ANY.RUN Reveals How JA3 Fingerprints Help SOC Teams Expose Hacker Attacks on Companies Earlier

DUBAI, DUBAI, UNITED ARAB EMIRATES, January 26, 2026 /EINPresswire.com/ -- ANY.RUN, a recognized provider of interactive malware analysis and threat intelligence solutions trusted by over 15,000 SOC teams worldwide, today released comprehensive research showing how JA3 TLS fingerprinting can elevate security operations from chasing disposable indicators to identifying persistent attacker tools.

□□□ □□ □ □□□□-□□□□□ □□□□□□

Unlike IP addresses, domains, or file hashes, JA3 fingerprints capture the structure of a TLS ClientHello handshake, effectively reflecting the network behavior of the underlying tool or library. ANY.RUN's team analyzed 30 days of unique sandbox sessions, identifying JA3 hashes where malicious analyses exceeded 85% of total occurrences. This approach allowed them to identify suspicious JA3 fingerprints associated with malware such as Remcos RAT, WannaCry, and Go-based data exfiltration tools linked to the Skuld malware family.

Key takeaways from the research include:

· JA3 reflects attacker tooling, not just individual attack artifacts;

· The same JA3 often appears across multiple samples and campaigns;

· Sudden JA3 frequency spikes can indicate new malicious tools early;

· JA3 is harder for attackers to rotate than IPs or domains;

· JA3 is most effective when enriched with additional context.

The full article, including technical explanations, real-world case studies, and indicators of compromise, is available on ANY.RUN's blog.

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

ANY.RUN's Threat Intelligence Lookup enables analysts to search directly by JA3 hash and immediately see associated malware families and network infrastructure.

From a business perspective, this context-rich approach to threat intelligence directly reduces risk and response time. Faster, more confident investigations mean fewer false positives, lower operational costs, and stronger protection of critical business assets. In this way, JA3-powered threat intelligence becomes not just a technical advantage, but a measurable business safeguard.

ANYRUN FZCO
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
LinkedIn
X