ANY.RUN Researches Ducex: Packer Used in Triada Android Malware

DUBAI, DUBAI, UNITED ARAB EMIRATES, July 8, 2025 /EINPresswire.com/ -- Cybersecurity analysts at ANY.RUN, an established provider of threat analysis and intelligence solutions, published comprehensive research revealing the sophisticated code packing tool Ducex used by Triada Android malware. The research uncovered an advanced obfuscation system that employs multiple layers of encryption and anti-analysis techniques to evade security detection.

□□□ □□□□□□□□□

Ducex is an advanced Chinese Android packer found in Triada samples, whose primary goal is to complicate analysis and confuse the detection of its payload.

· □□□□□□□□□□ □□□□□□□□□□: The packer employs serious obfuscation through function encryption using a modified RC4 algorithm with added shuffling.

· □□□□□ □□□□□□□□: Beyond functions, all strings used by Ducex are also encrypted using a simple sequential XOR algorithm with a changing 16-byte key.

· □□□□□□□□□□ □□□□□□□□□□□: Ducex creates major roadblocks for debugging. It performs APK signature verification, failing if the app is re-signed. It also employs self-debugging using fork and ptrace to block external tracing and stops running if tools like Frida are detected in memory.

These capabilities represent a concerning trend toward more resilient malware that can adapt to and evade security measures.

□□□□□□ □□ □□□□□□□□□ □□□□□□□□□□□□□

The findings have significant implications for the cybersecurity community:

· □□□□□□□□□ □□□□□□□□□□: Traditional signature-based detection methods are largely ineffective against this level of obfuscation, requiring more sophisticated behavioral analysis techniques.

· □□□□□□□□ □□□□□□□□□□: Security researchers must develop new methodologies to analyze heavily obfuscated malware, potentially requiring specialized tools and extended analysis timeframes.

· □□□□□□ □□□□□□□□ □□□□□□□□: The integration of such sophisticated protection mechanisms into mobile malware represents an escalation in the mobile threat landscape, particularly for Android devices.

The research contributes to the broader understanding of advanced persistent threats (APTs) and sophisticated malware families. It provides detailed technical documentation, including decryption scripts and indicators of compromise (IOCs) to assist the security community in detecting and analyzing similar threats.

Read the full article in ANY.RUN's blog.

□□□□□ □□□.□□□

ANY.RUN is an interactive malware analysis and threat intelligence provider trusted by SOCs, CERTs, MSSPs, and cybersecurity researchers. The company's solutions are leveraged by 15,000 corporate security teams for incident investigations worldwide.

With real-time visibility into malware behavior, a focus on real-time interaction and actionable intelligence, ANY.RUN accelerates incident response, supports in-depth research, and helps defenders stay ahead of evolving threats.

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