

Updated Cyber Threat Actor Naming System

By Google Threat Intelligence Group

Published: 2026-07-24 · Archived: 2026-08-07 02:00:21 UTC

Update (July 30): A table listing the new names of select prominent threat actors was appended to this post.

Introduction

Today, Google Threat Intelligence Group (GTIG) will begin rolling out a unified naming schema for tracking threat actors. This new naming taxonomy represents an effort to standardize tracking across platforms and public reporting.

Why are we Adopting a Different Naming System?

Historically, Mandiant and Google's Threat Analysis Group (TAG) maintained distinct tracking systems, relying on parallel naming schemas that grew independently over time. The creation of GTIG has necessitated a new, fused tracking system, and a new naming system. Thinking to the future, GTIG's new system will rely on cryptonyms. Relying on sequential numbers or disparate identifiers (e.g. APT1) fails to provide defenders the critical context needed to operate quickly. Threat tracking shouldn't be an exercise in memorization, but rather one of intuition. The new naming convention aligns with industry standard threat actor naming systems.

Our New Schema

Our new schema utilizes a cryptonym-based approach, employing memorable two-word combinations for each distinct threat actor:

- The **first word** is a unique and memorable term chosen to represent the specific actor, particularly names that may have been used in prior public reporting. If no previously used term exists, this word is randomly generated to remove bias, then vetted by our analysts.
- The **second word** categorizes threat clusters by motivation, attribution, or activity type based on which category we consider to be most important for defense and response strategies.

The table below provides a sample of how threat actor categories will map to the second word in each cryptonym:

Origin or Type	Group Name
People's Republic of China	CASTLE

Iran	ION
North Korea	NEPTUNE
Russia	RELIC
Cybercriminal	COMET

Table 1: Examples of Google’s new threat actor naming system categories

We know there are many threat actor tracking schemas in the industry, so we are intentionally seeking to keep this system as simple as possible to streamline operations and facilitate mapping to other naming taxonomies. However, a significant caveat remains: because no two organizations have the exact same visibility into the threat landscape, direct, apples-to-apples comparisons between threat actors are rarely possible. Transitioning to a convention that is simpler to follow and remember is a practical step toward managing a highly intricate tracking problem.

A Work in Progress

We have initially prioritized renaming several dozen of the most active groups, and will continue this process on a rolling basis. Previous names will remain indexed and searchable in the Google Threat Intelligence (GTI) platform, with MITRE ATT&CK mappings and other vendor aliases preserved, see Figure 1.

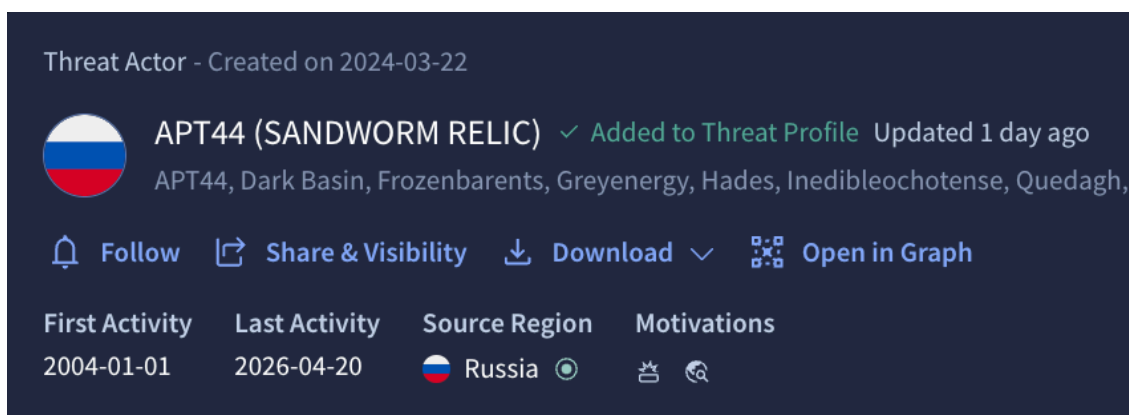


Figure 1: Threat actor name appearance in GTI platform on initial rollout

We will continue to use UNC, or “uncategorized” designations for threat clusters that are still in the early stages of investigation, as described [here](#).

Selection of Re-Named Threat Actors

Origin or Type	Previously Used Names	New Names
Cybercriminal	FIN11	RAZOR COMET
Cybercriminal	FIN6	SQUID COMET
Cybercriminal	FIN7	WILD COMET
Cybercriminal	FIN8	PUNCH COMET
Iran	APT33	BLEAK ION
Iran	APT34	SOLAR ION
Iran	APT35	RICH ION
Iran	APT39	CINDER ION
Iran	APT42, CALANQUE	CALANQUE ION
Iran	TEMP.Zagros, MUDDYCOAST	MUDDY ION
North Korea	APT37	PLAIN NEPTUNE
North Korea	APT45	GRASS NEPTUNE
North Korea	UNC1069, MASAN	MIDNIGHT NEPTUNE
North Korea	Temp.Hermit	HERMIT NEPTUNE

People's Republic of China (PRC)	APT15	RIVER CASTLE
PRC	APT20	RIDGE CASTLE
PRC	UNC1088	RAVINE CASTLE
PRC	APT27	SHORE CASTLE
PRC	APT30	ISTHMUS CASTLE
PRC	APT31	TIDE CASTLE
PRC	APT40	ISLAND CASTLE
PRC	APT41	SPIRE CASTLE
PRC	APT5	BASALT CASTLE
PRC	Tonto Team	LONE CASTLE
PRC	TEMP.Tick	TICK CASTLE
PRC	UNC2814	DARK CASTLE
PRC	Naikon Team	NAIKON CASTLE
PRC	Conference Crew	CONFERENCE CASTLE
PRC	TEMP.Hex	BASIN CASTLE

PRC	TEMP.Overboard	CAVERN CASTLE
Russia	APT28, FROZENLAKE	LAKE RELIC
Russia	APT29, ICECAP	ICE RELIC
Russia	APT44, FROZENBARENTS	SANDWORM RELIC
Russia	UNC4057, COLDRIVER	COLD RELIC
Russia	TEMP.Vermin	VERMIN RELIC
Russia	Turla Team	TURLA RELIC

Table 2: Selection of Re-named Threat Actors

Posted in

- [Threat Intelligence](#)

Source: <https://cloud.google.com/blog/topics/threat-intelligence/updated-cyber-threat-actor-naming-system/>