ID: 337761
Sample Name: Paypal Payment Authorization pdf.exe
Cookbook: default.jbs
Time: 08:25:19
Date: 10/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

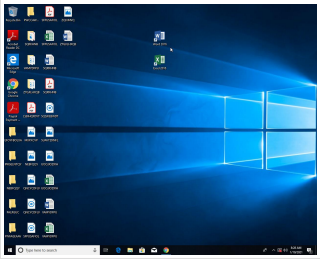
Analysis Report Paypal Payment Authorization pdf.exe

Overview

General Information

Sample Name:	Paypal Payment Authorization pdf.exe
Analysis ID:	337761
MD5:	43796c264cd571..
SHA1:	cd0af8e864d885c..
SHA256:	1d7e3f93b597143.
Tags:	exe NanoCore RAT

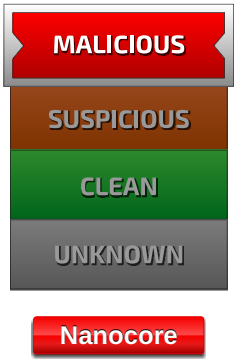
Most interesting Screenshot:



Errors

Sigma syntax error: Has an empty selector, Rule: Abusing Azure Browser SSO

Detection

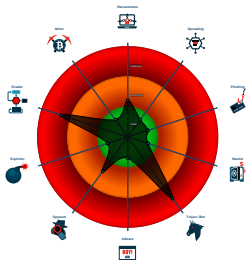


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Executable has a suspicious name (…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …

Classification



Startup

- **System is w10x64**
- Paypal Payment Authorization pdf.exe (PID: 4544 cmdline: 'C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe' MD5: 43796C264CD5716211CCA1333D02C545)
  - Paypal Payment Authorization pdf.exe (PID: 6136 cmdline: C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe MD5: 43796C264CD5716211CCA1333D02C545)
    - schtasks.exe (PID: 2800 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp2E95.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - dhcpmon.exe (PID: 788 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 43796C264CD5716211CCA1333D02C545)
    - schtasks.exe (PID: 5496 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp3184.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Paypal Payment Authorization pdf.exe (PID: 5444 cmdline: 'C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe' 0 MD5: 43796C264CD5716211CCA1333D02C545)
  - Paypal Payment Authorization pdf.exe (PID: 4348 cmdline: C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe MD5: 43796C264CD5716211CCA1333D02C545)
- dhcpmon.exe (PID: 5912 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 43796C264CD5716211CCA1333D02C545)
  - dhcpmon.exe (PID: 4928 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 43796C264CD5716211CCA1333D02C545)
- dhcpmon.exe (PID: 4352 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 43796C264CD5716211CCA1333D02C545)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "185.244.38.210"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.281240988.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000002.281240988.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000002.281240988.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000007.00000002.264202941.000000000395000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000007.00000002.264202941.000000000395000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x435bd:$a: NanoCore • 0x43616:$a: NanoCore • 0x43653:$a: NanoCore • 0x436cc:$a: NanoCore • 0x56d77:$a: NanoCore • 0x56d8c:$a: NanoCore • 0x56dc1:$a: NanoCore • 0x6fd4b:$a: NanoCore • 0x6fd60:$a: NanoCore • 0x6fd95:$a: NanoCore • 0x4361f:$b: ClientPlugin • 0x4365c:$b: ClientPlugin • 0x43f5a:$b: ClientPlugin • 0x43f67:$b: ClientPlugin • 0x56b33:$b: ClientPlugin • 0x56b4e:$b: ClientPlugin • 0x56b7e:$b: ClientPlugin • 0x56d95:$b: ClientPlugin • 0x56dca:$b: ClientPlugin • 0x6fb07:$b: ClientPlugin • 0x6fb22:$b: ClientPlugin
Click to see the 50 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
12.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
12.2.dhcpmon.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
12.2.dhcpmon.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
7.2.Paypal Payment Authorization pdf.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 7 entries				

Sigma Overview

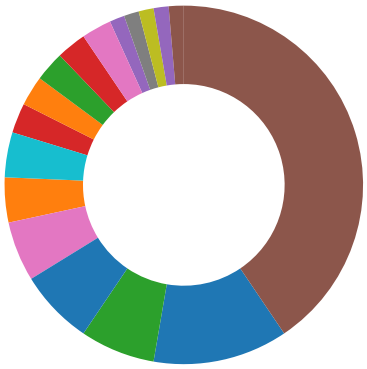
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Conhost Parent Proces Executions

Signature Overview



- AV Detection
- Compliance
- 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:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Found malware configuration

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:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

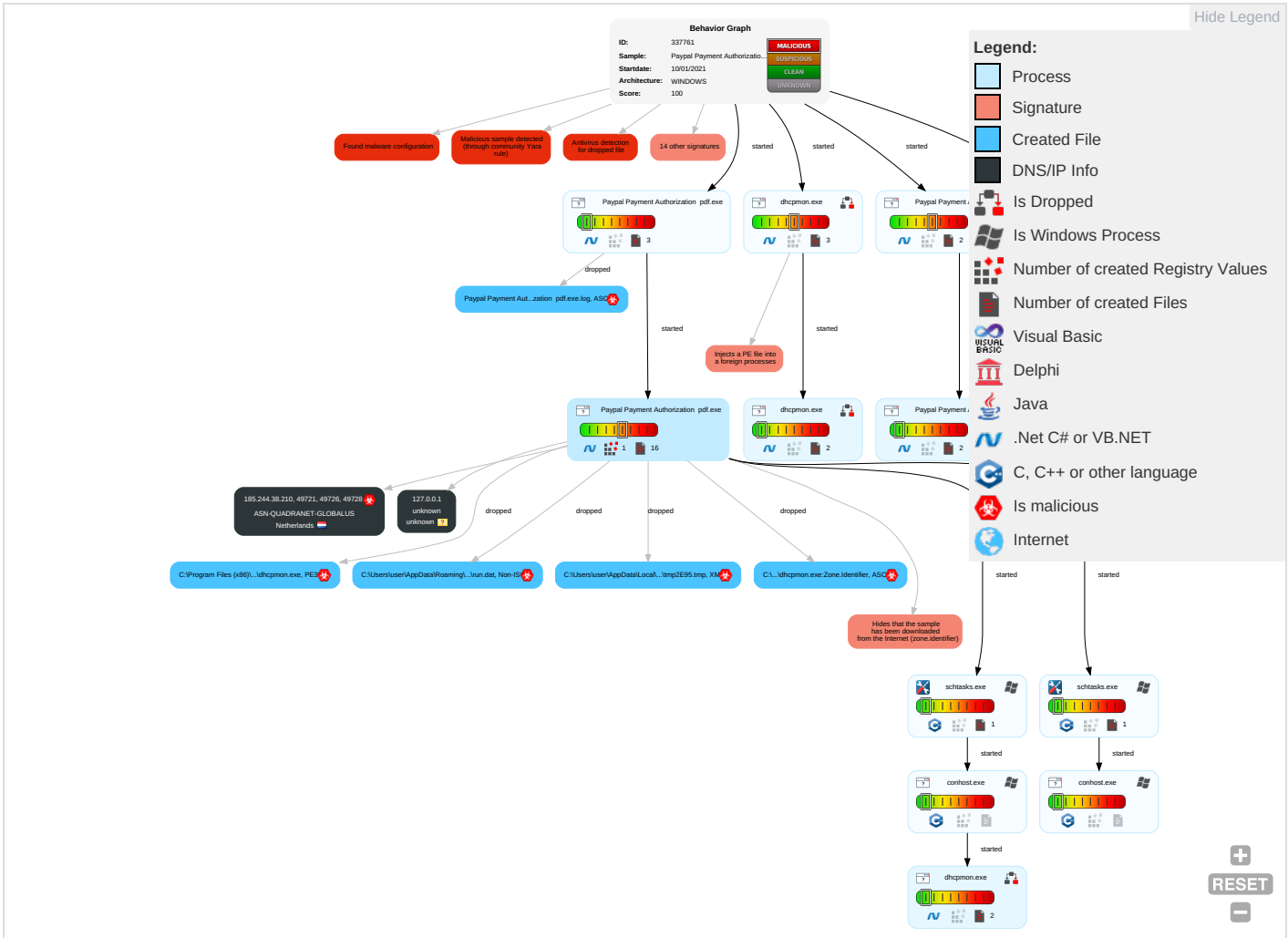
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 1	Masquerading 2	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

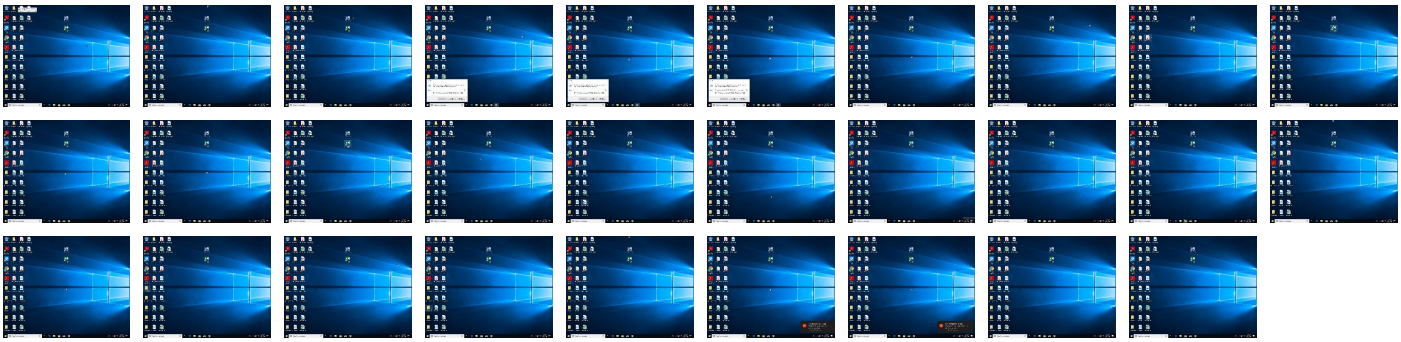
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Paypal Payment Authorization pdf.exe	52%	ReversingLabs	ByteCode-MSIL.Trojan.Cryptos	
Paypal Payment Authorization pdf.exe	100%	Avira	TR/Dropper.MSIL.Gen	
Paypal Payment Authorization pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	52%	ReversingLabs	ByteCode-MSIL.Trojan.Cryptos	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.dhcpmon.exe.470000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
0.0.Paypal Payment Authorization pdf.exe.440000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
6.2.Paypal Payment Authorization pdf.exe.930000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
12.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.dhcpmon.exe.450000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
8.0.dhcpmon.exe.470000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
6.0.Paypal Payment Authorization pdf.exe.930000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
10.0.dhcpmon.exe.9d0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
7.2.Paypal Payment Authorization pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.dhcpmon.exe.450000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
9.0.dhcpmon.exe.450000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
9.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.Paypal Payment Authorization pdf.exe.630000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
7.0.Paypal Payment Authorization pdf.exe.630000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
10.2.dhcpmon.exe.9d0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
0.2.Paypal Payment Authorization pdf.exe.440000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
1.0.Paypal Payment Authorization pdf.exe.ab0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
12.2.dhcpmon.exe.450000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File

Domains

No Antivirus matches

URLs

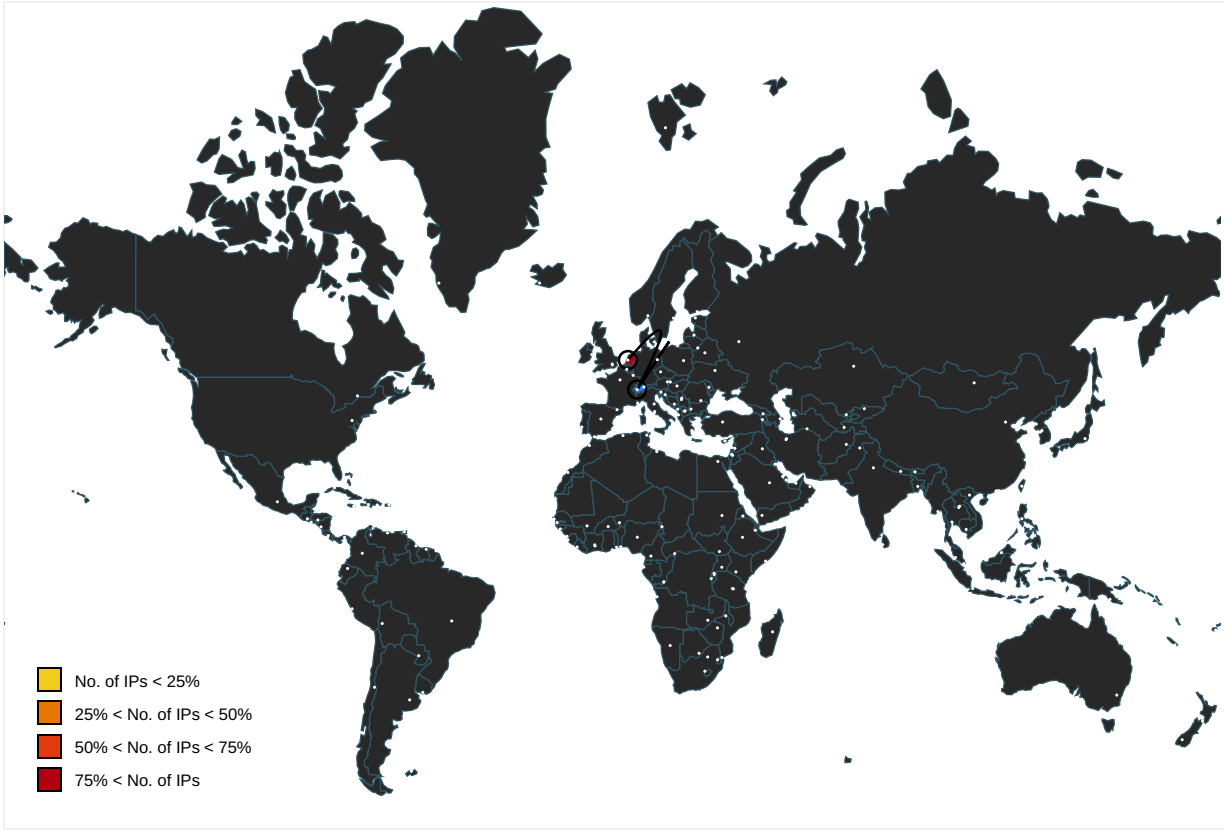
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.244.38.210	unknown	Netherlands		8100	ASN-QUADRANET-GLOBALUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337761
Start date:	10.01.2021
Start time:	08:25:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Paypal Payment Authorization pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@18/12@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 84.5% • Quality standard deviation: 15.5%
HCA Information:	• Successful, ratio: 93% • 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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found.
Errors:	• Sigma syntax error: Has an empty selector, Rule: Abusing Azure Browser SSO

Simulations

Behavior and APIs

Time	Type	Description
08:26:14	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe" s>$(Arg0)
08:26:14	API Interceptor	1432x Sleep call for process: Paypal Payment Authorization pdf.exe modified
08:26:14	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
08:26:16	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.244.38.210	Scan_00059010189_ ref. 004118379411_ pdf.exe	Get hash	malicious	Browse	
	Payment_Confirmation pdf.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASN-QUADRANET-GLOBALUS	Scan_00059010189_ ref. 004118379411_ pdf.exe	Get hash	malicious	Browse	• 185.244.38.210
	nh8712Nx5J.xls	Get hash	malicious	Browse	• 185.174.102.105
	Payment_Confirmation pdf.exe	Get hash	malicious	Browse	• 185.244.38.210
	npp.7.9.2.Installer (1).exe	Get hash	malicious	Browse	• 192.169.6.95

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://linkprotect.cudasvc.com/url?a=http%3a%2f%2ffindcloud.id%2fwp-includes%2f8JTmzq3FN6z3OBJBdBCfXrdcZl5H7ZxOaOZzfl2H%2f&c=E,1,2CiyC7FGbs3Pvr1yrAWkewOmRL-xyrP42HL37xX4omRyLZqRrqWOt_1RKb6pLtfzxs7zIBTrrVMEwQ8pOUIr2mFuNwrd9eHNrfkptUp83QPlV-CrGIoXMw,,&typo=1	Get hash	malicious	Browse	• 173.254.250.226
	http://https://mrveggy.com/resgatecarrinho/jcWVa69vj8IDsQRCud8h6RNI9Mz17JqsPPJ0DFnlbXZGyMM2GcZ3/	Get hash	malicious	Browse	• 173.254.250.226
	1I72L29IL3F.doc	Get hash	malicious	Browse	• 173.254.250.226
	http://https://x9sademwnet.gb.net/bnbgfvgrthbg456tr54g6trvecds/?tuk5sx4dsb3=7df34dj4csa	Get hash	malicious	Browse	• 104.129.25.9
	xLH4kwOjXR.exe	Get hash	malicious	Browse	• 104.223.94.66
	utox.exe	Get hash	malicious	Browse	• 104.223.122.15
	QUOTES.exe	Get hash	malicious	Browse	• 69.174.99.26
	file.exe	Get hash	malicious	Browse	• 192.161.187.200
	http://jb092.com/rxlbakzd/goqmmbmi.html?kjmikw5x.3hllr	Get hash	malicious	Browse	• 185.174.103.81
	http://https://www.trackins.org/sale/cat/sale-c199387IoAL&C_fTkoAvATBo-1LAvvTgoAKL6_.T5.html?_emr=12e4edca-8183-44e0-bccb-e3d6e0eeb447&wfcs=cs2&dcrectxid=d48055ba-93d6-4b3f-80c6-70de3252bde6&_eml=2ec38d65-f3da-4587-bd38-7c1f333c6dc8&source=batch&batchid=04&varid=5&csnid=1eab81b4-e54d-4cc2-8735-a5d571cfe688&brcid=13&sm=1&refid=MKTEML_31000&emlid=1131&maiid=1913	Get hash	malicious	Browse	• 173.205.83.250
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• 192.161.187.200
	kWbmxCNnPIYLMvvPIVlMbDKbbQCNjT.exe	Get hash	malicious	Browse	• 69.174.99.26
	Purchase Order.exe	Get hash	malicious	Browse	• 104.129.26.162
	SecuriteInfo.com.Variant.Bulz.265335.2250.exe	Get hash	malicious	Browse	• 66.63.162.20
	New order.xls	Get hash	malicious	Browse	• 66.63.162.20
	http://https://app.box.com/s/rdobxcyrhp1cdxwej3pfeyvngfh3lwag	Get hash	malicious	Browse	• 173.254.237.250

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	352256
Entropy (8bit):	7.469885302599986
Encrypted:	false
SSDEEP:	6144:8iS9IvO+J0i2ttjKd4aOLlLFIbJU+M2ucUcjwxvHVZ0y1UCgVBL:8EvO+l2ttKdpYLFI3XucMx/f0ymCuB
MD5:	43796C264CD5716211CCA1333D02C545
SHA1:	CD0AF8E864D885C7495A0783A17DAA185C7AC224
SHA-256:	1D7E3F93B597143DC7762692AF6D463B43FEAC3372D01A1CED3E9E6741205533
SHA-512:	B1A795E53EF3F7905EAB4E19600C67ED78CC4EA7539A50C5733E2EF944A7F9C5353D5678D7D50236730E14B851E2B659FE356F3BCD36F041D0945EA83F5806C1
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 52%
Reputation:	low

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O._.....L.....>k... .....@.. ....@.....j..S..... ....H.....text...DK... ...L..... ..`.rsrc.....N.....@..@.rel oc.....^.....@..B..... k.....H....._.....!..,>.....0..C.....(....~....o....~....o....~....o.....~.....~.....o....&*..(....*..0..?.....(.....s. .....(....o....o.....o.....o.....o.....io.....*..0..F.....(....o....o.....-....'.o.....io....&.....,..o.....*.....$:.....0..V.....(.....r...p(....r...p(.....r...p(....r+..p(.....r7..p(..... ..rD..p.....*.....,..b.....-.W..w...R...v.~E.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.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_v4.0_32\UsageLogs\Paypal Payment Authorization pdf.exe.log	
Process:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	5.347480285514745
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCt92n4M9tDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:MLUE4Ko84qpE4Ks2wKDE4KhK3VZ9pKhk
MD5:	9871A1CB00306B3628E0BDC28B4ABB86
SHA1:	248B2FE82417AC0DED1E38C43A1EED261DB6CEE1
SHA-256:	569E5D399E50DD6D74918557AAEEA3306EFD86EFAC5A62C9CB97C6DBEC396B92
SHA-512:	FB2FB7D2F9894AC760ACDD0F9757B7E458A7A64C34C651155EE21DC96AC835063F6E194A52E7DA293C336AB8765DA166A2926A14D173D013E3E7465A0765673
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	5.347480285514745
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCt92n4M9tDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:MLUE4Ko84qpE4Ks2wKDE4KhK3VZ9pKhk
MD5:	9871A1CB00306B3628E0BDC28B4ABB86
SHA1:	248B2FE82417AC0DED1E38C43A1EED261DB6CEE1
SHA-256:	569E5D399E50DD6D74918557AAEEA3306EFD86EFAC5A62C9CB97C6DBEC396B92
SHA-512:	FB2FB7D2F9894AC760ACDD0F9757B7E458A7A64C34C651155EE21DC96AC835063F6E194A52E7DA293C336AB8765DA166A2926A14D173D013E3E7465A0765673
Malicious:	false
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp2E95.tmp	
Process:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmp2E95.tmp	
Size (bytes):	1327
Entropy (8bit):	5.091498852984887
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0gWxtn:cbk4oL600QydbQxIYODOLedq3PWj
MD5:	DA63AD4C680733ED83D564411CA76CAE
SHA1:	981FC459890E62849038DA2B99C711C00B7276B9
SHA-256:	31CB39FA68EB81E5B307A93444489CD4A509607DFA2131583C27DC96E976989B
SHA-512:	8A6D9270442D41A2C562F3C63B3F6451A440D94DDB3FEED72D154A6FBDEB89A7D0B59FB05F533D585A650AABBFFB9739AA4DAC8F5104A5483A8D05C73B31A0 35
Malicious:	**true**
Reputation:	low
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\tmp3184.tmp	
Process:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.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
Reputation:	moderate, very likely benign file
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\Paypal Payment Authorization pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	1488
Entropy (8bit):	7.108278141116062
Encrypted:	false
SSDEEP:	24:SJezZmuTsu1NJezZmuTsu1NJezZmuTsu1NJezZmuTsu1NJezZmuTsu1NJezZmuTA:SUzDgcUzDgcUzDgcUzDgcUzDgcUzDgd
MD5:	8B16E30AF998D03A9F3E00B4F0ED3D0B
SHA1:	C47D03FF6B7782FF69EA32E11592D40A860274D4
SHA-256:	4B51060E7C80DEA28F677EAED229CF741BC63E030116D5248041C7194E9A82C8
SHA-512:	6D7D8E4867C40B3063A31D9D48FCD51893A9688BDC05729FAB903A306DBB4008F50DC58B60AD225666E261F9EA385E84B41D77E38FBFA7EE4E56B31E75C6D2 1
Malicious:	false
Reputation:	low
Preview:	>.....]Z.S..._;yF..6..p..GK.>0hn....EY.+..U..y.Z..t.Z...k....s..\.'.i..pr....Y..Y..q.....'..z..P.....:.....F[?..6My|...5.....".@..i,F.H....H.....|U.y.,...z...}...,:...C{v.Q.5.....&.:.Z.}.. ..3..T. .....^3...f.1.....7%.]..2_>.....]Z.S..._;yF..6..p..GK.>0hn....EY.+..U..y.Z..t.Z...k....s..\.'.i..pr....Y..Y..q.....'..z..P.....:.....F[?..6My|...5.....".@..i,F.H....H.....|U.y.,...z...}...,:... C{v.Q.5.....&.:.Z.}.. ..3..T.....^3...f.1.....7%.]..2_>.....]Z.S..._;yF..6..p..GK.>0hn....EY.+..U..y.Z..t.Z...k....s..\.'.i..pr....Y..Y..q.....'..z..P.....:.....F[?..6My|...5..... .@..i,F.H....H.....|U.y.,...z...}...,:...C{v.Q.5.....&.:.Z.}.. ..3..T.....^3...f.1.....7%.]..2_>.....]Z.S..._;yF..6..p..GK.>0hn....EY.+..U..y.Z..t.Z...k....s..\.'.i..pr....Y..Y..q.....'..z..P.....:. ....F[?..6My|...5.....".@..i,F.H....H.....|U.y.,...z...}...,:...C{v.Q.5.....&.:.Z.}.. ..3..T.....^3...f.1.....7%.]..2_>.....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:uUQ9t:uUw
MD5:	1A0A28EF8DFB3131E4982E486A21008D
SHA1:	CFC76B6C72CC2B669FFCCC2D0458D7DA4A86DF0D
SHA-256:	9ADB8FB914B62C711C899B1DAFEDE996F60E2831C4468EB083A05C9EAAE7C287
SHA-512:	ECECE4BB05C92B1710DD0AA6F3762F80805923536F4971F1A5F40F525F4A03F8DF127672081FC97DCB71095130E1B5D8D6BCCE1A0EECB1186B0C6BB8D007924
Malicious:	**true**
Preview:	_ .q...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.584962500721156
Encrypted:	false
SSDEEP:	3:9bzY6oRDJoTBn:RzWDqTB
MD5:	3FCC766D28BFD974C68B38C27D0D7A9A
SHA1:	45ED19A78D9B79E46EDBFC3E3CA58E90423A676B
SHA-256:	39A25F1AB5099005A74CF04F3C61C3253CD9BDA73B85228B58B45AAA4E838641
SHA-512:	C7D47BDAABEEBB8C9D9B31CC4CE968EAF291771762FA022A2F55F9BA4838E71FDBD3F83792709E47509C5D94629D6D274CC933371DC01560D13016D944012D5
Malicious:	false
Preview:	9iH...}Z.4..f.....l.d

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
File Type:	data
Category:	modified
Size (bytes):	64
Entropy (8bit):	5.425704882778696
Encrypted:	false
SSDEEP:	3:9bzY6oRDJoTBPcgY6oRDMjmPl:RzWDqTdRWDMCd
MD5:	CA214D2E41394F5ADA74FA4F2EA15CB5
SHA1:	32E3F863838177349F2AF70CA1CE695B3C184166
SHA-256:	B6E370AF3F5C1001C79BC19706D1A5B1803C59BC45AEFAB4BD18FC67034F47A1
SHA-512:	E9C268BCDE8872F4DD2964ACA6F9C51834E42E2AF7FF2E1C327573CEDC98127B0EDBBF8E76E456FFF82A28FC46A210D91EEEA2242ECED5368D107436B3492C14
Malicious:	false
Preview:	9iH...}Z.4..f.....l.d9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_....Xf.p^.....>a..$...e.6:7d.(a.A...=.)*....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<..._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.540873781480404
Encrypted:	false
SSDEEP:	3:oN0naRR1EbFO5ruERXXJ:oNcSROhOFRXZ
MD5:	D6F6F97EB8A42120A5DF0383DBF051A0
SHA1:	4CD2851875E5F62990455C0AD9F55E41ABD77E31
SHA-256:	7F21E4C00136CAEA325254B47362330602F4CAEB7C080C35F4E065D72704705E
SHA-512:	1F44DB8EB78F81C8C69F35FD87B7AC27FE45231BC499368E74A040E2262DD3862853AC9B3CD1B45E1342A153E5AD8528CEB0B4A71A4B8230EA4C46772DD0CD6
Malicious:	false
Preview:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.469885302599986
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Paypal Payment Authorization pdf.exe
File size:	352256
MD5:	43796c264cd5716211cca1333d02c545
SHA1:	cd0af8e864d885c7495a0783a17daa185c7ac224
SHA256:	1d7e3f93b597143dc7762692af6d463b43feac3372d01a1ced3e9e6741205533
SHA512:	b1a795e53ef3f7905eab4e19600c67ed78cc4ea7539a50c5733e2ef944a7f9c5353d5678d7d50236730e14b851e2b659fe356f3bcd36f041d0945ea83f5806c1
SSDEEP:	6144:8iS9lvO+J0i2ttjKd4aOLlLFlbJU+M2ucUcjwxvHVZ0y1UCgVBL:8EvO+l2ttKdpYLFl3XucMx/f0ymCuB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O._.....L.....>k... .....@.. .....@.....

File Icon

Icon Hash:	8c125212d9cc348a

Static PE Info

General

Entrypoint:	0x446b3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFA4F12 [Sun Jan 10 00:49:22 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

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

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x46ae8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x48000	0x10e04	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x44b44	0x44c00	False	0.983686079545	data	7.99637698124	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x48000	0x10e04	0x11000	False	0.0745346966912	data	2.5624642962	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x48130	0x10828	data		
RT_GROUP_ICON	0x58958	0x14	data		
RT_VERSION	0x5896c	0x2ac	data		
RT_MANIFEST	0x58c18	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	0.0.0.0
InternalName	Paypal Payment Authorization pdf.exe
FileVersion	0.0.0.0
ProductVersion	0.0.0.0
FileDescription	
OriginalFilename	Paypal Payment Authorization pdf.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 10, 2021 08:26:15.299971104 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:15.478411913 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:15.478790998 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:15.544387102 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:15.735930920 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:15.745909929 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:15.923803091 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:15.924019098 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.152252913 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.155679941 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.379458904 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.379514933 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.379571915 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.379610062 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.379631042 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.379662037 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.379666090 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.379703045 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.379751921 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.379787922 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.379834890 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.379873037 CET	7008	49721	185.244.38.210	192.168.2.7

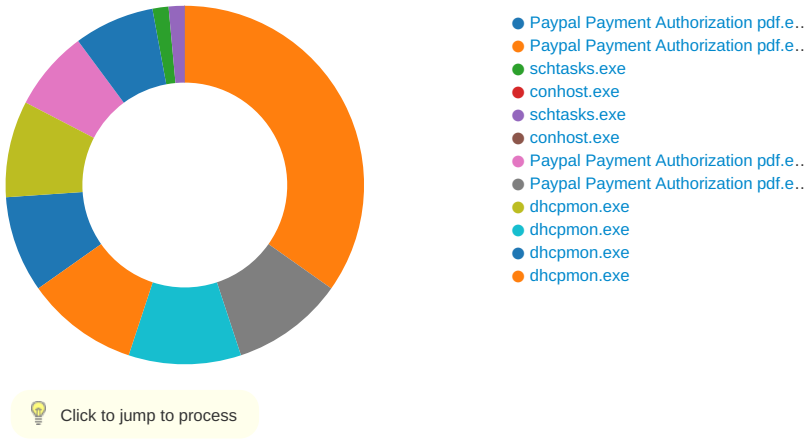
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 10, 2021 08:26:16.379945993 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.379960060 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.379964113 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.557372093 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.557468891 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.557512999 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.557537079 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.557552099 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.557604074 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.557641983 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.557662010 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.557713985 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.557720900 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.557754040 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.557800055 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.557832003 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.557868004 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.557909966 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.557921886 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.557971954 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.558020115 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.558020115 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.558079958 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.558121920 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.558139086 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.558175087 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.558209896 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.558223009 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.558260918 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.558299065 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.558320045 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.558370113 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.558428049 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.735799074 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.735827923 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.735840082 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.735861063 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.735877991 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.735901117 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.735899925 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.735917091 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.735932112 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.735941887 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.735949993 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.735969067 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.735990047 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736000061 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.736016989 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736033916 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736052990 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736073017 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736084938 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736102104 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.736108065 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736124992 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736148119 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736166000 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736177921 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736207962 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736226082 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736232996 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.736252069 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736268997 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.736273050 CET	7008	49721	185.244.38.210	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 10, 2021 08:26:16.736275911 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.736282110 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.736287117 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.736301899 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736327887 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736345053 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.736350060 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736370087 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736387014 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.736394882 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736413956 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736422062 CET	49721	7008	192.168.2.7	185.244.38.210
Jan 10, 2021 08:26:16.736453056 CET	7008	49721	185.244.38.210	192.168.2.7
Jan 10, 2021 08:26:16.736471891 CET	49721	7008	192.168.2.7	185.244.38.210

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Paypal Payment Authorization pdf.exe PID: 4544 Parent PID: 5784

General

Start time:	08:26:08
Start date:	10/01/2021
Path:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe'
Imagebase:	0x440000
File size:	352256 bytes
MD5 hash:	43796C264CD5716211CCA1333D02C545
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.229389547.0000000003839000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.229389547.0000000003839000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.229389547.0000000003839000.00000004.00000001.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	6D57CF06	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	6D57CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Paypal Payment Authorization pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D88C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Paypal Payment Authorization pdf.exe.log	unknown	617	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.	success or wait	1	6D88C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown

Analysis Process: Paypal Payment Authorization pdf.exe PID: 6136 Parent PID: 4544

General

Start time:	08:26:09
Start date:	10/01/2021
Path:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
Imagebase:	0xab0000
File size:	352256 bytes
MD5 hash:	43796C264CD5716211CCA1333D02C545
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000001.00000003.248761049.0000000004A77000.00000004.00000001.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	6D57CF06	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	6D57CF06	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	6C3CBEFF	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	6C3C1E60	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	6C3CBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6C3CDD66	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	6C3CDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2E95.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C3C7038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C3C1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp3184.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C3C7038	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	6C3CBEFF	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	6C3CBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	12	6C3C1E60	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	6C3C1E60	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	6C3C1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C3CDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2E95.tmp	success or wait	1	6C3C6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp3184.tmp	success or wait	1	6C3C6A95	DeleteFileW
C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe:Zone.Identifier	success or wait	1	6C342935	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	success or wait	1	6C3C6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	5f 20 fe 71 84 b5 d8 48	_ .q...H	success or wait	1	6C3C1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	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 80 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 50 45 00 00 4c 01 03 00 12 4f fa 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 4c 04 00 00 12 01 00 00 00 00 00 3e 6b 04 00 00 20 00 00 00 80 04 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 05 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....O._.......... ....L..........>k... ....@.. ....@................	success or wait	3	6C3CDD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C3CDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2E95.tmp	unknown	1327	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	6C3C1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	64	43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 44 65 73 6b 74 6f 70 5c 50 61 79 70 61 6c 20 50 61 79 6d 65 6e 74 20 41 75 74 68 6f 72 69 7a 61 74 69 6f 6e 20 20 70 64 66 2e 65 78 65	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe	success or wait	1	6C3C1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp3184.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.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6C3C1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	248	3e e1 17 01 a6 1c c4 a3 e0 d8 5d 5a dd 53 92 ec 02 5f 3b 79 46 f7 c6 36 92 f7 70 a9 f3 47 4b d4 8a 3e 30 68 6e 02 d7 04 15 45 59 88 2b 11 08 55 bc c0 79 92 5a 97 19 74 8b 5a b1 cb d9 6b fa fa 0f e9 ba 86 73 ac fc 5c f0 be 27 03 69 1d b4 70 72 80 1a 9c 93 59 c6 92 10 59 a7 0c 71 0c b1 13 82 bd b4 27 16 b8 7a 12 83 50 b4 a0 bc 90 92 3a a0 e6 1d e8 07 46 5b 3f f5 aa 36 4d 79 7c e5 fa ac 35 a4 ac 06 d6 17 f4 bd 2e f8 b9 ae e1 8c 1c 22 ef 40 85 0d 69 2c 46 c5 48 04 a6 d6 03 48 0b 18 07 11 00 7c 55 9d 79 04 2c 10 9b de 7a c2 f7 b6 7d 81 8a 1a 2c 3a 1f 8d de 43 7b 76 7f 51 14 35 9c ad f6 08 9b b9 d3 26 cf 3a 9a 5a 9c 7d 81 b6 20 82 a9 33 aa fa 54 ac a3 d3 1c 80 ab 01 d7 05 c2 5e 33 a4 1a 8a 66 fa 31 b1 f5 b2 f5 b6 97 37 25 18 5d 85 e5 32 5f	>.....]Z.S..._;yF..6..p..GK..>0hn....EY.+..U..y.Z..t.Z...k.....s..\..'.i..pr....Y...Y..q.....'..z..P.....:.....F[?..6My|...5.....".@..i,F.H....H.....|U.y.,...z...}...;....C{v.Q.5.....&.:.Z.}...3..T.....^3...f.1.....7%.]..2_	success or wait	6	6C3C1B4F	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	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_...Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...l.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6C3C1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d db 87 b1 98 c9 6c f6 64	9iH....}Z..4..f.....l.d	success or wait	1	6C3C1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	0	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d db 87 b1 98 c9 6c f6 64	9iH....}Z..4..f.....l.d	success or wait	1	6C3CDD66	CopyFileW
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 85 16 f4 a5 20 38 a2 6a 80 a4 a3 f3 7c 88 26 58 b6 ca 65 a6 46 b8 2a 80	9iH....}Z..4..f..... 8.j....|. &X..e.F.*.	success or wait	1	6C3C1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D53D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D53D72F	unknown
C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe	unknown	4096	success or wait	1	6D53D72F	unknown
C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe	unknown	512	success or wait	1	6D53D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6C3C646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 2800 Parent PID: 6136

General

Start time:	08:26:12
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp2E95.tmp'
Imagebase:	0xd80000
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\tmp2E95.tmp	unknown	2	success or wait	1	D8AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2E95.tmp	unknown	1328	success or wait	1	D8ABD9	ReadFile

Analysis Process: conhost.exe PID: 4352 Parent PID: 2800

General

Start time:	08:26:13
Start date:	10/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 5496 Parent PID: 6136

General

Start time:	08:26:13
Start date:	10/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp3184.tmp'
Imagebase:	0xd80000
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\tmp3184.tmp	unknown	2	success or wait	1	D8AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3184.tmp	unknown	1311	success or wait	1	D8ABD9	ReadFile

Analysis Process: conhost.exe PID: 2776 Parent PID: 5496

General

Start time:	08:26:14
Start date:	10/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: Paypal Payment Authorization pdf.exe PID: 5444 Parent PID: 1104

General

Start time:	08:26:14
Start date:	10/01/2021
Path:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe' 0
Imagebase:	0x930000
File size:	352256 bytes
MD5 hash:	43796C264CD5716211CCA1333D02C545
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: 00000006.00000002.243400566.0000000003E79000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.243400566.0000000003E79000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.243400566.0000000003E79000.00000004.00000001.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	6D57CF06	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	6D57CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown

Analysis Process: Paypal Payment Authorization pdf.exe PID: 4348 Parent PID: 5444

General

Start time:	08:26:15
Start date:	10/01/2021
Path:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Paypal Payment Authorization pdf.exe
Imagebase:	0x7ff724940000
File size:	352256 bytes
MD5 hash:	43796C264CD5716211CCA1333D02C545
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.264202941.0000000003959000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.264202941.0000000003959000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.257617015.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.257617015.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.257617015.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.264137814.0000000002988000.00000004.00000001.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	6D57CF06	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	6D57CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 5912 Parent PID: 1104

General

Start time:	08:26:16
Start date:	10/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x7ff6e70f0000
File size:	352256 bytes

MD5 hash:	43796C264CD5716211CCA1333D02C545
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: 00000008.00000002.248386256.00000000038D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.248386256.00000000038D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.248386256.00000000038D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 52%, ReversingLabs
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	6D57CF06	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	6D57CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D88C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	617	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.	success or wait	1	6D88C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown

Analysis Process: dhcpmon.exe PID: 4928 Parent PID: 5912

General

Start time:	08:26:17
Start date:	10/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x450000
File size:	352256 bytes
MD5 hash:	43796C264CD5716211CCA1333D02C545
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.268198186.0000000003809000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.268198186.0000000003809000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.266349011.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.266349011.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.266349011.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.268089458.0000000002801000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.268089458.0000000002801000.00000004.00000001.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	6D57CF06	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	6D57CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 4352 Parent PID: 3292

General

Start time:	08:26:23
Start date:	10/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x9d0000
File size:	352256 bytes
MD5 hash:	43796C264CD5716211CCA1333D02C545
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: 0000000A.00000002.267647233.0000000003D09000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.267647233.0000000003D09000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.267647233.0000000003D09000.00000004.00000001.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	6D57CF06	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	6D57CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown

Analysis Process: dhcpmon.exe PID: 788 Parent PID: 4352

General

Start time:	08:26:26
Start date:	10/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x450000
File size:	352256 bytes
MD5 hash:	43796C264CD5716211CCA1333D02C545
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.00000002.281240988.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.281240988.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.281240988.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.282400561.00000000027E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.282400561.00000000027E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.282484135.00000000037E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.282484135.00000000037E9000.00000004.00000001.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	6D57CF06	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	6D57CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile

Disassembly

Code Analysis