ANY.RUN Unveils New Techniques to Intercept Data Exfiltrated by Malware via Telegram and Discord

DUBAI, DUBAI, UNITED ARAB EMIRATES, September 30, 2024 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis solutions, has published a comprehensive guide demonstrating how cybersecurity professionals can intercept data exfiltrated by malware through Telegram's API. The guide offers a deep dive into how threat actors use Telegram and Discord to steal sensitive information from infected machines and explains how security analysts can hijack the exfiltration process to retrieve critical intelligence.

□ □□□□□□□□ □□□□□□□: □□□□□□□□ □□□□□□□□□□□□□ □□□ □□□□□□□□□ □□□ □□□□□□□□

Cybercriminals increasingly rely on platforms like Telegram and Discord to exfiltrate sensitive data due to their simplicity and lack of server infrastructure requirements. In response to this trend, ANY.RUN's detailed article highlights how security professionals can leverage Telegram's API to intercept the data flow, revealing critical information such as bot tokens and chat IDs.

By analyzing malware behavior in ANY.RUN's sandbox environment, professionals can obtain essential data about threat actors, including their bot tokens and chat IDs, and use this information to intercept the stolen data.

□□□□□□□□□ □□□□□□□□□ □□□□ □□□□□□□□□□□□□□□ □□□□□□□□□

For cybersecurity analysts, this guide offers actionable insights and practical steps to intercept data exfiltrated by malware through Telegram and Discord.

Key topics covered in the guide include:

· □□□ □□□□□ □□□ □□□□ □□ □□□□□□□□□□□: Analysts can uncover key information such as bot tokens and chat IDs from Telegram communications, which is critical for tracing malware activity.
· □□□□□□□□□□□□ □□□□ □□□□□□□□□□□□□: Detailed steps are provided to hijack the data exfiltration process, allowing analysts to see stolen information.
· □□□□□□□□□ □□□□□□□□□□ □□□□□ □□□□□□ □□□□□□□: Practical Python scripts are included for automating the extraction and forwarding of messages between compromised and monitoring systems.

For more detailed information, including code samples and specific API usage techniques, visit the ANY.RUN blog.

□□□□□ □□□.□□□

ANY.RUN is trusted by over 400,000 cybersecurity professionals worldwide. The platform provides an interactive sandbox that simplifies malware analysis for both Windows and Linux threats. With its powerful threat intelligence tools, such as TI Lookup, Yara Search, and Feeds, ANY.RUN enables users to quickly identify IOCs and gather critical information to respond to incidents more efficiently.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
X
