# Goblin Panda, Cycldek, Conimes - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:46:24 UTC



## APT group: Goblin Panda, Cycldek, Conimes

| | | |
|---|---|---|
| Names | Goblin Panda *(CrowdStrike)*<br>Cycldek *(Kaspersky)*<br>Conimes *(Anomali)*<br>1937CN *(?)* | |
| Country | China | |
| Motivation | Information theft and espionage | |
| First seen | 2013 | |
| Description | (CrowdStrike) CrowdStrike first observed Goblin Panda activity in September 2013 when indicators of its activity were discovered on the network of a technology company operating in multiple sectors.<br><br>Malware variants primarily used by this actor include PlugX and HttpTunnel. This actor focuses a significant amount of its targeting activity on entities in Southeast Asia, particularly Vietnam. Heavy activity was observed in the late spring and early summer of 2014 when tensions between China and other Southeast Asian nations were high, due to conflict over territory in the South China Sea. Goblin Panda targets have been primarily observed in the defense, energy, and government sectors. | |
| Observed | Sectors: Defense, Energy, Government.<br>Countries: Cambodia, India, Indonesia, Laos, Malaysia, Myanmar, Philippines, Thailand, USA, Vietnam. | |
| Tools used | 8.t Dropper, BlueCore, BrowsingHistoryView, ChromePass, CoreLoader, DropPhone, FoundCore, HDoor, HTTPTunnel, JsonCookies, nbtscan, NewCore RAT, PlugX, ProcDump, PsExec, QCRat, RedCore, Sisfader, USBCulprit, ZeGhost, Living off the Land. | |
| Operations performed | Jul 2016 | A group identifying as Chinese hackers has attacked digital signage screens, overhead announcement systems and airline systems at airports across Vietnam. |

| | | |
|---|---|---|
| | | <https://www.infosecurity-magazine.com/news/chinese-hackers-attack-airports/> |
| | Sep 2017 | Recently, FortiGuard Labs came across several malicious documents that exploit the vulnerability CVE-2012-0158. <https://www.fortinet.com/blog/threat-research/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations> |
| | 2018 | Attacks have been witnessed in government organizations across several Southeast Asian countries, namely Vietnam, Thailand and Laos, using a variety of tools and new TTPs. <https://securelist.com/cycldek-bridging-the-air-gap/97157/> |
| | Jun 2020 | The leap of a Cycldek-related threat actor <https://securelist.com/the-leap-of-a-cycldek-related-threat-actor/101243/> |
| Information | <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-august-goblin-panda/> | |
| Playbook | <https://www.fortinet.com/blog/threat-research/cta-security-playbook--goblin-panda.html> | |

Last change to this card: 15 May 2021

Download this actor card in PDF or JSON format

---