Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:54:05 UTC

Description(Menlo Labs) The term “Soc” in the “SocGholish” framework refers to the attack’s use of social engineering toolkits masquerading as a software update. Thus far, Menlo has observed this particular framework using several social engineering themes that impersonate browser updates (Chrome/Firefox), Flash Player updates, and more recently, Microsoft Teams updates.
