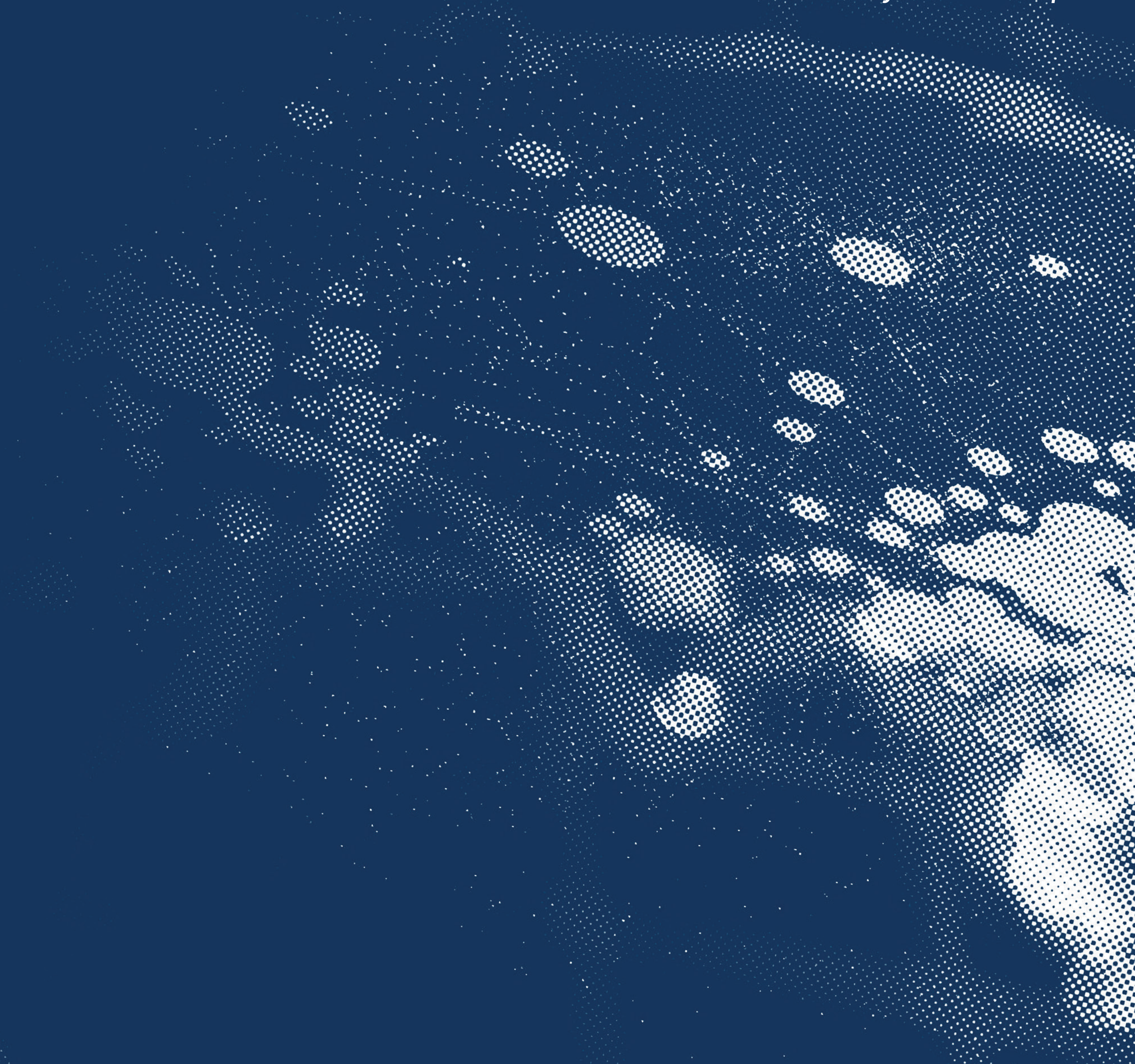
Recorded Future®

Recorded Future's Threat Actor and Malware Taxonomy

By Insikt Group®



Insikt Group, the threat intelligence research arm of Recorded Future, tracks a wide variety of threat actors and threat activity groups linked to governments, militaries, hacktivist elements, and cybercriminal gangs globally. Beginning in 2018, Insikt adopted a simple taxonomy for classifying advanced persistent threat (APT; cyber espionage) groups linked to the various countries which comprise the “Big 4” — China, Russia, Iran, and North Korea — based on a color on the respective country’s national flag and a unique codeword from the NATO phonetic alphabet (for example, “RedAlpha” for the first named China-based group). Since that time, Insikt’s threat actor tracking tradecraft and methodology has advanced significantly, enabling us to name more APT or advanced cybercriminal groups in a way that reflects Recorded Future’s unique visibility into the threat actors and their activities.

This white paper serves as a reference document for Recorded Future’s naming conventions for threat actor groups. The use of our own naming taxonomy ensures that Insikt Group is able to accurately reflect overlaps and divergences in activity, infrastructure, or tactics, techniques, and procedures (TTPs) with already established group names from other cyber intelligence researchers. Additionally, this taxonomy provides us with the flexibility to create additional group names for APT groups outside of the Big 4, or transnational cybercrime groups, as needed. Our intention is not to unnecessarily add to the already complex landscape of threat actor group names across the community, but rather to appropriately refer to the activity we observe in an analytically rigorous fashion so as to avoid confusion or conflict with existing clusters into which we do not have full visibility.

Insikt Group’s currently assigned colors and their respective countries are shown below.

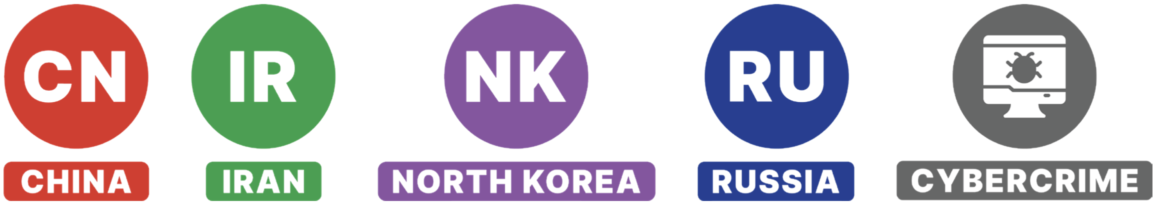


Figure 1: *Currently assigned colors and their respective attribution*

The table below describes Recorded Future's taxonomy for naming APT groups, advanced cybercriminal gangs, hacktivists, and newly identified malware families.

Type	Schema
State-Sponsored APTs	**Named groups (such as "RedDelta"):** A "color + codeword" combination, constructed as follows: • A color or mixture of colors found on the attributed country's national flag (such as "Red" for China) • A unique codeword from the NATO phonetic alphabet Derivations of colors (such as "Burgundy" instead of "Red") are chosen as needed to refer to new countries when the "base" color is already in use by another country. **Threat activity group (TAG-##; such as TAG-22):** Created in ascending sequential order. TAGs are country-attribution agnostic. *Note: Attribution to specific government ministries, military units, front companies, or individuals, when possible, is not reflected in APT group names, as they are reflective of assessments of national origin. Such linkages will be identified with supporting evidence in relevant reporting.*
Advanced Cybercriminal Gangs	**Groups lacking names:** "Gray" and a cardinal number, in sequential ascending order (such as Gray1, Gray2, and so on). Gray-named groups, intended to represent advanced transnational or non-state sponsored cybercrime groups, are not attributed to a given geography. **Groups naming themselves:** Use the self-given names (such as "Conti Ransomware Gang").
Hacktivists	Use their self-given names (such as "KillNet").
Newly Identified Malware	Mathematical and scientific terms (such as "GraphicalNeutrino").

Table 1: *Insikt Group's threat actor and malware naming conventions schema.*

TAGs and Named Groups

Insikt Group uses a two-tier taxonomy for classifying threat activity linked to APT groups specifically: Threat Activity Groups (TAGs) and "named groups" (such as "BlueBravo").

We track developing APT group activity as TAGs under the syntax "TAG-##", such as "TAG-22". TAGs are agnostic with respect to country-level attribution and are used prior to graduating to a formally named group. This approach is conceptually similar to that adopted by numerous other cyber intelligence research groups, such as Microsoft's "Storm-XXXX" and Mandiant's "UNC####" groups. We use these TAG-## designations when:

- We have limited information about a threat activity group
- We do not have sufficient evidence to attribute the activity to an existing group name
- We lack sufficient information to attribute the activity to a particular country (adversary vertex of the Diamond Model of Intrusion Analysis)

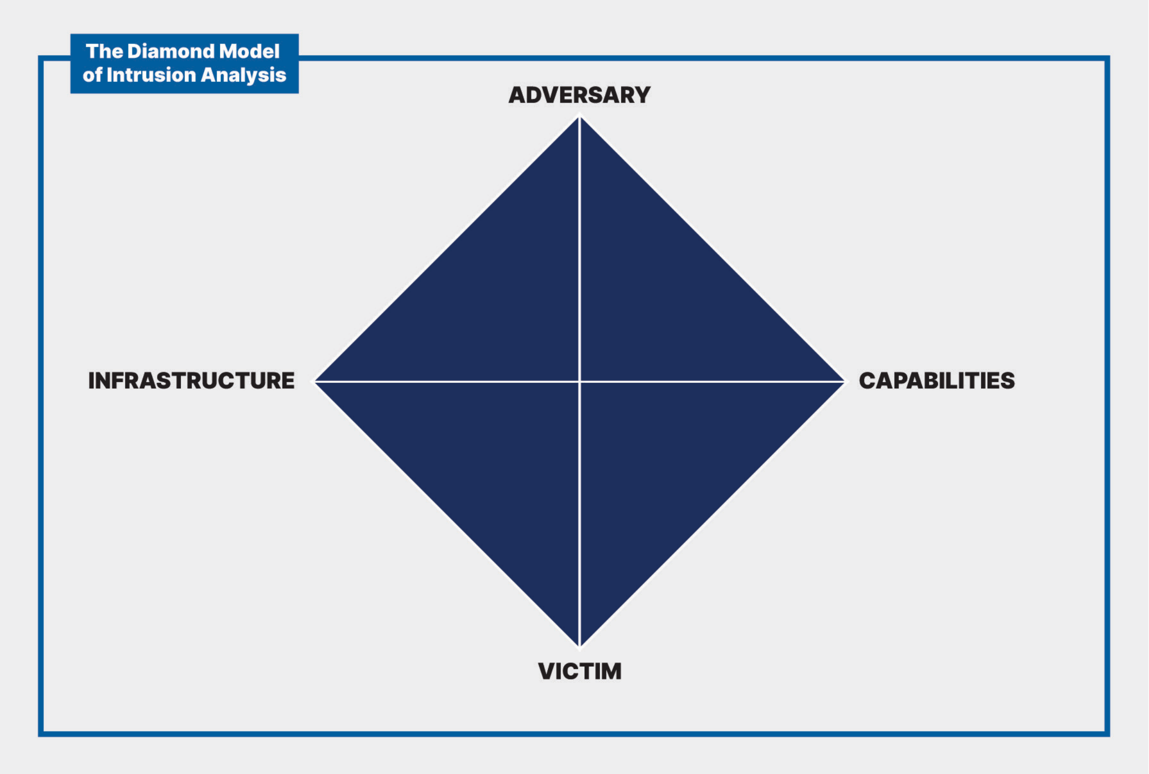


Figure 2: *The Diamond Model of Intrusion Analysis*

TAGs are often used to describe a cluster of activity or TTPs we observe that may be linked to an existing APT group but has not yet crossed the threshold of being graduated into a named group. For Insikt to create a TAG, Insikt Group analysts must at a minimum be able to sufficiently populate 2 vertices of the Diamond Model of Intrusion Analysis.

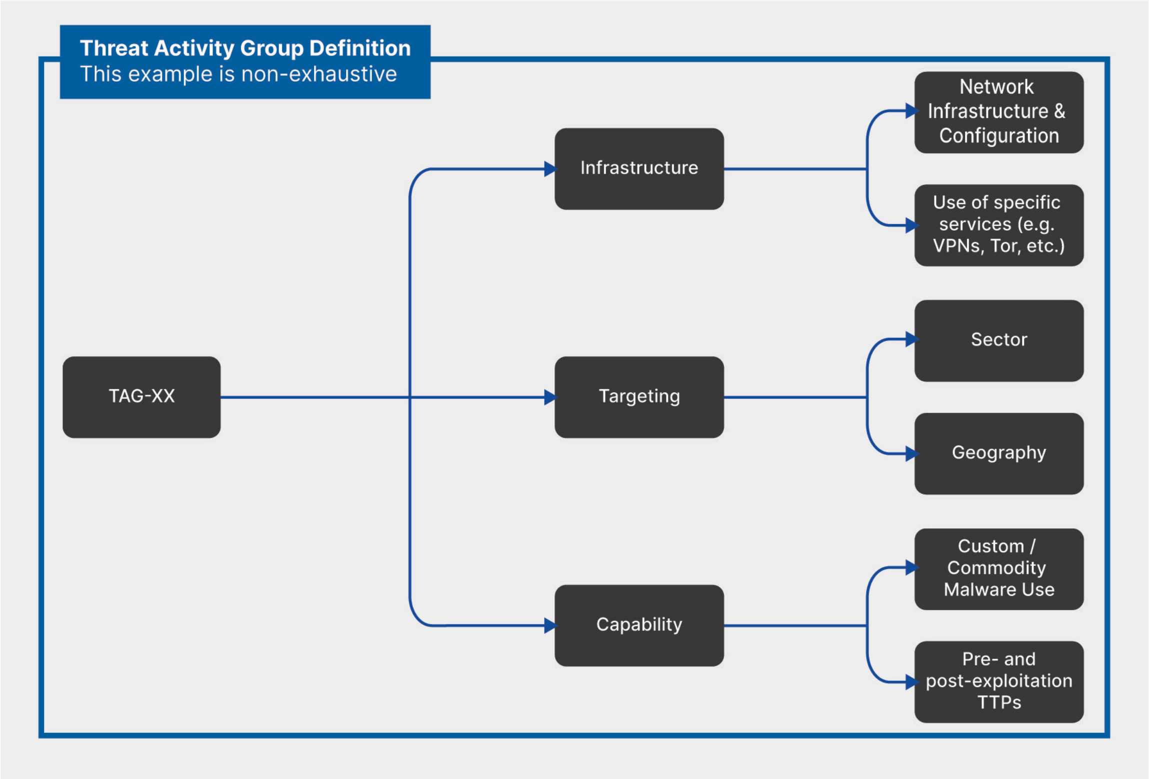

Threat Activity Group Definition
This example is non-exhaustive
TAG-XX
Infrastructure
Targeting
Capability
Network Infrastructure & Configuration
Use of specific services (e.g. VPNs, Tor, etc.)
Sector
Geography
Custom / Commodity Malware Use
Pre- and post-exploitation TTPs

Figure 3: *A high-level visual representation of some of the facets of a TAG.*

Over time, as more data is accumulated and confidence in our assessments of a TAG (or a collection of interrelated TAGs) grows, we will graduate the cluster(s) to a formal, named group. The key element of the decision to graduate a TAG is the amassing of enough supporting evidence to form a high-confidence assessment of the location of the group or the national origin.

Beyond country-level attribution, Insikt is occasionally able to more definitively link between particular APT groups and specific government ministries, military units, front companies, or even individuals. On such occasions, we will identify such linkages with appropriate supporting evidence in public reporting, as we did with our June 2021 report on RedFoxtrot, linked to Chinese People's Liberation Army (PLA) Unit 69010, in Urumqi, Xinjiang province, China. This more granular attribution, however, is not reflected in our naming taxonomy, and the chosen group name remains national-level.

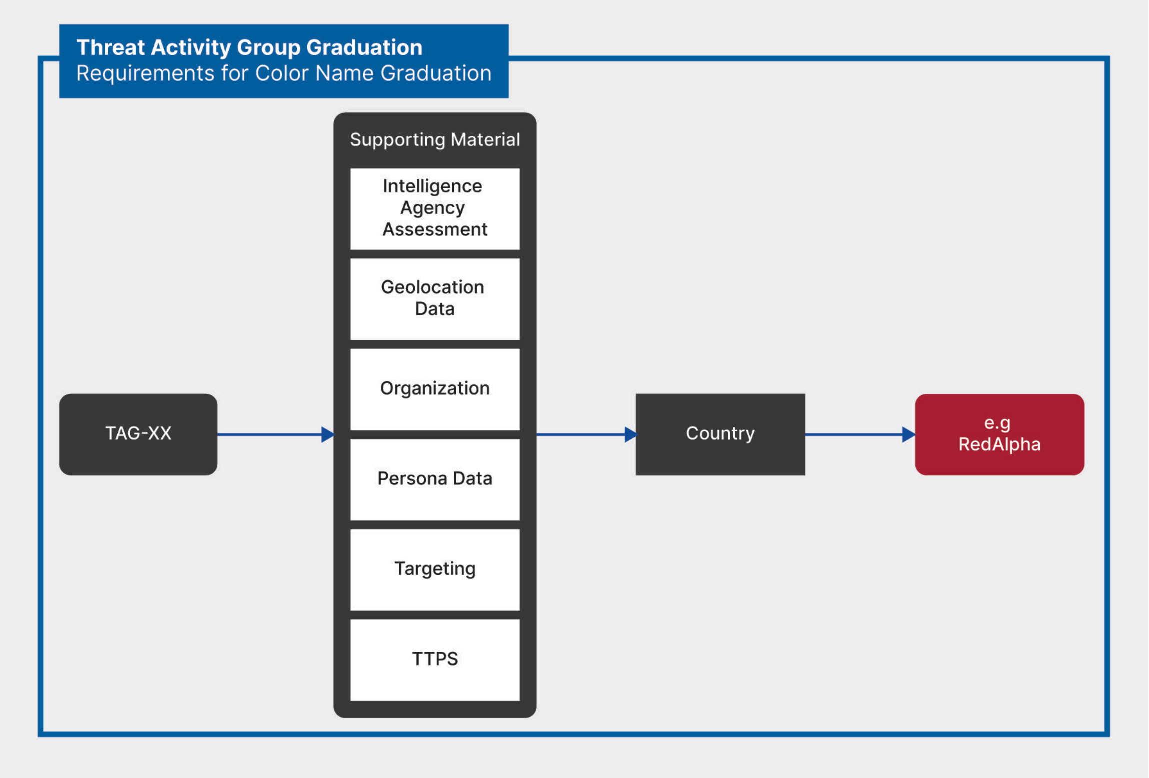

Threat Activity Group Graduation
Requirements for Color Name Graduation
TAG-XX
Supporting Material
Intelligence Agency Assessment
Geolocation Data
Organization
Persona Data
Targeting
TTPS
Country
e.g RedAlpha

Figure 4: *The process of graduating a TAG to a named group.*

Publicly Named Groups

As of April 2023, Insikt Group has formally named 9 distinct APT groups using our taxonomy, as well as made public a small subset of the over 80 TAGs which we track. The table below shows the current publicly released TAG and named groups, their attribution, known overlaps with existing naming conventions, and relevant Insikt Group reporting.

Name	Attributed Country	Overlapping Groups	Reports
BlueAlpha	Russia	Gamaredon, Aqua Blizzard, Primitive Bear	Operation Gamework: Infrastructure Overlaps Found Between BlueAlpha and Iranian APTs
BlueBravo	Russia	APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, Midnight Blizzard, The Dukes, Cozy Bear, CozyDuke	BlueBravo Uses Ambassador Lure to Deploy GraphicalNeutrino Malware
RedAlpha	China	DeepCliff, Red Dev 3	RedAlpha: New Campaigns Discovered Targeting the Tibetan Community RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations
RedBravo	China	APT31, Violet Typhoon	From Coercion to Invasion: The Theory and Execution of China's Cyber Activity in Cross-Strait Relations

Name	Attributed Country	Overlapping Groups	Reports
RedDelta	China	BRONZE PRESIDENT, HoneyMyte, Mustang Panda, Red Lich, TA416	Chinese State-Sponsored Group 'RedDelta' Targets the Vatican and Catholic Organizations Back Despite Disruption: RedDelta Resumes Operations RedDelta Targets European Government Organizations and Continues to Iterate Custom PlugX Variant
RedEcho	China	N/A	China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions
RedFoxtrot	China	Moshen Dragon, Temp. Trident, Red Wendigo, Nomad Panda	Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries 4 Chinese APT Groups Identified Targeting Mail Server of Afghan Telecommunications Firm Roshan
RedGolf	China	BRONZE ATLAS, Brass Typhoon, Blackfly, Earth Baku, Red Kelpie, Wicked Panda, Winnti Group, APT41	With KEYPLUG, China's RedGolf Spies On, Steals From Wide Field of Targets
GreenAlpha	Iran	Cobalt Dickens, MABNA Institute, Silent Librarian, TA407	Iran-Linked Threat Actor The MABNA Institute's Operations in 2020 **Note: Graduation to GreenAlpha was determined post-report publication.*
TAG-16	China	FunnyDream, Red Harissa, BRONZE EDGEWOOD	Chinese State-Sponsored Cyber Espionage Activity Supports Expansion of Regional Power and Influence in Southeast Asia
TAG-22	China	Red Dev 10, Earth Baku, Charcoal Typhoon, BRONZE UNIVERSITY, Red Scylla, Aquatic Panda	Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling
TAG-28	China	N/A	China-Linked Group TAG-28 Targets India's "The Times Group" and UIDAI (Aadhaar) Government Agency With Winnti Malware
TAG-38	China	N/A	Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group
TAG-53	Russia	Callisto Group, COLDRIVER, Star Blizzard	Exposing TAG-53's Credential Harvesting Infrastructure Used for Russia-Aligned Espionage Operations
TAG-56	Iran	APT42, Mint Sandstorm	Suspected Iran-Nexus TAG-56 Uses UAE Forum Lure for Credential Theft Against US Think Tank

Table 2: *Public, Insikt Group-named APT groups and TAGs*

About Recorded Future®

Recorded Future is the world’s largest intelligence company. Recorded Future’s cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,600 businesses and government organizations across more than 70 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.