# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:10:12 UTC

## APT group: TA428

| | |
|---|---|
| Names | TA428 *(Proofpoint)*<br>Panda *(NTT)*<br>ThunderCats *(SentinelLabs)* |
| Country | China |
| Motivation | Information theft and espionage |
| First seen | 2013 |
| Description | (Proofpoint) Proofpoint researchers initially identified email campaigns with malicious RTF document attachments targeting East Asian government agencies in March 2019. These campaigns originated from adversary-operated free email sender accounts at yahoo[.]co[.].jp and yahoo[.]com. Sender addresses often imitated common names found in the languages of targeted entities. Spear phishing emails included malicious .doc attachments that were actually RTF files saved with .doc file extensions.<br><br>The lures used in the subjects, attachment names, and attachment content in several cases utilized information technology themes specific to Asia such as governmental or public training documents relating to IT. On one specific occasion an email utilized the subject “ITU Asia-Pacific Online CoE Training Course on ‘Conformity & Interoperability in 5G’ for the Asia-Pacific Region, 15-26 April 2019” and the attachment name “190315_annex 1 online_course_agenda_coei_c&i.doc”. The conference referenced in the lure was an actual event likely selected due to its relevance to potential victims. This is significant as countries in the APAC region continue to adopt Chinese 5G technology in government as well as heavy equipment industries.<br><br>This actor worked together with Emissary Panda, APT 27, LuckyMouse, Bronze Union in Operation StealthyTrident. |
| Observed | Sectors: Government and industrial plants, design bureaus and research institutes.<br>Countries: Afghanistan, Belarus, Mongolia, Russia, Ukraine and East Asia. |
| Tools used | 8.t Dropper, Albaniiutas, Cotx RAT, CoughingDown, PhantomNet, PlugX, Poison Ivy, TManger. |

| | | |
|---|---|---|
| Operations performed | Mar 2019 | Operation “LagTime IT”<br>Attackers relied on Microsoft Equation Editor exploit CVE-2018-0798 to deliver a custom malware that Proofpoint researchers have dubbed Cotx RAT.<br>Additionally, this APT group utilizes Poison Ivy payloads that share overlapping command and control (C&C) infrastructure with the newly identified Cotx campaigns.<br><https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology><br><https://insight-jp.nttsecurity.com/post/102gi9b/pandas-new-arsenal-part-1-tmanger> |
| | Jun 2020 | Operation “StealthyTrident”<br>ESET researchers discovered that chat software called Able Desktop, part of a business management suite popular in Mongolia and used by 430 government agencies in Mongolia.<br><https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/><br><https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/> |
| | Dec 2020 | China-linked TA428 Continues to Target Russia and Mongolia IT Companies<br><https://www.recordedfuture.com/china-linked-ta428-threat-group/> |
| | May 2021 | ThunderCats Hack the FSB<br><https://labs.sentinelone.com/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op/><br><https://blog.group-ib.com/task> |
| | Jan 2022 | Targeted attack on industrial enterprises and public institutions<br><https://securelist.com/targeted-attack-on-industrial-enterprises-and-public-institutions/107054/> |
| Information | <https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology><br><https://st.drweb.com/static/new-www/news/2021/april/drweb_research_attacks_on_russian_research_institutes_en.pdf><br><https://labs.sentinelone.com/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op/> | |

Last change to this card: 12 September 2022

Download this actor card in PDF or JSON format

---