# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:16:27 UTC



## APT group: Bronze Highland

| | |
|---|---|
| Names | Bronze Highland *(SecureWorks)*<br>Evasive Panda *(Malwarebytes)*<br>Daggerfly *(Symantec)*<br>Storm Cloud *(Volexity)*<br>StormBamboo *(Volexity)*<br>TAG-102 *(Recorded Future)*<br>TAG-112 *(Recorded Future)*<br>Digging Taurus *(Palo Alto)* |
| Country | China |
| Sponsor | State-sponsored |
| Motivation | Information theft and espionage |
| First seen | 2012 |
| Description | (SecureWorks) BRONZE HIGHLAND has been observed using spearphishing as an initial infection vector to deploy the MgBot remote access trojan against targets in Hong Kong. Third party reporting suggests the threat group also targets India, Malaysia and Taiwan and leverages Cobalt Strike and KsRemote Android Rat. CTU researchers assess with moderate confidence that BRONZE HIGHLAND operates on behalf of China and has a remit covering espionage against domestic human rights and pro-democracy advocates and nations neighbouring China. |
| Observed | Sectors: Telecommunications and human rights and pro-democracy advocates. Countries: China, Hong Kong, India, Macao, Malaysia, Myanmar, Nigeria, Philippines, Taiwan, Tibet, Vietnam and Africa. |
| Tools used | CloudScout, Cobalt Strike, GIMMICK, Nightdoor, Macma, MgBot, KsRemote, RELOADEXT, Living off the Land. |

| | | |
|---|---|---|
| Operations performed | 2020 | Evasive Panda APT group delivers malware via updates for popular Chinese software <https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/> |
| | Late 2021 | Storm Cloud on the Horizon: GIMMICK Malware Strikes at macOS <https://www.volexity.com/blog/2022/03/22/storm-cloud-on-the-horizon-gimmick-malware-strikes-at-macos/> |
| | 2022 | CloudScout: Evasive Panda scouting cloud services <https://www.welivesecurity.com/en/eset-research/cloudscout-evasive-panda-scouting-cloud-services/> |
| | Nov 2022 | Daggerfly: APT Actor Targets Telecoms Company in Africa <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt-attacks-telecoms-africa-mgbot> |
| | Mid 2023 | StormBamboo Compromises ISP to Abuse Insecure Software Update Mechanisms <https://www.volexity.com/blog/2024/08/02/stormbamboo-compromises-isp-to-abuse-insecure-software-update-mechanisms/> |
| | Sep 2023 | Evasive Panda leverages Monlam Festival to target Tibetans <https://www.welivesecurity.com/en/eset-research/evasive-panda-leverages-monlam-festival-target-tibetans/> |
| | May 2024 | China-Nexus TAG-112 Compromises Tibetan Websites to Distribute Cobalt Strike <https://go.recordedfuture.com/hubfs/reports/cta-cn-2024-1112.pdf> |
| | Jul 2024 | Daggerfly: Espionage Group Makes Major Update to Toolset <https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset> |
| Information | <https://www.secureworks.com/research/threat-profiles> <https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware/> <https://vb2020.vblocalhost.com/uploads/VB2020-43.pdf> | |

Last change to this card: 27 June 2025

Download this actor card in PDF or JSON format