Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:46:31 UTC

Other threat group: Bismuth

Names	Bismuth *(Microsoft)* Canvas Cyclone *(Microsoft)*
Country	Vietnam
Motivation	Information theft and espionage, Financial gain
First seen	2012
Description	(Microsoft) BISMUTH, which shares similarities with APT 32, OceanLotus, SeaLotus, has been running increasingly complex cyberespionage attacks as early as 2012, using both custom and open-source tooling to target large multinational corporations, governments, financial services, educational institutions, and human and civil rights organizations. But in campaigns from July to August 2020, the group deployed Monero coin miners in attacks that targeted both the private sector and government institutions in France and Vietnam. Because BISMUTH's attacks involved techniques that ranged from typical to more advanced, devices with common threat activities like phishing and coin mining should be elevated and inspected for advanced threats. More importantly, organizations should prioritize reducing attack surface and hardening networks against the full range of attacks. In this blog, we'll provide in-depth technical details about the BISMUTH attacks in July and August 2020 and mitigation recommendations for building organizational resilience.
Observed	Sectors: Education, Financial, Government. Countries: France, Vietnam.
Tools used	
Information	<https://www.microsoft.com/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them/>

Last change to this card: 26 April 2023

Download this actor card in PDF or JSON format