

ANY.RUN Uncovers DeerStealer Malware Campaign Exploiting Fake Google Authenticator Websites

DUBAI, DUBAI, UNITED ARAB EMIRATES, July 31, 2024

/EINPresswire.com/ -- [ANY.RUN](#), a trusted provider of cybersecurity solutions, has revealed a new malware distribution campaign. This campaign uses fake Google Authenticator websites to spread DeerStealer malware.

██████████████████: █ ███ ████████
██████████████ █ ████████
████████████████████

DeerStealer, detected by ANY.RUN's expert team, is distributed through fraudulent websites designed to mimic official Google Authenticator websites. These deceptive sites trick users into downloading malware. When users click the Download button, their information is sent to a Telegram bot named Tuc-tuc before the malware is downloaded from GitHub.

██-██████ ██████████ █ ████████████████████

- ANY.RUN's team conducted a comprehensive analysis of the DeerStealer malware. Key findings include:
- Fake site analysis: Attackers are using websites mimicking legitimate Google pages, tricking users into downloading the malware.
 - Telegram bot logging: The bot logs visitor information, including IP addresses and countries.
 - Stealer on GitHub: The malware, hosted on GitHub, is written in Delphi and executes directly in memory, employing obfuscation techniques to avoid detection.
 - C2 communication: The malware communicates with a C2 server, sending encrypted data using



single-byte XOR encryption.

□ □ □ □ □ □ □ □ □ □ □ □ □

Cybersecurity experts can use this analysis to study the behavior of the DeerStealer malware and collect Indicators of Compromise (IOCs) identified by ANY.RUN's experts.

For more information on the malware campaign, [visit the ANY.RUN blog](#).

□□□□□ □□□.□□□

ANY.RUN offers a comprehensive suite of cybersecurity products, including an interactive sandbox and a Threat Intelligence portal. Trusted by over 400,000 professionals globally, the sandbox provides an efficient and user-friendly platform for analyzing malware targeting both Windows and Linux systems. Additionally, ANY.RUN's Threat Intelligence services, comprising Lookup, Feeds, and YARA Search, enable users to gather critical information about threats and respond to incidents with enhanced speed and accuracy.

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/731882963>

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.