AhnLab

eBook

Threat Actor Naming and Taxonomy

In modern cybersecurity, systematically classifying and naming threat actors is a critical challenge. Accurately understanding and analyzing threat actors is a prerequisite for effectively responding to increasingly sophisticated cyber attacks. Recognizing this need, AhnLab has developed a new threat actor taxonomy and a three-stage framework for managing cyber threat activities.

AhnLab's new approach aims to complement the limitations of existing classification methods while pursuing more flexible and accurate threat analysis. The framework is characterized by its ability to acknowledge and manage information uncertainty, while continuously reflecting changes in threat actors. Additionally, the three-stage cyber threat management framework presents a structured approach for systematically analyzing cyber threats—from individual attacks to long-term campaigns.

In this whitepaper, we explore the importance of naming threat actors and the challenges involved in the process, and introduce AhnLab's threat actor naming taxonomy and management framework for classifying and managing threat intelligence.

1. The Benefits and Difficulties of Naming Threat Actors

Cybersecurity organizations find exchanging threat actor information challenging due to differing situations and interests. Organizations name and share threat actor information based on the data they collect, identify, and analyze from their perspectives. The good news is that the culture of exchanging threat actor information is well-maintained and serves as a cornerstone of today's global cyber threat intelligence.

Naming and managing threat actors offers the following benefits.

- **Ease of Identification and Classification:** Assigning unique names to threat actors allows for easy identification and classification of each actor.
- **Better Communication:** Using specific names enables clearer and more efficient communication when discussing certain threat actors within the security community.
- **Enhancing Threat Intelligence:** Organizations can obtain more detailed and sophisticated threat intelligence by recording and analyzing the characteristics, tactics, techniques, and procedures of each threat actor with a specific name.
- **Designing an Effective Threat Response Strategy:** Understanding the patterns and behaviors of threat actors with specific names makes it easier to develop tailored response strategies for those groups.
- **Consistent Research and Analysis:** Threat researchers can compare and integrate their research findings by using consistent names for the same threat actors.
- **Understanding Threat Severity:** Raising awareness of threat actors with specific names contributes to enhancing awareness of cybersecurity and threat severity within an organization.

However, there are also the following challenges in naming threat actors.

- **Different Level of Visibility:** Each cybersecurity organization has a different level of information and visibility into threat actors.
- **Different Names:** The same threat actors can be assigned multiple names or different threat actors may be referred to by the same name.
- **Spread of Inaccurate Information:** There can be a risk of generating and spreading inaccurate information about threat actors as organizations indiscriminately use names assigned by other organizations without sufficient analysis.

Therefore, cybersecurity organizations must manage threat actor information clearly and make continuous efforts to sustain this practice.

2. AhnLab Threat Actor Naming Taxonomy

To address these challenges, AhnLab has developed a new threat actor naming taxonomy. This taxonomy is designed to complement existing classification methods in the cybersecurity industry while remaining flexible enough to reflect the inherent uncertainty of threat actor information. The taxonomy considers that threat actors exist in various forms, including not only state-sponsored APT groups, but also unattributed APT groups, cybercriminals, ransomware groups, and hacktivists.

AhnLab classifies threat actors into Larva and Arthropod based on their identification stage. This concept is inspired by the transformation process in which larvae that initially appear similar evolve into distinct arthropods over time. It intuitively represents how the true identity of threat actors is gradually revealed as analysis progresses.

2-1. Larva: Unidentified Threat Actor

Larva refers to an unidentified threat actor in the early stage, where attribution information has not yet been confirmed. All threat actors are initially classified and managed as Larva until additional attribution details are identified.

Category	Name	Threat Actor Type
Unidentified Threat Actor	Larva	Unidentified threat actor

Table 1: Unidentified threat actor naming structure

Unidentified threat actors are assigned an ID in the format “Larva-YY###”, where “YY” indicates the year of detection and “###” indicates the order of detection within that year. For example, “Larva-26001” refers to the first unidentified threat actor confirmed in 2026.

Larva is a fixed designation assigned at or above the Incident level within the cyber threat management framework. Once sufficient attribution is obtained through further analysis, the Larva is linked to an Arthropod, representing an identified threat actor.

Figure 1. The process of our new threat actor taxonomy

2-2. Arthropod: Identified Threat Actor

Once sufficient attribution information is obtained for a Larva, it is linked to a corresponding Arthropod based on its association with a specific country or organization. Arthropods are broadly categorized into state-sponsored threat actors and non-state threat actors.

State-Sponsored Threat Actors

State-sponsored threat actors are classified using unique Arthropod names assigned to each country. For example, Ant refers to North Korea–linked threat actors and Cricket refers to China–linked threat actors. If a threat actor exhibits APT characteristics but its sponsoring country is not clearly identified, it is classified as Mantis.

The linkage to an Arthropod is not fixed and may be updated (added, modified, or removed) as new information becomes available. For instance, if a threat actor initially attributed to North Korea is later identified as originating from China, the associated Arthropod can be changed from Ant to Cricket.

Category	Name	Threat Actor Type
State-Sponsored	Mantis	APT – sponsoring nation unconfirmed
	Ant	North Korea suspected
	Cricket	China suspected
	Dragonfly	South Korea suspected
	Butterfly	Vietnam suspected
	Firefly	Pakistan suspected
	Mosquito	India suspected
	Tick	Kazakhstan suspected
	Wasp	Russia suspected
	Spider	United States suspected
	Scorpion	Iran suspected
	Hornet	Israel suspected
	Moth	Lebanon suspected
	Glowworm	UAE suspected
	Earwig	Türkiye suspected

Table 2: State-sponsored threat actor naming structure

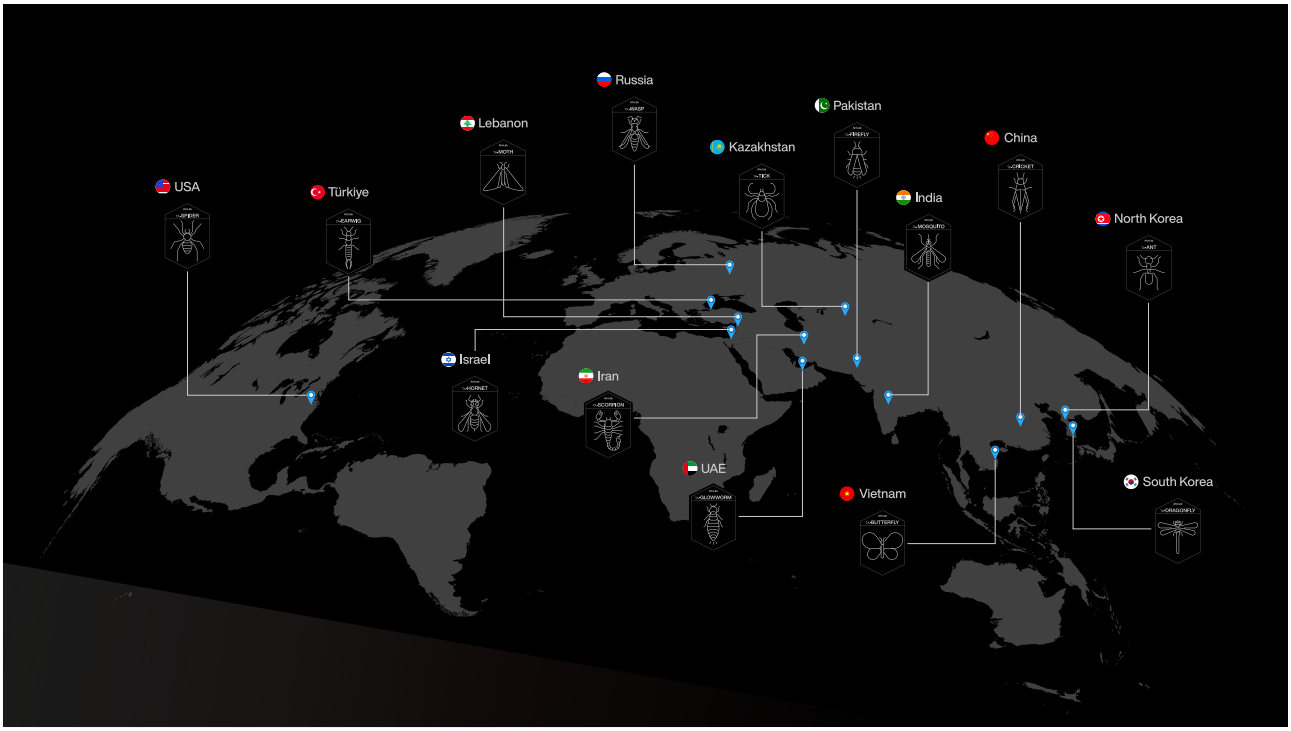

Figure 2: Global distribution of threat actors

Since multiple distinct threat groups can exist within a single nation, AhnLab uses a TA prefix + Modifier + Arthropod naming structure to identify and differentiate them. This approach preserves country-level representation while enabling clear distinction between threat actors operating within the same nation.

AhnLab currently manages certain threat actors under the following names:

- **TA-GiantAnt:** A North Korean-sponsored attack group known as Lazarus
- **TA-RedAnt:** A North Korean-sponsored attack group known as RedEyes
- **TA-ShadowCricket:** A Chinese-sponsored attack group known as ShadowForce

Once a Larva's country of origin is confirmed, it is linked to the corresponding national Arthropod. If further analysis identifies or attributes the actor to a specific known group, it is then linked to that group's designated name.

Non-State Threat Actors

Cybercriminals, ransomware groups, and hacktivists may have ties to specific nations, but for classification purposes, activity type takes precedence over national affiliation. Non-state threat actors are categorized and managed according to their primary objective and attack characteristics, as shown in Table 3.

Category	Name	Threat Actor Type
Non-State Threat Actor	Beetle	Cybercriminal group
	Tarantula	Ransomware group
	Cicada	Hacktivist group

Table 3: Non-state threat actor naming structure

Non-state threat actors are large in number, and some groups use self-assigned names, which makes it difficult to assign unique names to each actor. Therefore, AhnLab applies a different naming rule from that used for state-sponsored threat actors. The naming of non-state threat actors follows the structure: TA prefix + Arthropod + YY + ###.

Example: TA-Beetle-25001

This approach enables systematic classification based on the year and identification number, allowing efficient tracking and management of numerous non-state threat actors.

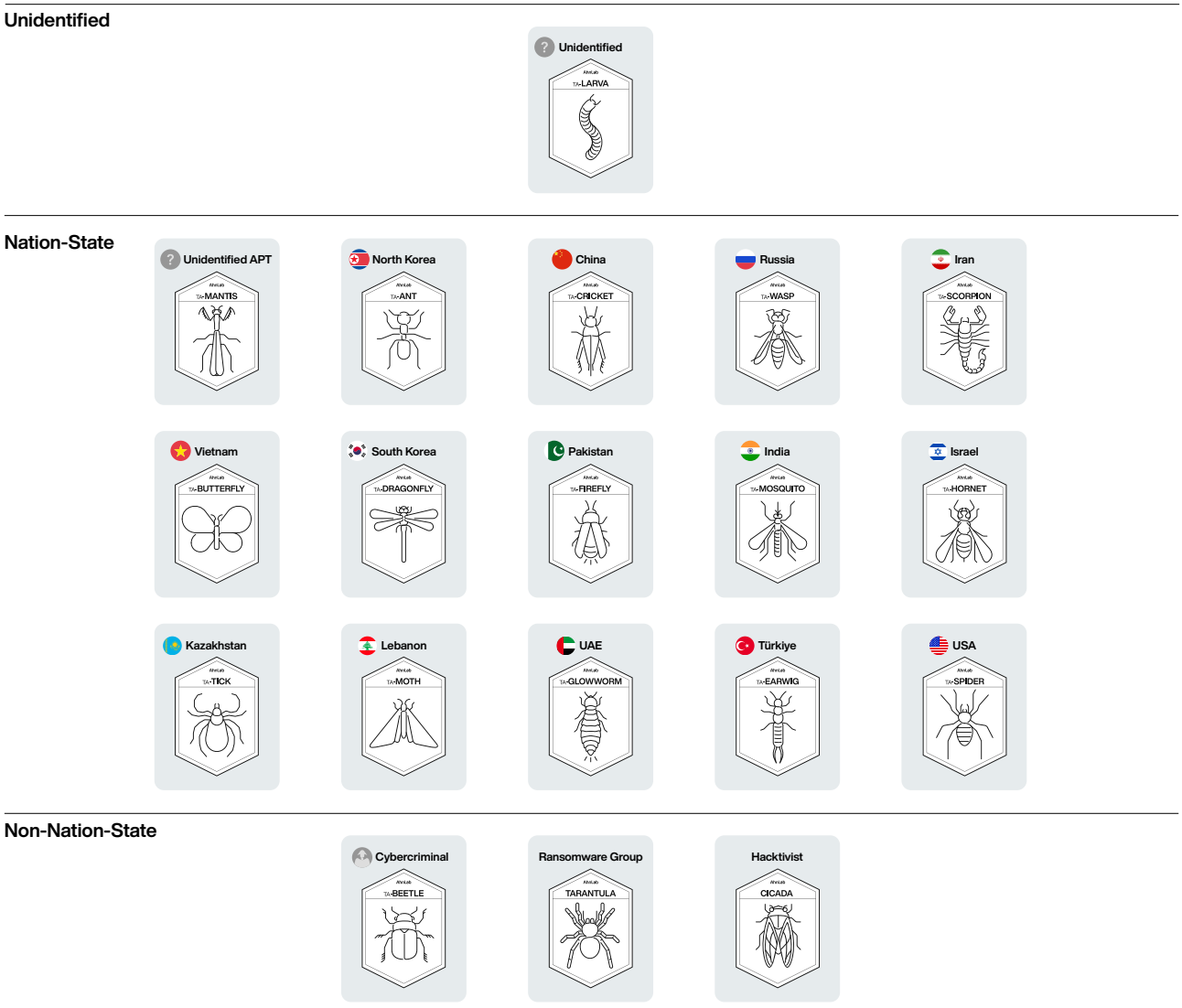

Figure 3: Threat actor icons and names

3. Three-Stage Cyber Threat Management Framework

AhnLab's three-stage cyber threat management framework defines the levels of cyber threat activity as: Incident (individual attack case) → Operation (coordinated attack activity) → Campaign (long-term, organized attack activity). The framework provides a structured approach to managing threat elements at each stage, from individual attacks to long-term campaigns.

Category	Name	Meaning	Description
Stage 1	Incident	Individual attack case	An individual attack case with an identified victim or affected organization
Stage 2	Operation	Attack activity	A unit grouping multiple incidents into a single coordinated attack activity
Stage 3	Campaign	Long-term, organized attack activity	An organized attack activity comprising two or more operations, sustained over a minimum of several months to more than a year

Table 4: Three-stage cyber threat management framework

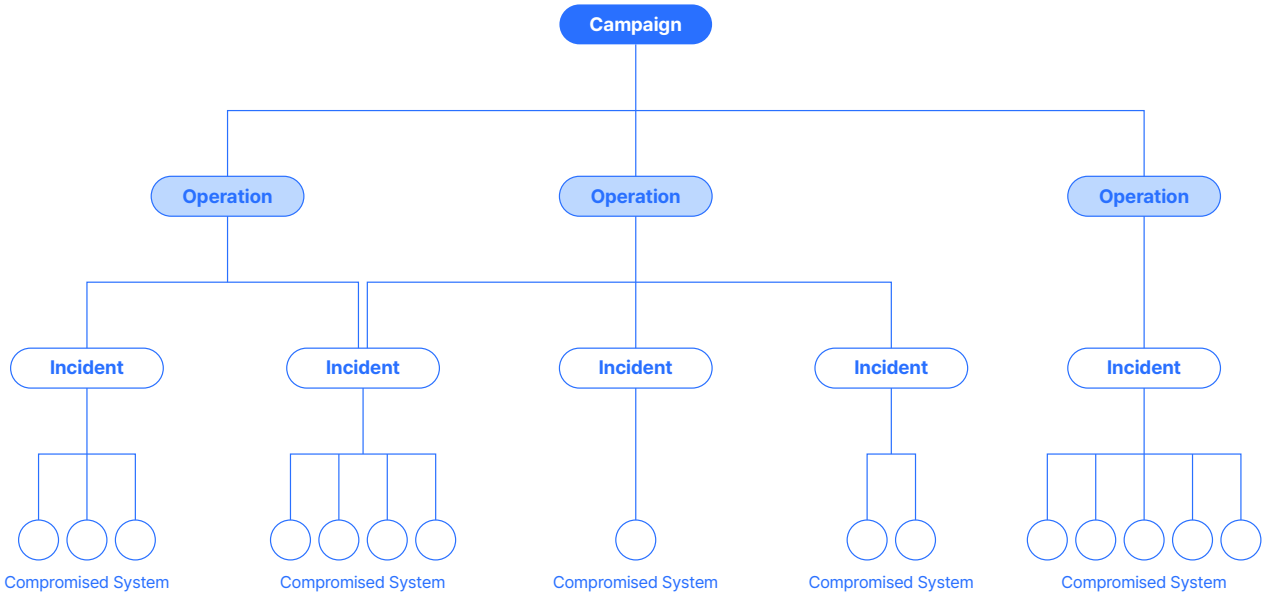

Figure 4: Three-stage cyber threat management framework diagram

Stage 1: Incident

An incident refers to an individual attack with an identified victim or an affected organization. According to our framework, we assign a title “INC-YYMMDD-###“ for each incident. It means “INC (Incident)YYMMDD (Year/Month/Day)-### (Order)”. The focus is on analyzing the characteristics of the event, the extent of the damage, and the techniques leveraged by a threat actor. As a result, organizations can accurately identify the cyber attack case and set the foundation for investigating the operation at a higher level.

Stage 2: Operation

An operation is composed of multiple incidents. The priority in this stage is to comprehensively analyze the characteristics, targets, and techniques to identify connections between multiple incidents. It is also important to understand the patterns and intentions of malicious activities. We assign the name of an operation as “OP-YYMMDD—###”, which follows the same structure as the Incident naming convention.

As for the analysis of the operation, we considered key elements as follows:

- **Goal:** The attacker’s ultimate objective
- **Target:** Attack targets including organizations, industries, and regions
- **Malware:** Types and characteristics of malware used
- **Tool:** Software and program used in the attack
- **Vulnerability:** Exploited vulnerabilities
- **Technique:** Leveraged tactics, techniques and procedures
- **Infrastructure:** Infrastructure (C2, proxy, etc.) used in the attack

By analyzing these factors, we can identify the unique characteristics and patterns of each operation and more accurately track the activities of threat actors. In this stage, it is important to understand that multiple threat actors can be involved in a single operation. Our framework considers that multiple threat actors can collaborate to perform cyber attacks, which is why a larva can be linked to multiple arthropods. In real-world scenarios, it is common for individuals, hired hackers, or cyber threat groups to collaborate toward a common goal.

Stage 3: Campaign

A campaign is a long-term, organized cyber attack activity that lasts for at least several months to over a year. It consists of two or more operations and utilizes various techniques over a long period to achieve long-term goals. We define campaigns after conducting relentless analysis and investigations.

The campaign analysis focuses on uncovering malicious activities comprised of multiple operations to achieve long-term goals rather than a short-term individual cyber-attack. The objective at this stage is to understand the attacker's ultimate strategies and goals. Therefore, we investigate cases where multiple threat actors have cooperated or acted independently over a long period of time.

3-1. The Relationship Between Threat Actors and Their Activities

Let's examine how threat actors and cyber threat activities are related in our framework.

As explained, an operation is a set of incidents. Initially, we consider a larva (unidentified threat actor) to have carried out the operation. Once the identity of the larva is confirmed after further investigation, it is linked to an arthropod that matches its characteristics. If a follow-up analysis reveals that the actual entity behind the operation is different from what was defined or if another threat actor was involved, the arthropod can be modified or added.

For example, if a threat actor initially named larva was identified as an individual threat actor, we will name it "TA-FireBeetle". However, if further research reveals that a threat actor is actually suspected to be sponsored by Russia, we will change the name to "TA-BigWasp".

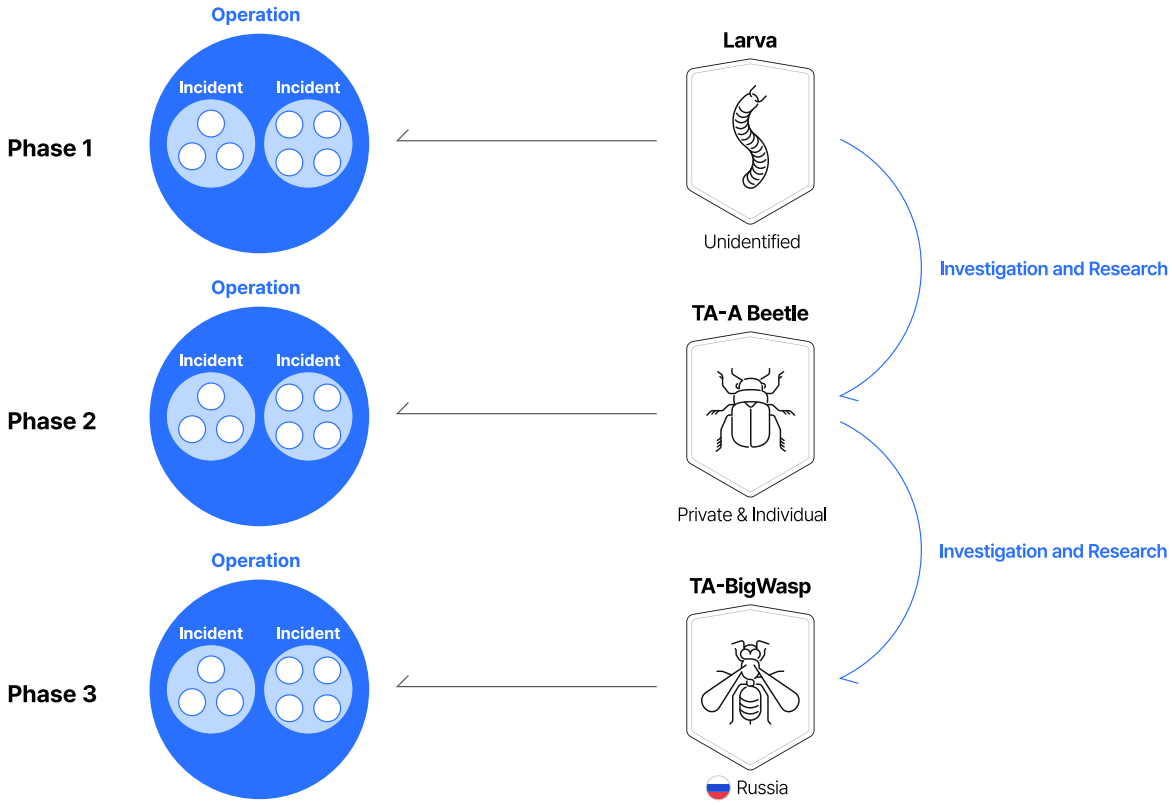

Figure 5: The relationship between operation and threat actor

In addition, a single threat actor may carry out multiple operations. In this case, we initially see each operation as being carried out by individual larvae. However, if the investigation reveals that operations are the work of the same threat actor, these larvae can be linked to the same arthropod. For example, if a single threat actor group suspected to be sponsored by North Korea, simultaneously conducted cyber espionage and pursued financial gain through ransomware, the structure would be as shown in Figure 6.

In addition, a single threat actor may carry out multiple operations. In this case, we initially see each operation as being carried out by individual larvae. However, if the investigation reveals that operations are the work of the same threat actor, these larvae can be linked to the same arthropod. For example, if a single threat actor group suspected to be sponsored by North Korea, simultaneously conducted cyber espionage and pursued financial gain through ransomware, the structure would be as shown in Figure 6.

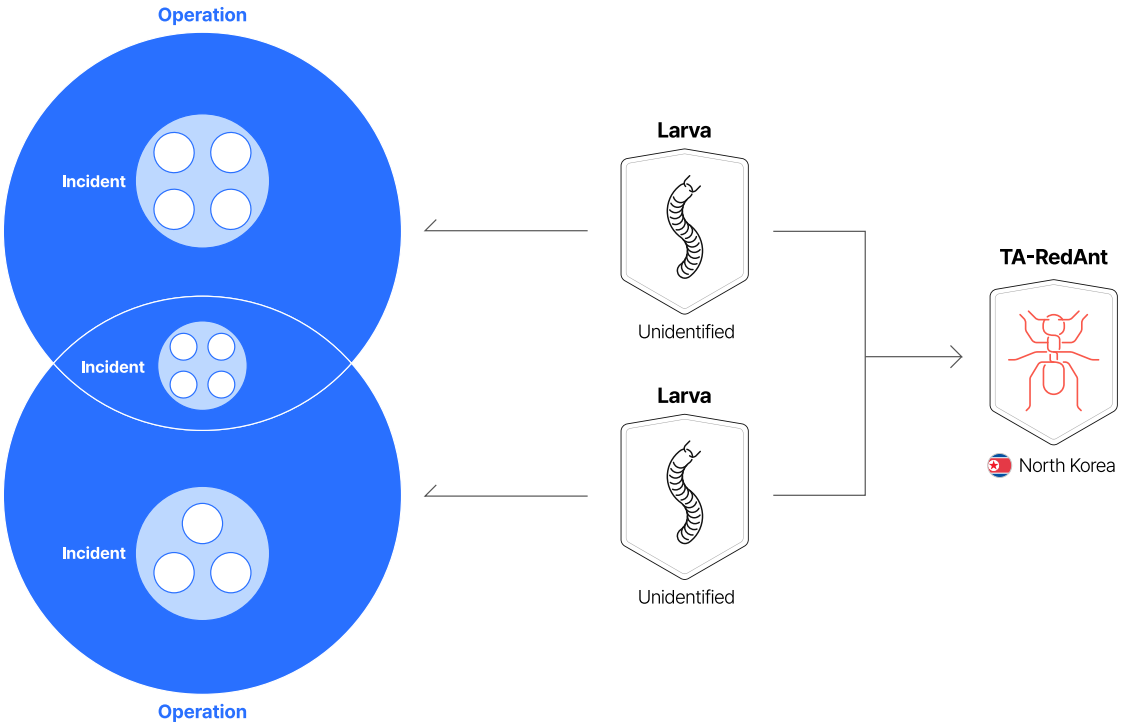

Figure 6: The structure of a single threat actor performing multiple operations

In contrast, there are cases where multiple threat actors jointly participate in a single operation. Recently, there has been increasing cooperation between malware developers, cybercriminal organizations, and state-sponsored threat actors to achieve a common objective. If we apply this to our framework, there will be multiple arthropods performing a single operation.

Figure 7 shows a case where an operation initially identified as the work of a single threat actor was later revealed to be an attack by two different suspected North Korean-sponsored threat actors upon further investigation. Accordingly, considering the characteristics of the threat actors, we give names "TA-RedAnt" and "TA-BlueAnt", while also leaving open the possibility of another threat actor being involved.

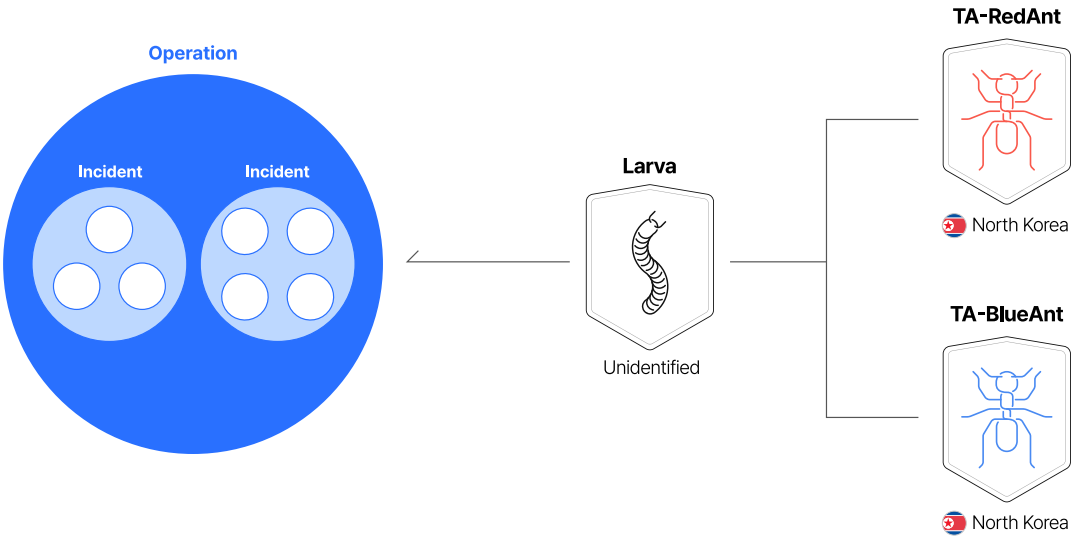

Figure 7: The structure of multiple threat actors performing a single operation

4. Why Our Framework Is Unique

As introduced, we designed a new threat actor taxonomy and a three-stage framework to manage their malicious activities. The traits below highlight how our framework is unique.

- **Accepting Information Uncertainty:** We initially manage threat actors who have conducted cyber-attacks as larva because their identities are not confirmed. Once we obtain additional information and the identity becomes clear, we link the larva to the corresponding arthropod.
- **Preventing Information Distortion:** The framework assigns confidence and weight to information to sustain its reliability.
- **Reflecting Changes in Threat Actors:** We continuously track changes in threat actors through flexible connections between larva and arthropod.
- **Considering the Involvement of Multiple Threat Actors:** The framework accounts for the possibility that multiple threat actors may be involved simultaneously in a single operation or campaign.
- **Application of Threat Intelligence Framework:** We built the framework by referring to renowned CTI frameworks such as MITRE ATT&CK, Lockheed Martin Cyber Kill Chain, and the Diamond Model of Intrusion Analysis.

5. Conclusion

We developed the threat actor taxonomy and three-stage cyber threat activity framework based on values including accuracy, flexibility, and reliability. This helps organizations understand the complexity of cyber threats and respond quickly to the ever-changing cybersecurity environment. We expect our framework to allow for close tracking of threat actor activities and the development of more effective response strategies. In the future, we will continuously improve and develop the framework to provide more sophisticated and reliable threat intelligence.

AhnLab

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com / en global.sales@ahnlab.com