Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:17:43 UTC

APT group: Bronze Starlight

Names	Bronze Starlight *(SecureWorks)* DEV-0401 *(Microsoft)* Cinnamon Tempest *(Microsoft)* Operation ChattyGoblin *(SentinelLabs)* SLIME34 *(?)* HighGround *(CrowdStrike)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2021	
Description	(SecureWorks) BRONZE STARLIGHT has been active since mid 2021 and targets organizations globally across a range of industry verticals. The group leverages HUI Loader to load Cobalt Strike and PlugX payloads for command and control. CTU researchers have observed BRONZE STARLIGHT deploying ransomware to compromised networks as part of name-and-shame ransomware schemes, and posted victim names to leak sites. CTU researchers assess with moderate confidence that BRONZE STARLIGHT is located in China based on observed tradecraft, including the use of HUI Loader and PlugX which are associated with China-based threat group activity. It is plausible that BRONZE STARLIGHT deploys ransomware as a smokescreen rather than for financial gain, with the underlying motivation of stealing intellectual property theft or conducting espionage.	
Observed	Sectors: Casinos and Gambling. Countries: Philippines and Southeast Asia.	
Tools used	AtomSilo, Cobalt Strike, HUI Loader, LockFile, NightSky, Pandora, PlugX, Rook.	
Operations performed	Mar 2023	Chinese Entanglement | DLL Hijacking in the Asian Gambling Sector

		<https://www.sentinelone.com/labs/chinese-entanglement-dll-hijacking-in-the-asian-gambling-sector/>
Information	<https://www.secureworks.com/research/threat-profiles/bronze-starlight> <https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader>	

Last change to this card: 28 June 2025

Download this actor card in PDF or JSON format
