Decoding njRAT traffic with NetworkMiner

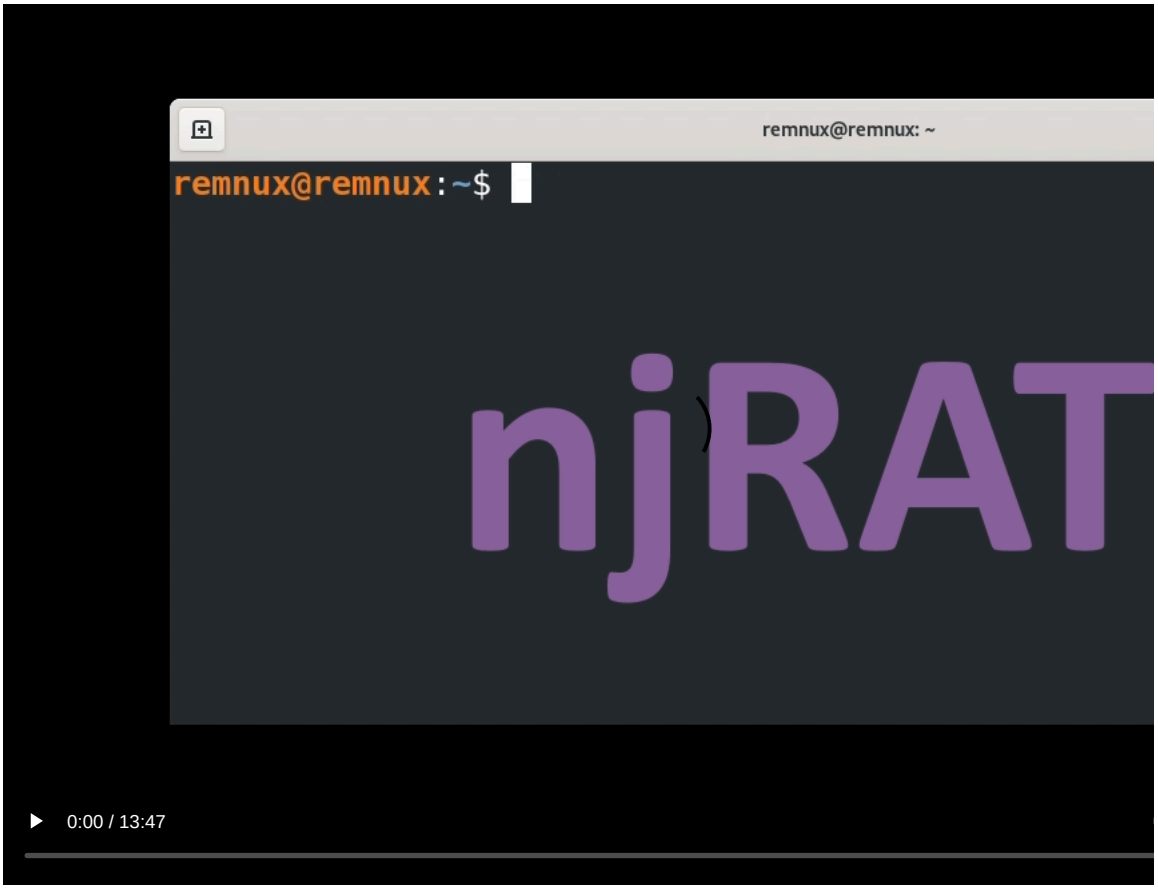
By Erik Hjelmvik

Published: 2025-04-28 · Archived: 2026-04-05 14:38:05 UTC

,

Monday, 28 April 2025 06:00:00 (UTC/GMT)

I investigate network traffic from a Triage sandbox execution of njRAT in this video. The analysis is performed using NetworkMiner in Linux (REMnux to be specific).



About njRAT / Bladabindi

njRAT is a Remote Access Trojan (RAT) that can be used to remotely control a hacked computer. It has been around since 2013, but despite being over 10 years old it still remains one of the most popular backdoors used by malicious actors. Anti virus vendors usually refer to njRAT as Bladabindi.

njRAT Artefacts Extracted by NetworkMiner

NetworkMiner has a built-in parser for the njRAT Command-and-Control (C2) protocol. This njRAT parser kicks in whenever there is traffic to a well-known njRAT port, such as TCP 1177 or 5552, plus a few extra ports (like TCP 14817 that was used by the analysed sample). You'll need NetworkMiner Professional to decode njRAT traffic to other ports, since it comes with a port-independent-protocol-identification (PIPI) feature that automatically detects the protocol regardless which port the server runs on.

As demonstrated in the video, NetworkMiner can extract the following types of artefacts from njRAT network traffic:

- Screenshots of victim computer
- Transferred files
- Commands from C2 server
- Replies from bot
- Stolen credentials/passwords
- Keylog data

Covered njRAT Commands and Plugins

These njRAT commands and plugins are mentioned in the video:

- CAP = Screen Capture
- ret = Get Passwords
- inv = Invoke Plugin
- PLG = Plugin Delivery
- kl = Key Logger
- Ex = Execute Plugin
- Ex proc = Process List
- Ex fm = File Manager

IOC List

- Sample (a.exe): cca1e0b65d759f4c58ce760f94039a0a
- C2 server: 5.tcp.eu.ngrok[.]io:14817
- njRAT inv (dll): 2d65bc3bff4a5d31b59f5bdf6e6311d7
- njRAT PLG (dll): c179e212316f26ce9325a8d80d936666
- njRAT ret (dll): ac43720c43dcf90b2d57d746464ad574
- Splitter: Y262SUCZ4UJJ

Posted by Erik Hjelmvik on Monday, 28 April 2025 06:00:00 (UTC/GMT)

Tags: #njRAT#NetworkMiner#REMnux#Video#videotutorial

Short URL: https://netresec.com/?b=2541a39
