

Forum:[Hack Forums](#)

Thread: [Why do Scambaiters still use Nanocore as their RAT?](#)

Exoliner - February 22, 2026, 2:54 am

Why do Scambaiting YouTubers use Nanocore as their RAT of choice? Is it an okay pick? Is it easy to use, or is there something deeper? Would they have to use any crypters? In Nanobaiter's newest video titled "TORTURING Scammers With 10,000 Viruses Live On CCTV!" (I can't post links) at 5:25, he uses Kali Linux to send a payload to the scammers pc wouldn't windows defender flag the payload unless he infected the network? As a person who's trying to get into scambaiting, what he did using Kali looks pretty advanced (at least from my perspective) and looks kinda cool, but why use an old RAT like Nanocore, though? Also, if anyone is knowledgeable or experienced in Kali, could they clarify what precisely he did? That would be cool.

DramaKing - February 22, 2026, 4:04 am

Nanocore should be detected by pretty much everything. "Infecting the network" is a nebulous term and has little meaning, not unless you take it to mean compromising an EDR console.

I now have many questions. Like why is someone typing into a Win7 Command Prompt like it's some ancient financial application? Why is the video using clips from Jim Browning?

Oh, it's to make computer illiterate people think that they somehow made the company send them too much money and have to refund part of the money. Oh, but wait, there's no error message after each line. I can only explain it as the Command Prompt being fake.

That popup message that you're referring to? Totally fake. I mean, it would have to be at least simulated because the scammer, I mean, the scambaiter, wouldn't be able to record the screen before getting a remote connection. Pinging a local device from Kali is not sending a payload. And that very simple thing was all that he used Kali for. It's just there to make him look like Mr. Hackerman.

The so-called AnyDesk rep giggling about hacking the scammers was funny. Or the part where Nanobaiter called a scam center after having their phone service terminated. Or using SmokeLoader to load Amadey, Redline, Rhadamthys, and something called DarkGate all at once. Rhadamthys Stealer doesn't even exist anymore. At 13:42 you can see in Command Prompt that the program either shows access denied or is not found.

This may not be the most authoritative source, but unlike the State Farm commercial says, people can put things on the Internet that are not true. <https://www.reddit.com/r/scambait/s/Ino1VV6xZR> If you want to know how to do this, get Sora 2 or whatever, maybe some stock footage, and spin up some VMs.

Exoliner - February 22, 2026, 2:01 pm

(Feb 22, 2026 05:04 AM)DramaKing Wrote: [\[CITE\]](#) Nanocore should be detected by pretty much everything. "Infecting the network" is a nebulous term and has little meaning, not unless you take it to mean compromising an EDR console.

I now have many questions. Like why is someone typing into a Win7 Command Prompt like it's some ancient financial application? Why is the video using clips from Jim Browning?

Oh, it's to make computer illiterate people think that they somehow made the company send them too much money and have to refund part of the money. Oh, but wait, there's no error message after each line. I can only explain it as the Command Prompt being fake.

That popup message that you're referring to? Totally fake. I mean, it would have to be at least simulated because the scammer, I mean, the scambaiter, wouldn't be able to record the screen before getting a remote connection. Pinging a local device from Kali is not sending a payload. And that very simple thing was all that he used Kali for. It's just there to make him look like Mr. Hackerman.

The so-called AnyDesk rep giggling about hacking the scammers was funny. Or the part where Nanobaiter called a scam center after having their phone service terminated. Or using SmokeLoader to load Amadey, Redline, Rhadamthys, and something called DarkGate all at once. Rhadamthys Stealer doesn't even exist anymore. At 13:42 you can see in Command Prompt that the program either shows access denied or is not found.

This may not be the most authoritative source, but unlike the State Farm commercial says, people can put things on the Internet that are not. If you want to know how to do this, get Sora 2 or whatever, maybe some stock footage, and spin up some VMs.

So from your experience, are there any legitimate reverse access Scambaiters? Like, I know Jim Browning is legitimate, maybe Scambaiter is legitimate too? I'm starting to doubt Scammer Payback, but I think he was legitimate in the past. Like Scambaiter (the YouTube channel) got me interested in cybersecurity, or at least perusing it, and I'm interested in red teaming/ethical hacking (I know they aren't the same thing, but you get what I mean), so if it turns out that a person you looked up to that got you interested in a profession was faking his content, that kinda sours my motivation, or at least for me it does.