Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:05:46 UTC

Description(Cofense) RedLine Stealer, first seen in 2020, is probably the most well-known stealer on this list. It uses Simple Object Access Protocol (SOAP) for communication with its command-and-control center and can use a variety of plugins. It’s used to collect information from various installed programs including credentials stored in browsers, email applications, as well as cryptocurrency wallet data. RedLine Stealer is often associated with sophisticated phishing campaigns that, after a successful infection, can deliver additional payloads like ransomware or more advanced malware.
