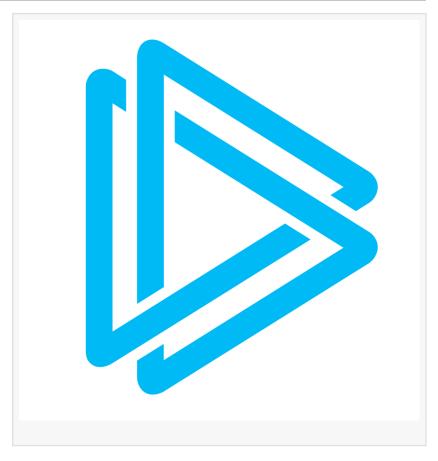# ANY.RUN Shares Research on Zhong Stealer: The New Malware Targeting Fintech and Cryptocurrency

DUBAI, DUBAI, UNITED ARAB EMIRATES, February 18, 2025 /EINPresswire.com/ -- ANY.RUN, the leading provider of interactive malware analysis and threat intelligence solutions, has revealed a new stealer malware exploiting customer support chat systems to infiltrate the fintech and cryptocurrency industries. Zhong Stealer deceives help desk agents by posing as frustrated customers and delivering weaponized attachments designed to steal credentials and exfiltrate sensitive data.

ANY.RUN's Research Report: Uncovering Zhong Stealer in Fintech Cryptocurrency

The campaign, active from December 20-24, 2024, leveraged Zendesk and other support platforms, where attackers created fake tickets and pressured agents into opening malicious ZIP files. ANY.RUN's real-time malware analysis sandbox exposed Zhong's behavior, revealing its stealthy execution chain, data exfiltration tactics, and C2 infrastructure.

ANY.RUN's Discovery During Analysis Zhong's Behavior

By running Zhong Stealer inside ANY.RUN's interactive sandbox, researchers observed:

· Social Engineering in the Attack Process - Fake support requests, written in broken Chinese, pressured help desk agents into opening infected attachments.

· Registry Modification Persistence - The malware modified Windows registry keys and

leveraged scheduled tasks to maintain long-term access.

· □□□□□□□□□ □□□□□□□□□ - Zhong targeted Brave, Edge, and Internet Explorer browsers, stealing saved passwords and user session data.

· □□□□ □□□□-□□□□□ □□ □□□□□□□□□□□□□ - Stolen credentials were exfiltrated over port 1131 to a command-and-control server hosted on Alibaba Cloud.

For a more detailed analysis of Zhong Stealer, including technical breakdowns and IOCs, visit the [ANY.RUN blog](#).

□□□□□ □□□.□□□

ANY.RUN is a provider of interactive malware analysis and threat intelligence solutions, allowing cybersecurity professionals to analyze threats in real time, detect malicious activity, and respond proactively. With its cloud-based sandboxing environment, TI Lookup, and Safebrowsing, ANY.RUN delivers deep visibility into malware behavior, threat intelligence, and web-based risks. These tools help organizations track emerging threats, extract indicators of compromise (IOCs), investigate suspicious files and URLs, and enhance their security posture.

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