Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:41:52 UTC

APT group: Hydrochasma

Names	Hydrochasma *(Symantec)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2022
Description	(Symantec) Shipping companies and medical laboratories in Asia are being targeted in a likely intelligence-gathering campaign that relies exclusively on publicly available and living-off-the-land tools. Hydrochasma, the threat actor behind this campaign, has not been linked to any previously identified group, but appears to have a possible interest in industries that may be involved in COVID-19-related treatments or vaccines. This activity has been ongoing since at least October 2022. While Symantec, by Broadcom Software, did not see any data being exfiltrated in this campaign, the targets, as well as some of the tools used, indicate that the most likely motivation in this campaign is intelligence gathering.
Observed	Sectors: Healthcare, Shipping and Logistics. Countries: Asia.
Tools used	BrowserGhost, Cobalt Strike, GO Simple Tunnel, HackBrowserData, ProcDump, SoftEther VPN, Living off the Land.
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hydrochasma-asia-medical-shipping-intelligence-gathering>

Last change to this card: 25 April 2023

Download this actor card in PDF or JSON format