

Microsoft Threat Intelligence on X: "SocGholish, a malware distribution network, started updating its tradecraft toward the end of 2021 with new C2 infrastructure almost every month, additional ways to deploy Cobalt Strike, and the use of publicly available tools for discovery and credential dumping." / X

Published: 2022-05-06 · Archived: 2026-04-05 17:02:04 UTC

Don't miss what's happening

People on X are the first to know.

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly.

Post

Conversation



SocGholish, a malware distribution network, started updating its tradecraft toward the end of 2021 with new C2 infrastructure almost every month, additional ways to deploy Cobalt Strike, and the use of publicly available tools for discovery and credential dumping.

Sign up now to get your own personalized timeline!

Trending now

What's happening

Source: <https://twitter.com/MsftSecIntel/status/1522690116979855360>