

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



