AhnLab

eBook

Threat Actor Naming and Taxonomy

In modern cybersecurity landscape, it is critical to systematically name and classify threat actors because organizations must accurately understand and analyze them to combat increasingly sophisticated cyber attacks. Therefore, AhnLab has developed a new threat actor taxonomy and a four-stage framework to manage their malicious activities.

Our new approach aims to complement the limitations of existing taxonomy while pursuing more flexible and accurate threat analysis. The newly designed framework acknowledges and manages information uncertainty while continuously reflecting changes in threat actors. Additionally, it presents a framework for systematically analyzing cyber threats, from individual attacks to long-term campaigns, through four-stage malicious activities.

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. Our Cyber Threat Management Framework

AhnLab has developed a new cyber threat management framework to address the challenges facing the cybersecurity community. Our framework consists mainly of a "threat actor taxonomy" and a "four-stage framework for cyber threat activities." Before we explore the framework, let us clarify the terms and definitions used to describe it.

Type	Name	Description
Threat Actor Taxonomy	Larva	Unidentified threat actor
	Arthropod	Identified threat actor in general
	Ant	Identified threat actor – North Korea suspected
	Cricket	Identified threat actor – China suspected
	Wasp	Identified threat actor – Russia suspected
	Scorpion	Identified threat actor – Iran suspected
	Butterfly	Identified threat actor – Vietnam suspected
	Dragonfly	Identified threat actor – South Korea suspected
	Firefly	Identified threat actor – Pakistan suspected
	Mosquito	Identified threat actor – India suspected
	Beetle	Identified threat actor – individual
Four-Stage Threat Activities	Compromised System	Systems compromised due to a cyber attack
	Incident	Each breach case with identified victim or affected organization
	Operation	A unit composed of multiple incidents as a single cyber attack activity
	Campaign	A cyber attack activity composed of two or more operations that lasted at least several months to over a year

2-1. New Threat Actor Taxonomy

We designed the new threat actor taxonomy to complement existing methods used in the cybersecurity industry and effectively manage threat actors. We acknowledge the uncertainty of information and consider the fact that threat actors are not limited to a single group; they can exist in various forms, such as individuals or hired by others.

From a broad perspective, we classify threat actors as "larva" (unidentified threat actors) and "arthropod" (identified threat actors).

A. Larva: Unidentified Threat Actor

Larva refers to attackers who have yet to be identified. All threat actors are initially managed as larva until additional information is discovered.

Threat actors classified as larva are documented in the "Larva-YY###“ format, which is interpreted as “Larva-YY (year)### (order). For instance, the threat actor "Larva-24009" refers to a threat actor unidentified and the ninth confirmed in 2024.

We name the threat actor as larva when the attacker is not clearly identified in the “operation" phase, the third stage of the “four-stage cyber threat activities“, which will be explained later. Upon additional research and analysis, the larva is linked to an arthropod, which signifies an identified threat actor.

To be more straightforward, if a threat actor in the larva state is suspected to be sponsored by North Korea upon further investigation, it is linked to an “ant." Larva is the fixed initial name for the entity that performed the operation, but the linked arthropod can change based on the information found.

Figure 1. The process of our new threat actor taxonomy

B. Arthropod: Identified Threat Actor

Once sufficient information about the larva is obtained, it is linked to the corresponding arthropod based on its connection to a specific country or organization. We have come up with the taxonomy from the fact that all larvae look similar, but they transform into various types of arthropods over time.

According to our naming convention, a threat actor suspected of being sponsored by North Korea is named “ant,” and one related to China is named “Cricket.” In addition, Russia is designated as a “wasp”, Iran as a “scorpion”, and Vietnam as a “butterfly” with each country defining threat actors as unique arthropods.

The connection to Arthropod is flexible and can be modified (added, changed, or deleted) at any time when new information is found. If a cybercriminal group initially identified as a North Korean threat actor is later revealed to be a Chinese attacker after further analysis, the arthropod can change from ant to cricket.

Arthropods cover not only state-sponsored threat groups engaged in geopolitical conflict or national interest but also cybercriminal organizations seeking financial gain, and individual or hired threat actors. Also, we name financially motivated private organizations or individual threat actors as a “beetle.”

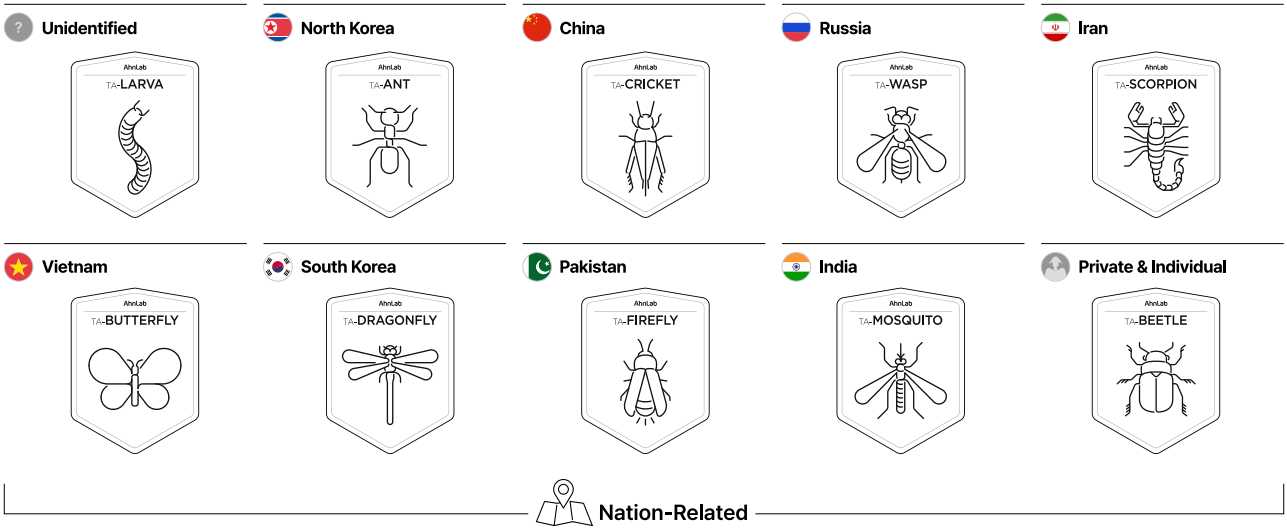

Figure 2. The threat actor names and icons

Figure 3. A worldwide distribution of threat actors

2-2. Four-Stage Cyber Threat Activity Framework

Our four-stage cyber threat activity framework defines the level of cyber threat activities as follows: compromised system > incident > operation > campaign. The framework analyzes and defines various elements of cyber threats at each stage to enable organizations to properly manage them from a single attack to long-term campaigns.

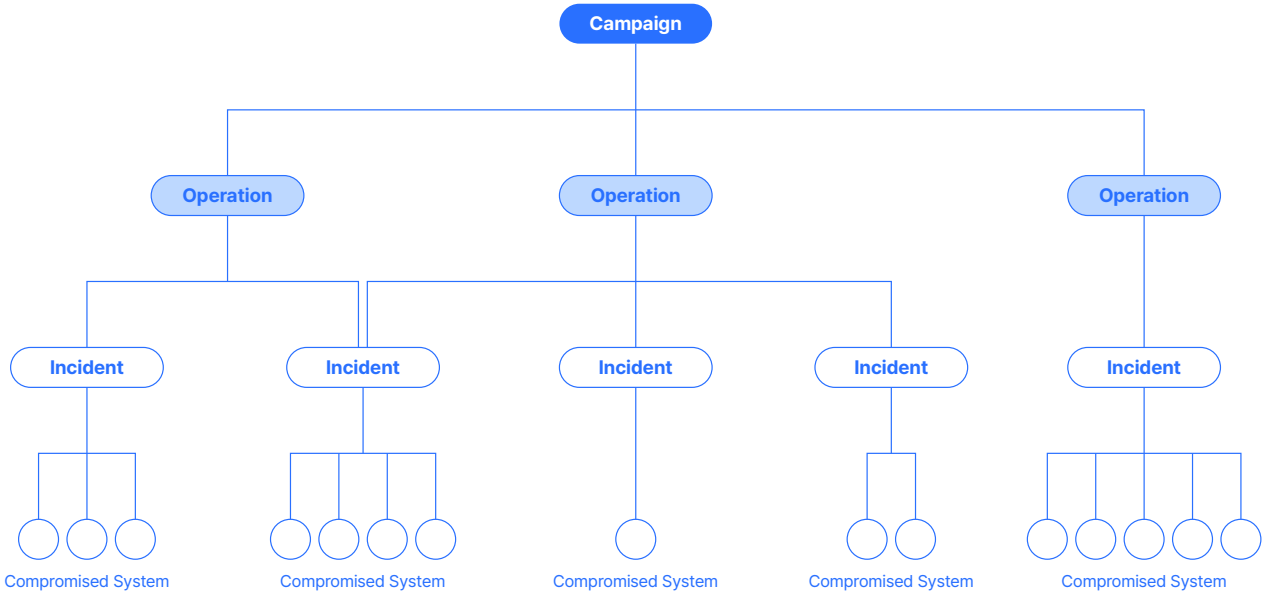

Figure 4. The structure of the four-stage cyber threat activity framework

Stage 1: Compromised System

A compromised system represents breached systems from a cyber attack and it is the most basic unit of cyber threat analysis. The system encompasses assets such as PCs, servers, and physical devices. In this stage, organizations perform digital forensics on elements of cyber attack, including malware, vulnerabilities, and other tools. This information serves as foundational data for subsequent analysis.

Stage 2: 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 3: 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 4: 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.

2-3. 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".

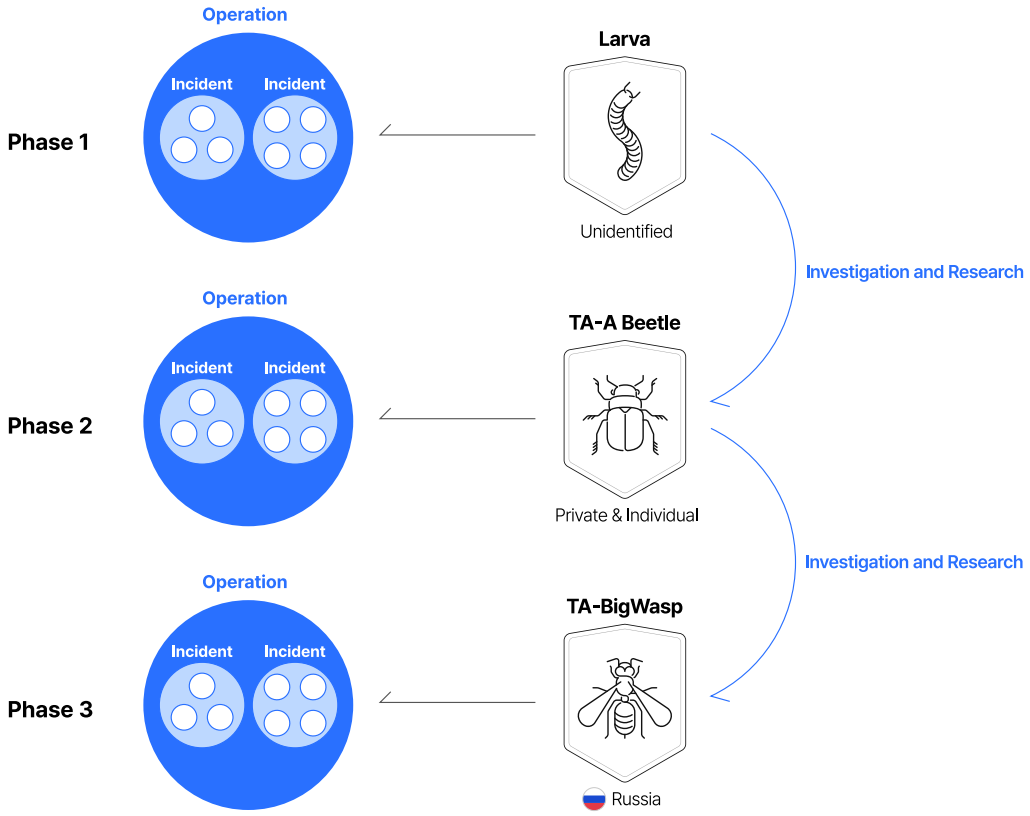

Figure 5: The relationship between operation and threat actor

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.

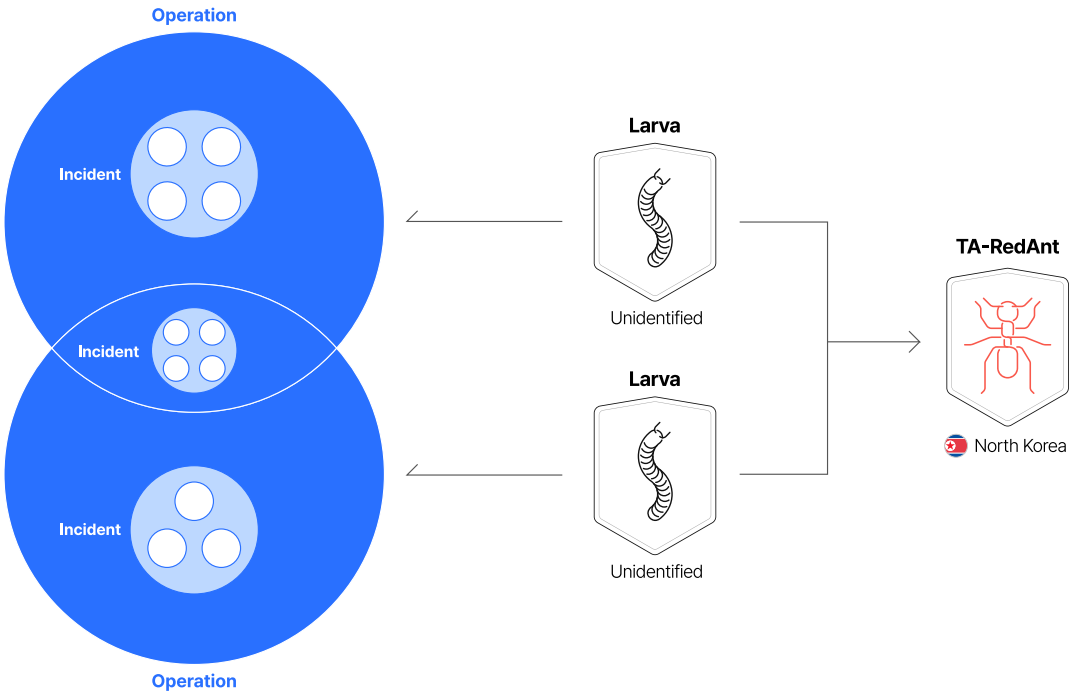

Figure 6: The structure of a single threat actor performing multiple operations

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.

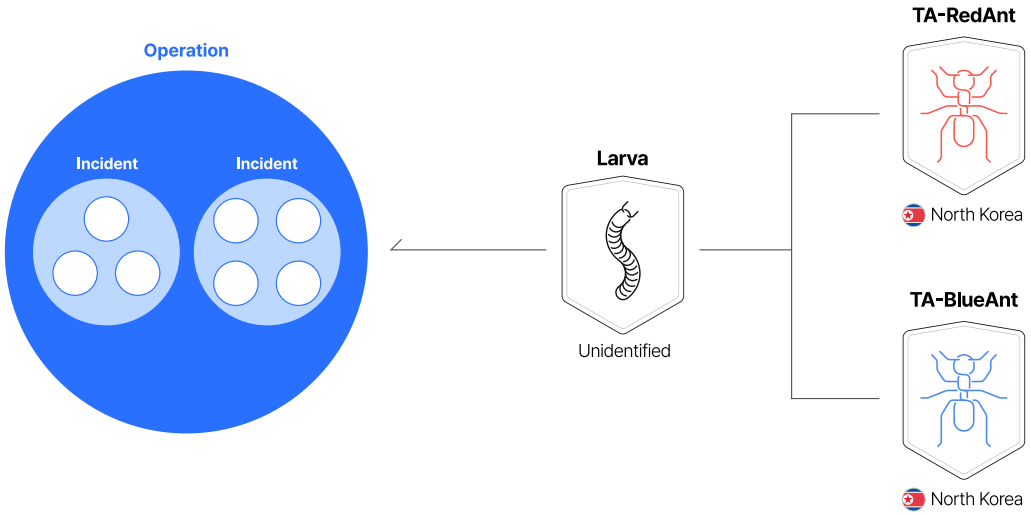

Figure 7. The structure of multiple threat actors performing a single operation

2-4. Why Our Framework Is Unique

As introduced, we designed a new threat actor taxonomy and a four-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.

3. Conclusion

We developed the threat actor taxonomy and four-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