Venom Spider, Golden Chickens - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:16:23 UTC

Description(Proofpoint) Since the middle of 2018, Proofpoint has been tracking campaigns abusing legitimate messaging services, offering fake jobs, and repeatedly following up via email to ultimately deliver the More_eggs backdoor. These campaigns primarily targeted US companies in various industries including retail, entertainment, pharmacy, and others that commonly employ online payments, such as online shopping portals.

The actor sending these campaigns attempts to establish rapport with potential victims by abusing LinkedIn's direct messaging service. In direct follow-up emails, the actor pretends to be from a staffing company with an offer of employment. In many cases, the actor supports the campaigns with fake websites that impersonate legitimate staffing companies. These websites, however, host the malicious payloads. In other cases, the actor uses a range of malicious attachments to distribute More_eggs.

Taurus Loader has been observed to distribute GandCrab and Sodinokibi (Pinchy Spider, Gold Southfield) and Trickbot (Wizard Spider, Gold Blackburn), as well as their own tool More_eggs.
