

ANY.RUN Exposes Pentagon Stealer: Crypto and Data Theft Malware Targeting Businesses

DUBAI, DUBAI, UNITED ARAB
EMIRATES, April 29, 2025

/EINPresswire.com/ -- [ANY.RUN](#), a premier provider of interactive malware analysis and threat intelligence solutions, has published a comprehensive report by its analyst team exposing Pentagon Stealer, an evolving malware that poses a critical threat to organizations worldwide.

██████████ ██████████: ███ ██████████

Pentagon Stealer, in Python and Golang variants, steals sensitive data with advanced techniques:

- █████ █████: Extracts browser credentials, cookies, Atomic/Exodus wallet data, Discord/Telegram tokens, and files from Chromium- and Gecko-based browsers (Firefox, Zen, Waterfox).
- █████████ ██████████: The malware is extensively utilized under different names 1312, Acab, Vilsa, and BLX stealer.
- █████████ █████████ ██████████████: Replaces app.asar files in Atomic/Exodus wallets to steal mnemonics/passwords.
- █████████ █████: Launches Chromium browsers in debug mode to bypass DPAPI encryption, stealing unencrypted cookies.
- ███ ████████████████████████████████: Uses HTTP with pentagon[.]cy/stealer[.]cy servers; BLX uploads to gofile.io, sending links to C2.



Its evolution and integration into attack chains with droppers/miners amplify its risk.

[Read the analysis on ANY.RUN's blog.](#)

ANY.RUN is a cloud-based interactive sandbox that provides companies and SOC teams with the ability to detect and analyze malware attacks.

ANY.RUN's Interactive Sandbox provides companies and SOC teams with the ability to detect and analyze Pentagon Stealer attacks.

Businesses can leverage its real-time insights to extract Indicators of Compromise (IOCs), monitor C2 communications, and trace infection chains, enabling fast detection and mitigation.

ANY.RUN is a trusted partner for over 15,000 organizations in finance, healthcare, retail, technology, and beyond, delivering advanced malware analysis and threat intelligence products.

Its cloud-based Interactive Sandbox, Threat Intelligence Lookup, and TI Feeds enable businesses to detect, analyze, and investigate the latest malware and phishing campaigns to streamline triage, response, and proactive security.

The ANY.RUN team

ANYRUN FZCO

+1 657-366-5050

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/807733384>

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.

© 1995-2025 Newsmatics Inc. All Right Reserved.