


100 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:19:52 UTC

APT group: TAG-100

Names	TAG-100 (<i>Recorded Future</i>) Storm-2077 (<i>Microsoft</i>)
Country	 China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2024
Description	(Recorded Future) Recorded Future's Insikt Group identified new suspected cyber-espionage activity targeting high-profile government, intergovernmental, and private sector organizations globally. This activity, which we are tracking under the temporary group designator TAG100, has employed open-source remote access capabilities and exploited a wide range of internet-facing appliances for initial access. Using Recorded Future® Network Intelligence data, Insikt Group identified the likely compromise of the secretariats of two major Asia-Pacific intergovernmental organizations by TAG100 using the open-source, multi-platform Go backdoor Pantegana. Other targeted organizations include multiple diplomatic entities and ministries of foreign affairs, as well as industry trade associations and semiconductor supply-chain, non-profit, and religious organizations globally. At this time, Insikt Group is continuing to explore potential attribution for this activity; however, the specific targeting and victimology identified align with a suspected espionage motive.
Observed	Sectors: Embassies , Financial , Government , High-Tech . Countries: Bolivia , Cambodia , Cuba , Djibouti , Dominican Republic , Fiji , France , Indonesia , Italy , Japan , Malaysia , Netherlands , Taiwan , UK , USA , Vietnam .
Tools used	Cobalt Strike , CrossC2 , LESLIELOADER , Pantegana , SparkRAT .
Information	< https://go.recordedfuture.com/hubfs/reports/cta-2024-0716.pdf > < https://www.microsoft.com/en-us/security/blog/2024/11/22/microsoft-shares-latest-intelligence-on-north-korean-and-chinese-threat-actors-at-cyberwarcon/ >

Last change to this card: 26 December 2024

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.eta.or.th/cgi-bin/showcard.cgi?u=b01702b6-b1dc-4292-8a10-dfb87acfd59>