Jackpotting ESXi Servers For Maximum Encryption

Published: 2021-03-09 · Archived: 2026-04-05 13:41:39 UTC

SPRITE SPIDER is a major eCrime actor that has conducted numerous successful attacks using the Defray777 ransomware. Despite SPRITE SPIDER’s consistent operational tempo and numerous successes, there has been minimal public reporting on the adversary. This is likely due in part to the adversary’s particularly sophisticated tactics, techniques, and procedures (TTPs), which thwart many traditional cyber threat intelligence (CTI) methodologies. Our presentation describes SPRITE SPIDER’s current modus operandi, focusing on the adversary’s advanced operational security and uncommon TTPs. Eric Loui, Senior Intelligence Analyst, CrowdStrike Sergei Frankoff, Senior Security Researcher, CrowdStrike View upcoming Summits: http://www.sans.org/u/DuS Download the presentation slides (SANS account required) at http://www.sans.org/u/195g #CTISummit #cyberthreatintelligence

SANS 2021 CTI Summit

av SANS Digital Forensics and Incident Response
