />..
<Principals>..   <Principal
id="Author">..
<LogonType>InteractiveTo
ken</LogonType></td><td>success or wait</td><td>1</td><td>5B70CBB</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-
955C-4899F5F57B9A\task.dat</td><td>unknown</td><td>42</td><td>43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 50 61 63 6b 61 67 65 5f 64 65 74 61 69 6c 73 2e 65 78 65</td><td>C:\Users\user\Desktop\Pa
ckage_details.exe</td><td>success or wait</td><td>1</td><td>5B70CBB</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp33C5.tmp	unknown	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.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	5B70CBB	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	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.....[.&	success or wait	1	5B70CBB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	426832	c1 e9 67 26 6a 6f 1f 01 d5 49 50 67 08 81 cd a2 47 4d d1 a4 d4 0d a7 52 3e 69 e1 fc 09 6f 8c b1 04 49 e1 3e e3 bb b0 26 9f 72 7b d6 fa a5 93 38 a9 d3 a5 93 7d ff da 89 8a 45 03 7f ea e6 96 76 cf 21 37 95 75 33 65 bc fc 20 fb c0 05 b7 f7 64 62 bd 90 15 7d b2 c7 1d 02 02 ab e8 22 c2 74 28 06 78 43 39 b8 63 70 15 42 e6 e0 91 e1 37 82 0f 1b 27 bd 93 ad a1 d3 7f c2 25 bd 09 b2 06 eb c7 77 86 5e ac c1 5f 13 c4 d2 02 d8 9d d4 b4 f1 42 b7 57 25 fd 3c ce a6 d9 a4 69 e1 30 d1 7b 39 bb 78 53 fc ab fb 35 c5 d8 c7 29 05 ef 77 ca 0f 24 14 92 43 87 80 3f 60 46 d7 8f da 75 a8 35 db 92 54 b6 58 ab 77 27 53 69 f4 f0 7a b2 6e 7b 8f ef b9 ea 9f 84 59 21 6d d8 d3 1c 52 41 f8 b9 e3 78 67 d3 d0 ba 03 e9 5b 37 8a 18 89 7a b7 9f 39 40 02 4b ca 2d 9a fe 88 54 95 8d 2b d8 41 43 65	..g&jo...IPg....GM.....R>i...o ...I.>...&.r{....8....}....E.. ...v.!7.u3e.. .....db...}..... ..".t(.xC9.cp.B....7...'..... .%.....w.^._.....B.W%.<. ...i.0.{9.xS...5...)..w..$..C..? `F...u.5..T.X.w'Si..z.n{.... ..Y!m...RA...xg..... [7...z..9@.K.-...T..+.ACe	success or wait	1	5B70CBB	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	5B70CBB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	4	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5B70CBB	ReadFile

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	5B70E7A	RegSetValueExW

Analysis Process: conhost.exe PID: 2296 Parent PID: 4092

General

Start time:	15:29:02
Start date:	21/11/2020

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: 5464 Parent PID: 4092

General

Start time:	15:29:02
Start date:	21/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /Create /TN fonts /XML 'C:\Users\user\AppData\Local\Temp\3b53dd4f8dbc40fcb4ebf67bcf9e21d3.xml'
Imagebase:	0xe60000
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\3b53dd4f8dbc40fcb4ebf67bcf9e21d3.xml	unknown	2	success or wait	1	E6AB22	ReadFile
C:\Users\user\AppData\Local\Temp\3b53dd4f8dbc40fcb4ebf67bcf9e21d3.xml	unknown	1293	success or wait	1	E6ABD9	ReadFile

Analysis Process: schtasks.exe PID: 5592 Parent PID: 4156

General

Start time:	15:29:04
Start date:	21/11/2020
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\tmp30A7.tmp'
Imagebase:	0xe60000
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\tmp30A7.tmp	unknown	2	success or wait	1	E6AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp30A7.tmp	unknown	1306	success or wait	1	E6ABD9	ReadFile

Analysis Process: conhost.exe PID: 5548 Parent PID: 5592

General

Start time:	15:29:05
Start date:	21/11/2020
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: 5108 Parent PID: 4156

General

Start time:	15:29:05
Start date:	21/11/2020
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\tmp33C5.tmp'
Imagebase:	0xe60000
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\tmp33C5.tmp	unknown	2	success or wait	1	E6AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp33C5.tmp	unknown	1311	success or wait	1	E6ABD9	ReadFile

Analysis Process: conhost.exe PID: 1560 Parent PID: 5108

General

Start time:	15:29:05
Start date:	21/11/2020
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: Package_details.exe PID: 5804 Parent PID: 528

General

Start time:	15:29:06
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\Package_details.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Package_details.exe 0
Imagebase:	0xd90000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.239365689.00000000024E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.239365689.00000000024E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.239365689.00000000024E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.239365689.00000000024E0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AppData\sysfonts.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	DB8BFC	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>unknown</td><td>unknown</td><td>508426</td><td>4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 28 6b 2d ba 6c 0a 43 e9 6c 0a 43 e9 6c 0a 43 e9 03 7c dd e9 7b 0a 43 e9 03 7c e8 e9 5a 0a 43 e9 03 7c e9 e9 f9 0a 43 e9 65 72 d0 e9 63 0a 43 e9 6c 0a 42 e9 1d 0a 43 e9 03 7c ec e9 6d 0a 43 e9 03 7c d9 e9 6d 0a 43 e9 03 7c de e9 6d 0a 43 e9 52 69 63 68 6c 0a 43 e9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 f5 ac b8 5f 00 00 00</td><td>MZ......................@.....
....
............!..L.!This program
cannot be run in DOS
mode....$.......(k-
.l.C.l.C.l.C..|..{.
C..|..Z.C..|....C.er..c.C.l.B.
..C..|..m.C..|..m.C..|..m.C.R
ichl.C.........................
PE..L......_...</td><td>invalid handle</td><td>1</td><td>DB8C15</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Package_details.exe	unknown	508416	success or wait	1	DB8BC2	ReadFile
C:\Users\user\Desktop\Package_details.exe	unknown	508416	success or wait	1	DB8564	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile

Analysis Process: dhcpmon.exe PID: 4112 Parent PID: 528

General

Start time:	15:29:06
Start date:	21/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x300000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.243043280.0000000002970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.243043280.0000000002970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.243043280.0000000002970000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.243043280.0000000002970000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, Virustotal, Browse • Detection: 25%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AppData\sysfonts.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	328BFC	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	508426	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 28 6b 2d ba 6c 0a 43 e9 6c 0a 43 e9 6c 0a 43 e9 03 7c dd e9 7b 0a 43 e9 03 7c e8 e9 5a 0a 43 e9 03 7c e9 e9 f9 0a 43 e9 65 72 d0 e9 63 0a 43 e9 6c 0a 42 e9 1d 0a 43 e9 03 7c ec e9 6d 0a 43 e9 03 7c d9 e9 6d 0a 43 e9 03 7c de e9 6d 0a 43 e9 52 69 63 68 6c 0a 43 e9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 f5 ac b8 5f 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode....$.......(k- .l.C.l.C.l.C..|..{. C..|..Z.C..|....C.er..c.C.l.B. ..C..|..m.C..|..m.C..|..m.C.R ichl.C......................... PE..L......_...	invalid handle	1	328C15	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	508416	success or wait	1	328BC2	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	508416	success or wait	1	328564	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile

Analysis Process: Package_details.exe PID: 4168 Parent PID: 5804

General

Start time:	15:29:12

Start date:	21/11/2020
Path:	C:\Users\user\Desktop\Package_details.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Package_details.exe
Imagebase:	0xd90000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: 5712 Parent PID: 4112

General

Start time:	15:29:12
Start date:	21/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x300000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
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: 0000000C.00000002.254234385.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.254234385.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.254234385.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.254234385.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.255480144.00000000057B2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.255480144.00000000057B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.255480144.00000000057B2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.254375322.00000000013D8000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.254375322.00000000013D8000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.254375322.00000000013D8000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.255256887.000000000365E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.255432280.0000000005760000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.255432280.0000000005760000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.255432280.0000000005760000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.255432280.0000000005760000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.255293475.0000000004651000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.255293475.0000000004651000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.255293475.0000000004651000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: dhcpmon.exe PID: 4604 Parent PID: 3388

General

Start time:	15:29:13
Start date:	21/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x300000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.250138622.00000000024A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.250138622.00000000024A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.250138622.00000000024A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.250138622.00000000024A0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AppData\sysfonts.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	328BFC	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	508426	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 28 6b 2d ba 6c 0a 43 e9 6c 0a 43 e9 6c 0a 43 e9 03 7c dd e9 7b 0a 43 e9 03 7c e8 e9 5a 0a 43 e9 03 7c e9 e9 f9 0a 43 e9 65 72 d0 e9 63 0a 43 e9 6c 0a 42 e9 1d 0a 43 e9 03 7c ec e9 6d 0a 43 e9 03 7c d9 e9 6d 0a 43 e9 03 7c de e9 6d 0a 43 e9 52 69 63 68 6c 0a 43 e9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 f5 ac b8 5f 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......(k- .l.C.l.C.l.C..|..{. C..|..Z.C..|....C.er..c.C.l.B. ..C..|..m.C..|..m.C..|..m.C.R ichl.C........................ PE..L......_...	invalid handle	1	328C15	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	508416	success or wait	1	328BC2	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	508416	success or wait	1	328564	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile

Analysis Process: Package_details.exe PID: 2140 Parent PID: 5804

General

Start time:	15:29:14
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\Package_details.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Package_details.exe
Imagebase:	0xd90000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.256685765.0000000001110000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.256685765.0000000001110000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.256685765.0000000001110000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.256685765.0000000001110000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AppData\sysfonts.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	DB8BFC	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	508426	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 28 6b 2d ba 6c 0a 43 e9 6c 0a 43 e9 6c 0a 43 e9 03 7c dd e9 7b 0a 43 e9 03 7c e8 e9 5a 0a 43 e9 03 7c e9 e9 f9 0a 43 e9 65 72 d0 e9 63 0a 43 e9 6c 0a 42 e9 1d 0a 43 e9 03 7c ec e9 6d 0a 43 e9 03 7c d9 e9 6d 0a 43 e9 03 7c de e9 6d 0a 43 e9 52 69 63 68 6c 0a 43 e9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 f5 ac b8 5f 00 00 00	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......(k-.l.C.l.C.l.C..|..{.C..|..Z.C..|....C.er..c.C.l.B...C..|..m.C..|..m.C..|..m.C.Richl.C.........................PE..L......_...	invalid handle	1	DB8C15	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Package_details.exe	unknown	508416	success or wait	1	DB8BC2	ReadFile
C:\Users\user\Desktop\Package_details.exe	unknown	508416	success or wait	1	DB8564	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	DB6FC9	ReadFile

Analysis Process: dhcpmon.exe PID: 6236 Parent PID: 4604

General

Start time:	15:29:19
Start date:	21/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x300000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: 6296 Parent PID: 4604

General

Start time:	15:29:20
Start date:	21/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x300000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.265645463.0000000000BA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.265645463.0000000000BA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.265645463.0000000000BA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.265645463.0000000000BA0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AppData\sysfonts.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	328BFC	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	508426	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 28 6b 2d ba 6c 0a 43 e9 6c 0a 43 e9 6c 0a 43 e9 03 7c dd e9 7b 0a 43 e9 03 7c e8 e9 5a 0a 43 e9 03 7c e9 e9 f9 0a 43 e9 65 72 d0 e9 63 0a 43 e9 6c 0a 42 e9 1d 0a 43 e9 03 7c ec e9 6d 0a 43 e9 03 7c d9 e9 6d 0a 43 e9 03 7c de e9 6d 0a 43 e9 52 69 63 68 6c 0a 43 e9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 f5 ac b8 5f 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......(k- .l.C.l.C.l.C..|..{. C..|..Z.C..|....C.er..c.C.l.B. ..C..|..m.C..|..m.C..|..m.C.R ichl.C........................ PE..L......_...	invalid handle	1	328C15	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	508416	success or wait	1	328BC2	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	508416	success or wait	1	328564	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	326FC9	ReadFile

Analysis Process: Package_details.exe PID: 6304 Parent PID: 2140

General

Start time:	15:29:20
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\Package_details.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Package_details.exe
Imagebase:	0xd90000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
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: 00000013.00000002.273459332.0000000003EC1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.273459332.0000000003EC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.273459332.0000000003EC1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.270080502.0000000002970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.270080502.0000000002970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.270080502.0000000002970000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.270080502.0000000002970000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.269469613.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.269469613.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.269469613.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.269469613.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.269644528.0000000000966000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.269644528.0000000000966000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.269644528.0000000000966000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.273427338.0000000002ECE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.270811037.0000000002AD2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.270811037.0000000002AD2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.270811037.0000000002AD2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Package_details.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Package_details.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: dhcpmon.exe PID: 6532 Parent PID: 6296

General

Start time:	15:29:25
Start date:	21/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x300000
File size:	508416 bytes
MD5 hash:	CE3C5367FB067A45F5FA10C35CA23A28
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: 00000015.00000002.279047270.0000000002F10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.279047270.0000000002F10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.279047270.0000000002F10000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.279047270.0000000002F10000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.279458357.00000000042D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.279458357.00000000042D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.279458357.00000000042D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.278607358.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.278607358.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.278607358.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.278607358.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.278916305.0000000001444000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.278916305.0000000001444000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.278916305.0000000001444000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.279548840.0000000005472000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.279548840.0000000005472000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.279548840.0000000005472000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.279433728.00000000032DE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Disassembly

Code Analysis