njRAT runs MassLogger

By Erik Hjelmvik

Published: 2026-02-02 · Archived: 2026-04-05 23:35:28 UTC

,

Monday, 02 February 2026 19:39:00 (UTC/GMT)

njRAT is a remote access trojan that has been around for more than 10 years and still remains one of the most popular RATs among criminal threat actors. This blog post demonstrates how NetworkMiner Professional can be used to decode the njRAT C2 traffic to extract artifacts like screenshots, commands and transferred files.

A PCAP file with njRAT traffic was published on malware-traffic-analysis.net last week. After loading this PCAP file, NetworkMiner Professional reveals that the attacker downloaded full resolution screenshots of the victim's screen.

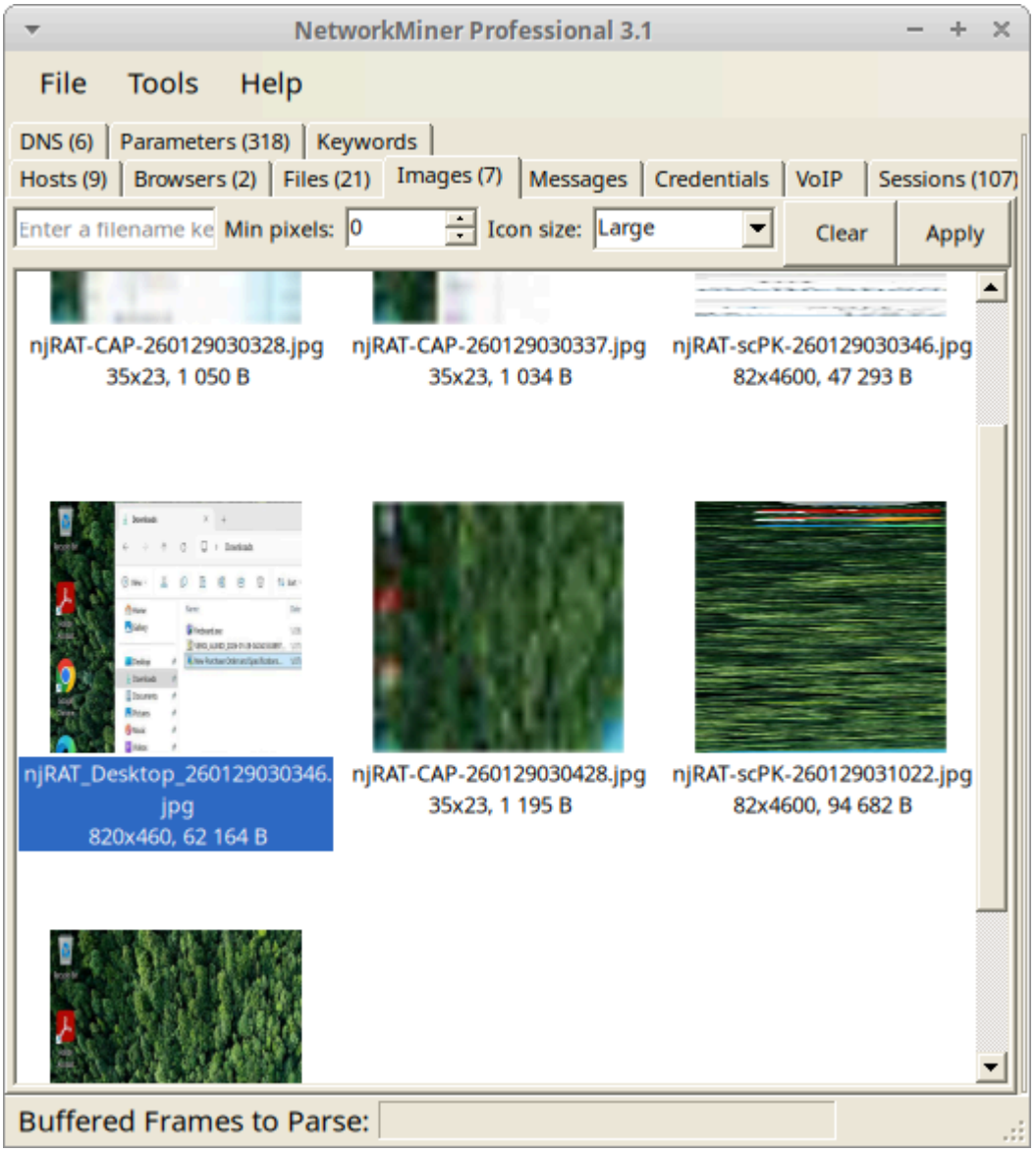


Image: Overview of screenshots sent to C2 server

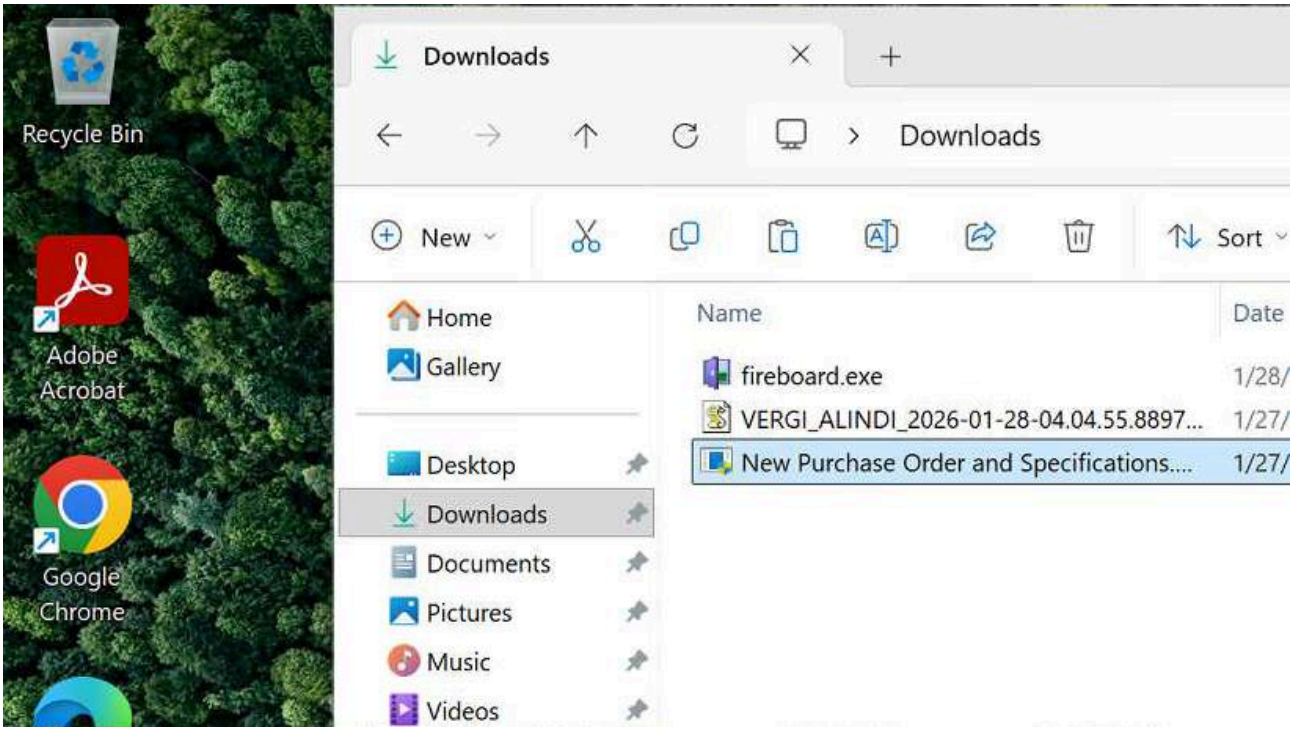
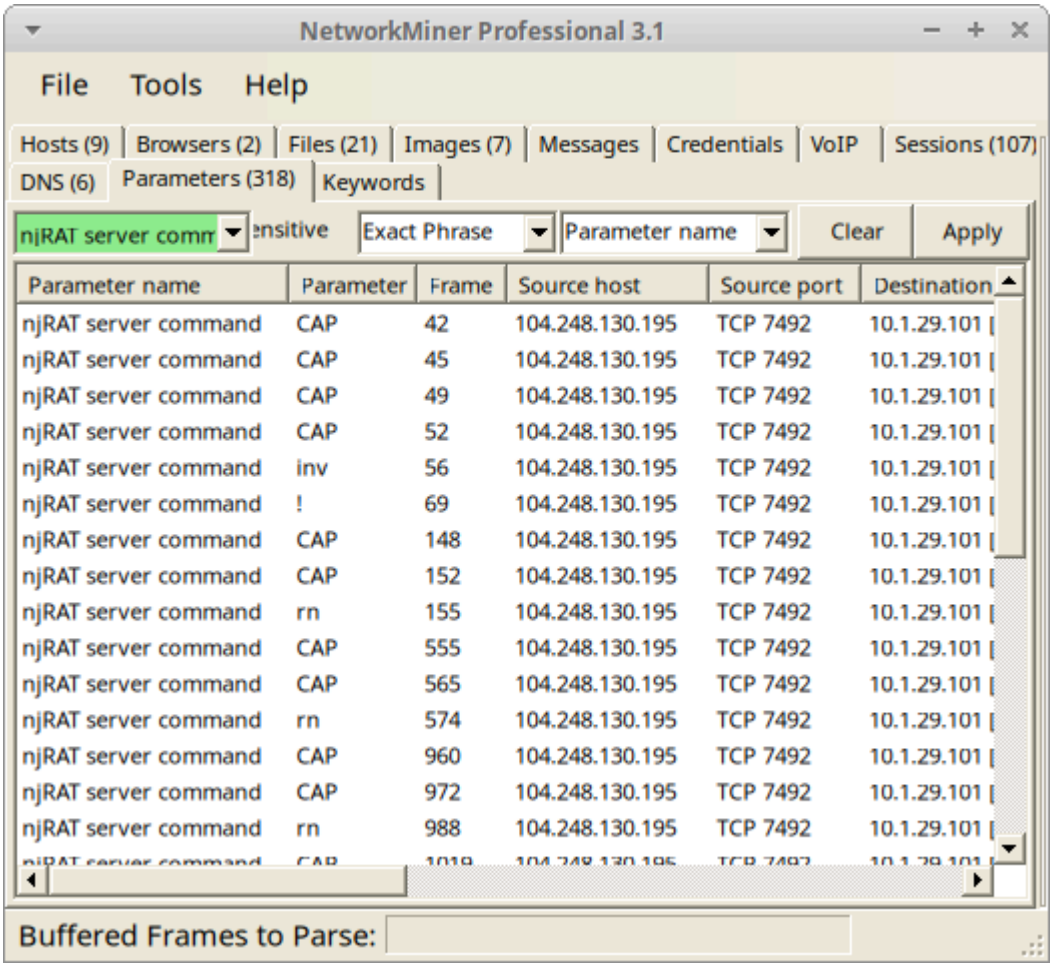


Image: Screenshot extracted from njRAT traffic by NetworkMiner

The file “New Purchase Order and Specifications.exe” in this screenshot is the njRAT binary that was used to infect the PC.

A list of njRAT commands sent from the C2 server to the victim can be viewed on NetworkMiner’s Parameters tab by filtering for ”njRAT server command”.



The following njRAT commands are present here:

- CAP = take screenshot
- inv = invoke (run) a plugin (dll)
- rn = run a tool (executable)

Additional njRAT commands can be found in our writeup for the Decoding njRAT traffic with NetworkMiner video, which we published last year.

njRAT File Transfers

The “inv” and “rn” commands both transfer and execute additional code on the victim machine. The “inv” command typically transfers a DLL file that is used as a plugin, while the “rn” commands sends an executable file. These DLL and EXE files are transferred in gzip compressed format, which is why NetworkMiner extracts them as .gz files.

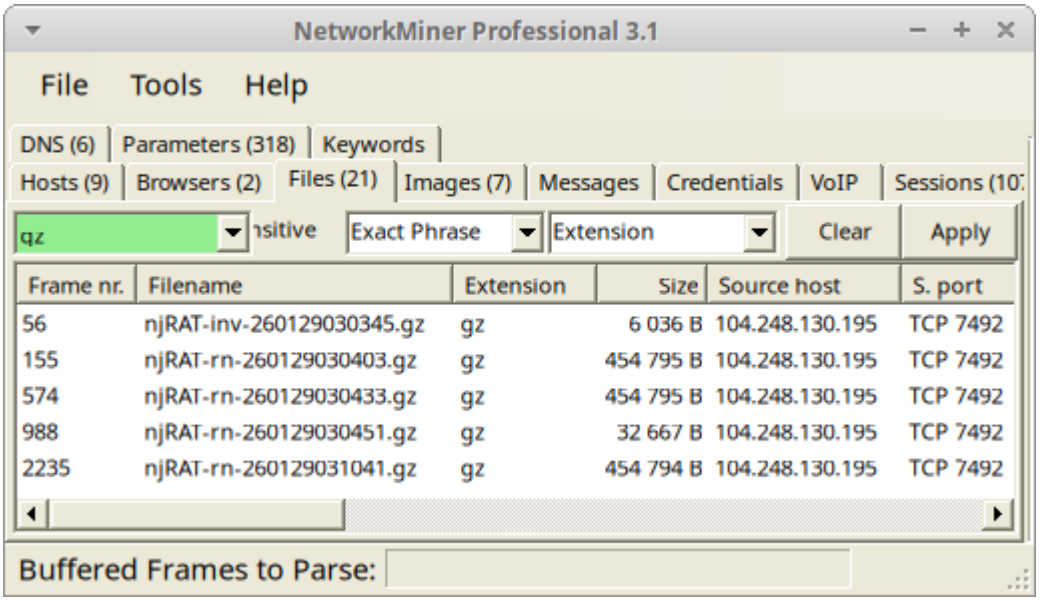
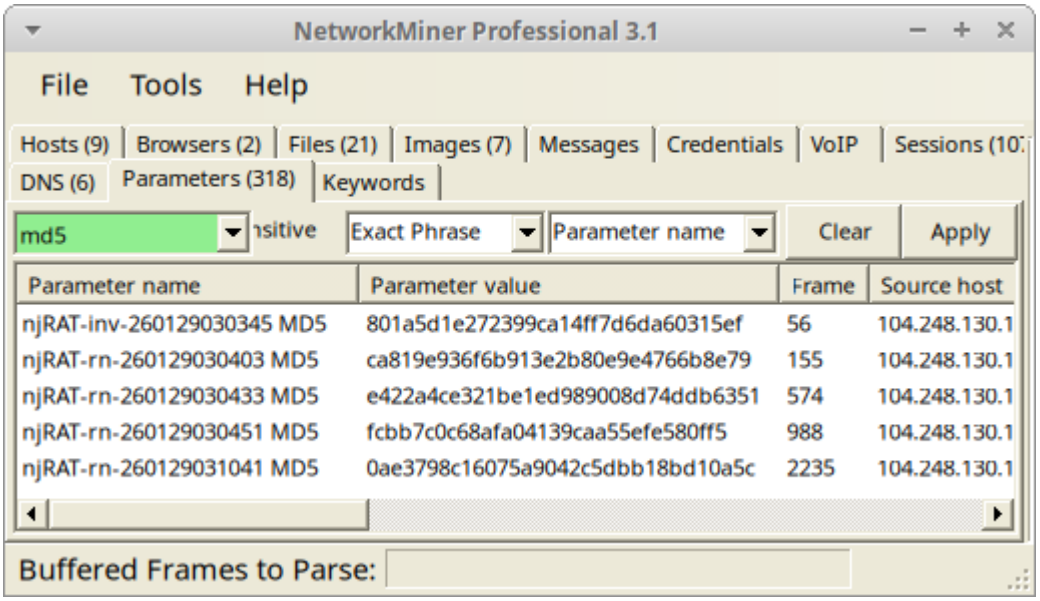


Image: Gzip compressed files extracted from njRAT traffic

This oneliner command lists the internal/original file names and corresponding MD5 hashes of the gzip compressed executables sent to the victim PC:

- for f in njRAT-rn*.gz; do echo $f; gunzip -c $f | exiftool - | grep Original; gunzip -c $f | md5sum; done
- njRAT-rn-260129030403.gz
- Original File Name : Stub.exe
- ca819e936f6b913e2b80e9e4766b8e79 -
- njRAT-rn-260129030433.gz
- Original File Name : Stub.exe
- e422a4ce321be1ed989008d74ddb6351 -
- njRAT-rn-260129030451.gz
- Original File Name : CloudServices.exe
- fcbb7c0c68afa04139caa55efe580ff5 -
- njRAT-rn-260129031041.gz
- Original File Name : Stub.exe
- 0ae3798c16075a9042c5dbb18bd10a5c -

The MD5 hashes of the files inside the gzip compressed streams can also be seen on the Parameters tab in NetworkMiner.



MassLogger

The “CloudServices.exe” executable is a known credential stealer called MassLogger. This particular MassLogger sample is hard coded to exfiltrate data in an email to kingsnakeresult@mcnzxz[.]com. The email is sent through the SMTP server cphost14.qhoster[.]net. See the execution of this sample on Triage for additional details regarding the MassLogger payload in CloudServices.exe.

IOC List

njRAT (splitter = "|Ghost|")

- 58f1a46dba84d31257f1e0f8c92c59ec = njRAT sample
- 104.248.130.195:7492 = njRAT C2 server
- burhanalassad.duckdns[.]org:7492 = njRAT C2 server
- 801a5d1e272399ca14ff7d6da60315ef = sc2.dll
- ca819e936f6b913e2b80e9e4766b8e79 = Stub.exe
- e422a4ce321be1ed989008d74ddb6351 = Stub.exe
- fcbb7c0c68afa04139caa55efe580ff5 = CloudServices.exe
- 0ae3798c16075a9042c5dbb18bd10a5c = Stub.exe

MassLogger

- fcbb7c0c68afa04139caa55efe580ff5
- kingsnakeresult@mcnzxz[.]com
- cphost14.qhoster.net:587
- 78.110.166.82:587

Posted by Erik Hjelmvik on Monday, 02 February 2026 19:39:00 (UTC/GMT)

Tags: #njRAT#NetworkMiner Professional#malware-traffic-analysis.net

Short URL: https://netresec.com/?b=262adb9
