ANY.RUN Publishes In-Depth Analysis on New Loader Used to Distribute SSLoad Malware

DUBAI, DUBAI, UNITED ARAB EMIRATES, October 7, 2024 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis solutions, has published an in-depth report on PhantomLoader, a new loader used to distribute the Rust-based malware SSLoad. This analysis uncovers advanced techniques used by PhantomLoader in recent attacks to deliver SSLoad, highlighting its stealthy distribution methods and malware behavior.

□□-□□□□□□ □□□□□□□□ □□□□□□□□□ □□ □□□□□□□□□□□□□□□ □□□□ □□□□□□□

The report dives into the technical nuances of PhantomLoader, which disguises itself as a legitimate DLL module for antivirus software called 360 Security Total.

Through a detailed walkthrough, researchers explain how this loader decrypts and deploys SSLoad, a malware known for its evasive tactics.

□□□□ □□□□□□□□□ □□□□□ □□□□ □□□□□□□□□:

· □□□□□□ □□ □□□□□□□□□□ □□□□□□: Attackers initiate the SSLoad distribution using malicious Word documents with embedded macros.

· □□□□□□□□□□□□□□□’□ □□□□□□□□ □□□□□□□□□□□□: PhantomLoader conceals itself within legitimate DLL modules, using encryption and self-modifying code to remain undetected.

· □□□□□□□'□ □□□□□-□□□□□□□□□ □□□□□□□□□□□□: SSLoad employs anti-debugging and anti-emulation techniques to evade detection and decrypts Command-and-Control (C2) URLs for communication.

· □□□□ □□ □□□□□□□□□ □□□□□□□□□□□□ □□□□□□□□□□□□: Scripts like IDAPython are used to decode and analyze the malware's encrypted payloads.

· □□□□□□□□□□□ □□ □□□□□□□□□□□□ (□□□□□): Key IOCs such as file paths, hashes, and C2 domains are provided to help analysts strengthen their defenses.

To read the full analysis, visit the ANY.RUN blog.

□□□□□ □□□.□□□
ANY.RUN is a trusted interactive malware analysis platform, relied upon by over 500,000 cybersecurity professionals worldwide. It simplifies the analysis of threats targeting Windows and Linux systems and offers a suite of threat intelligence tools, including TI Lookup, YARA Search, and Feeds, to enhance incident response and threat detection.

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