



- To ensure persistence on the infected system, the attackers employ scheduled tasks that run every two minutes.
- The final stage of the attacks involves executing the main payload, which includes malicious DLL and EXE files (AsyncRAT). These files establish communication with the attacker's Command and Control (C2) server.

The report also provides security professionals with actionable IOCs to safeguard their environments against AsyncRAT. The full analysis is available on [ANY.RUN's blog](#).

██████ ███.███

ANY.RUN serves over 500,000 cybersecurity professionals globally, offering an interactive platform for malware analysis targeting Windows and Linux environments. With advanced threat intelligence tools such as TI Lookup, YARA Search, and Feeds, ANY.RUN enhances incident response and provides analysts with essential data to counter cyber threats effectively.

The ANY.RUN team

ANYRUN FZCO

+1 657-366-5050

[email us here](#)

Visit us on social media:

X

---

This press release can be viewed online at: <https://www.einpresswire.com/article/758566147>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.