LevelBlue - Open Threat Exchange

By AlienVault

Archived: 2026-04-05 14:56:00 UTC

CVE: 5 | **FileHash-MD5:** 2 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 195 | **URL:** 4 | **YARA:** 1 | **Domain:** 2 | **Hostname:** 99

BlackTech is a cyber espionage group operating against targets in East Asia, particularly Taiwan, and occasionally, Japan and Hong Kong. Based on the mutexes and domain names of some of their C&C servers, BlackTech’s campaigns are likely designed to steal their target’s technology. Following their activities and evolving tactics and techniques helped us uncover the proverbial red string of fate that connected three seemingly disparate campaigns: PLEAD, Shrouded Crossbow, and of late, Waterbear. Over the course of their campaigns, we analyzed their modus operandi and dissected their tools of the trade—and uncovered common denominators indicating that PLEAD, Shrouded Crossbow, and Waterbear may actually be operated by the same group.
