LOLBin Cyberattacks Are Now a Major Threat to Businesses, but SOCs Found a Way to Detect Them

DUBAI, DUBAI, UNITED ARAB EMIRATES, November 20, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, has released a new technical guide, designed to help SOC managers navigate one of today's most overlooked intrusion techniques: attackers hiding malicious activity inside trusted Windows binaries.

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

Tools like rundll32, certutil, and mshta are built into every Windows environment and widely trusted. Threat actors take advantage of this trust to decode payloads, load disguised modules, and trigger in-memory execution with very few artifacts left behind.

For SOC teams, this means early activity often looks routine, forcing analysts to rely on subtle behavioral clues rather than signatures or file reputation.

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

Alongside the real-world attack examples, the guide gives SOC leaders actionable steps to operationalize LOLBin detection across their teams. Instead of treating rundll32, certutil, and mshta as background noise, the framework helps managers turn these binaries into high-value behavioral signals the SOC can act on quickly.

The guide outlines how SOC teams can use interactive sandboxing to:

· Confirm suspicious activity in trusted binaries within minutes, not hours

· Cut down false escalations by validating unclear alerts through live analysis

· Give analysts immediate visibility into decoding, module loading, and hidden PowerShell

· Standardize investigations with a repeatable workflow for “clean-looking” alerts

· Feed findings back into SIEM/EDR rules and strengthen detection over time

To discover more real-world examples and strengthen your team’s detection strategy, visit the ANY.RUN blog.

□□□□□ □□□.□□□

ANY.RUN is a cloud-based, interactive malware analysis and threat intelligence provider trusted by 15,000+ organizations and 500,000 analysts worldwide. It delivers real-time behavioral visibility, a user-friendly sandbox for Windows and Linux, and an extensive threat intelligence ecosystem. By helping SOC teams detect threats faster, validate alerts with confidence, and uncover hidden activity in minutes, ANY.RUN enables organizations to strengthen their security operations with greater accuracy and speed.

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