Redline Stealer: A Looming Threat in the Information-Stealing Landscape

A new, more evasive variant of the Redline Stealer trojan has been discovered. This malware hides its malicious code using Lua bytecode and employs multiple methods to stay persistent on infected systems. Disguised as a software installer named "Cheat.Lab.2.7.2.zip", it infects machines and steals user data like usernames and screenshots. The stolen information is then sent to the attacker's server. What makes this variant particularly concerning is its use of Lua bytecode, which makes detection by traditional security software more difficult. Additionally, the malware uses two techniques to ensure it keeps running on an infected system: scheduled tasks and a mechanism that exploits a Windows error handling process. This combination makes Redline Stealer a serious threat, highlighting the need for robust security solutions and caution when downloading software.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.