

eBook

위협 행위자 명명법 및 위협 행위 관리 체계

위협 행위자를 체계적으로 분류하고 명명하는 것은 현대 사이버 보안에서 매우 중요한 과제다. 고도화되는 사이버 공격에 효과적으로 대응하기 위해서는 위협 행위자에 대한 정확한 이해와 분석이 선행되어야 하기 때문이다. 안랩은 이러한 필요성을 인식하고 위협 행위자에 대한 새로운 분류 및 명명법과 위협 행위를 3단계로 관리하는 체계를 개발했다.

안랩의 새로운 접근법은 기존 분류 체계의 한계를 보완하는 동시에 더 유연하고 정확한 위협 분석을 목표로 한다. 본 체계의 특징은 정보의 불확실성을 인정하고 이를 관리하는 방식과 위협 행위자의 변화를 지속적으로 반영할 수 있도록 하는 것이다. 또한, 3단계 위협 행위 관리 체계를 통해 개별 공격부터 장기적인 캠페인까지 체계적으로 분석할 수 있는 프레임워크를 제시한다.

이번 글에서는 위협 행위자 명명의 중요성과 그 과정에서 발생하는 도전 과제를 살펴보고, 안랩의 위협 행위자 분류 체계와 명명법, 그리고 위협 정보를 관리하고 분류하는 구체적인 방식까지 소개한다.

1. 위협 행위자 명명의 중요성과 도전 과제

사이버 보안 조직 간 위협 행위자 정보 교류는 각 조직의 상황과 이해관계가 다르기 때문에 쉽지 않은 과제다. 조직들은 각자 관점에서 수집, 파악 및 분석한 정보를 기반으로 위협 행위자를 명명하고 정보를 공개해 교류하고 있으며, 다행히 이처럼 위협 행위자 정보를 교류하는 문화는 잘 유지되어 오늘날 글로벌 사이버 위협 인텔리전스의 초석 역할을 하고 있다.

위협 행위자를 명명해 관리하면 다음과 같은 이점이 있다.

- **식별 및 분류 용이성:** 위협 행위자에게 고유한 이름을 부여해 각 행위자를 쉽게 식별 및 분류할 수 있다.
- **정보 공유 및 커뮤니케이션 향상:** 보안 커뮤니티 내에서 특정 위협 행위자에 대해 논의할 때, 고유 명칭을 사용하면 더 명확하고 효율적인 의사소통이 가능하다.
- **위협 인텔리전스 강화:** 각 위협 행위자의 특성, 전술, 기술 등을 이름과 연관 지어 기록하고 분석해 보다 구체적이고 정교한 위협 인텔리전스를 구축할 수 있다.
- **효과적인 위협 대응 전략 수립:** 특정 명칭으로 식별된 위협 행위자의 패턴과 행동을 파악해 해당 그룹에 대한 맞춤형 대응 전략 수립이 수월해진다.
- **연구 및 분석의 일관성 유지:** 보안 연구자들이 동일한 위협 행위자에 대해 일관된 이름을 사용함으로써, 연구 결과 비교와 통합이 용이해진다.
- **위협의 심각성에 대한 인식 제고:** 특정 이름을 가진 위협 행위자의 존재감과 위험성에 대한 인식을 높여 조직 내 보안 의식 향상에 기여한다.

다만, 위협 행위자 명명에는 다음과 같은 도전 과제도 있다.

- **정보 가시성 차이:** 각 사이버 보안 조직이 위협 행위자에 대해 확보할 수 있는 정보와 가시성이 제한적이며, 조직별로 차이도 존재한다.
- **명칭 중복:** 동일한 위협 행위자에 여러 이름이 부여되거나, 여러 위협 행위자가 동일한 이름으로 불리는 경우가 발생할 수 있다.
- **부정확한 정보 전파 위험:** 충분한 분석 없이 타 조직에서 부여한 이름을 무분별하게 사용하면, 위협 행위자에 대한 부정확한 정보가 생성되고 전파될 위험이 있다.

따라서, 사이버 보안 조직은 정보 교류의 중요성을 인식하고 위협 행위자에 대한 정보를 명확하게 관리해 제공해야 하며, 이를 지속하기 위해 노력해야 한다.

2. 안랩의 위협 행위자 명명법

안랩은 이와 같은 도전 과제를 해결하기 위해 새로운 위협 행위자 명명법을 개발했다. 이 명명법은 기존 사이버 보안 업계의 분류 방식을 보완하고, 위협 행위자에 대한 정보의 불확실성을 반영해 유연하게 관리될 수 있도록 설계했다. 위협 행위자는 국가 배후의 APT 그룹뿐만 아니라, 국가가 식별되지 않은 APT 그룹, 사이버범죄자, 랜섬웨어 그룹, 해티비스트 등 다양한 형태로 존재할 수 있다는 점을 고려해 체계를 구성했다.

안랩의 명명법은 위협 행위자를 식별 단계에 따라 Larva(애벌레)와 Arthropod(절지동물)로 구분한다. 이는 초기에는 서로 유사해 보이는 애벌레가 시간이 지나며 서로 다른 절지동물로 변화하는 과정에서 착안한 개념으로, 분석이 진행될수록 위협 행위자의 실체가 점진적으로 드러나는 과정을 직관적으로 표현한다.

2-1. Larva(애벌레): 식별되지 않은 위협 행위자

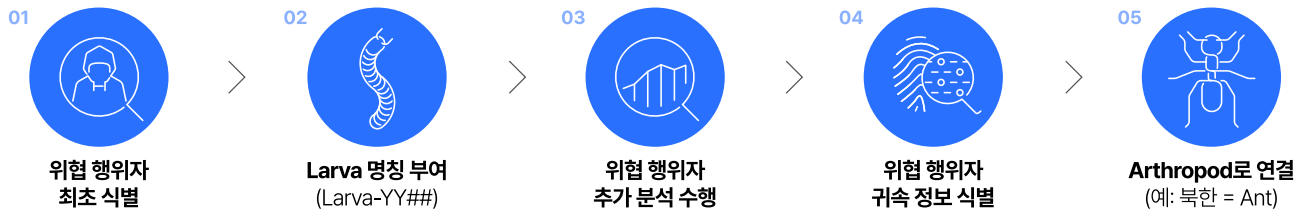
Larva는 귀속 정보가 확인되지 않은 초기 단계의 신원 미상 위협 행위자를 의미한다. 모든 위협 행위자는 최초 식별 시 추가적인 귀속 정보가 확인될 때까지 Larva 단계로 분류되어 관리된다.

구분	명칭	명칭 한글 의미	위협 행위자 유형
미식별 위협 행위자	Larva	애벌레	식별되지 않은 위협 행위자

[표 1] 식별되지 않은 위협 행위자 명명법

미식별 위협 행위자에는 'Larva-YY####' 형식의 식별 번호가 부여된다. 여기서 'YY'는 탐지 연도, '####'는 해당 연도 내 탐지 순서를 의미한다. 예를 들어 'Larva-26001'은 2026년 첫 번째로 확인된 미식별 위협 행위자다.

Larva는 후술할 '3단계 위협 행위 관리 체계' 중 1단계에 해당하는 'Incident(공격 활동)' 단위 이상에서의 위협 행위자에 부여되는 고정 명칭이다. 이후 추가적인 분석 및 정보 확보를 통해 특정 위협 그룹으로의 귀속이 확인되면, Larva는 식별된 위협 행위자를 의미하는 Arthropod 명칭으로 연결된다.



[그림 1] 안랩의 위협 행위자 명칭 부여 과정

2-2. Arthropod(절지동물): 식별된 위협 행위자

Larva에 대한 충분한 귀속 정보가 확보되면, 특정 국가 또는 조직과의 연관성을 기준으로 해당하는 Arthropod의 명칭으로 연결한다. Arthropod는 크게 국가 배후 위협 행위자와 비국가 위협 행위자로 구분된다.

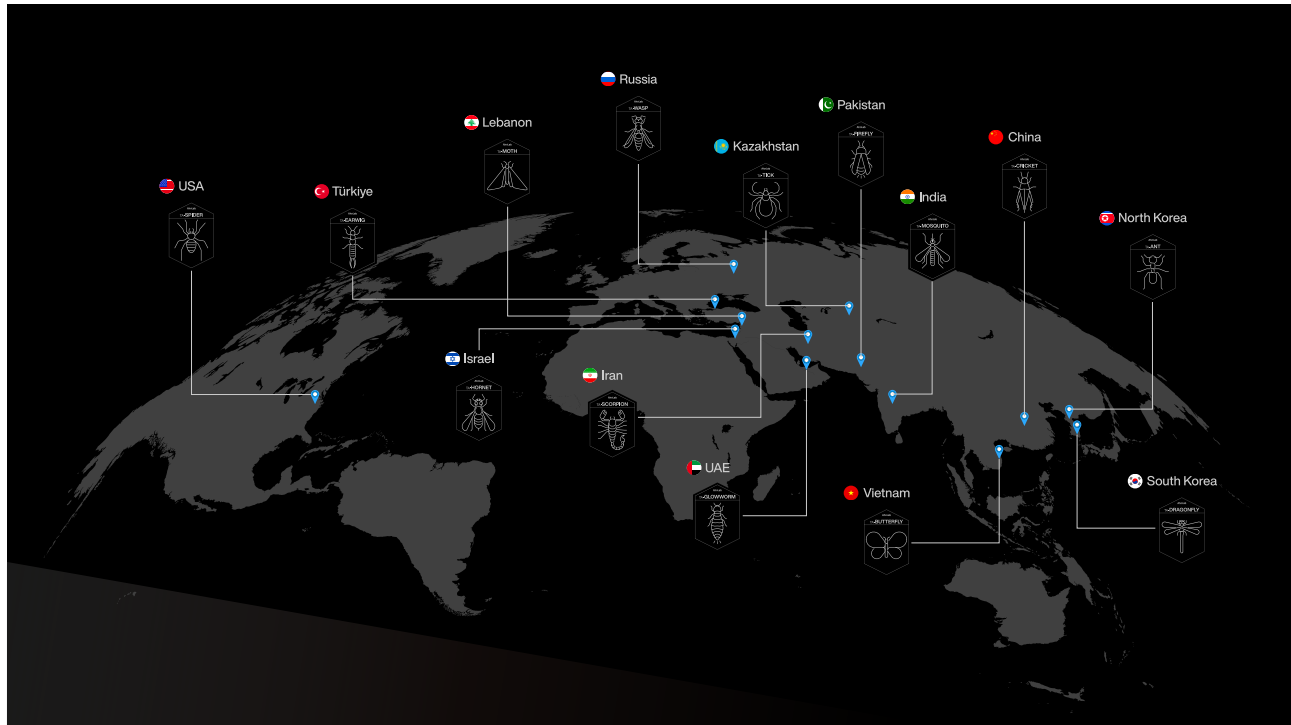
A. 국가배후 위협 행위자

국가 배후 위협 행위자는 국가별로 고유한 Arthropod 명칭을 사용해 구분한다. 예를 들어, 북한 배후로 추정되는 위협 행위는 Ant(개미), 중국 관련 위협 행위자는 Cricket(귀뚜라미)로 명명한다. 한편 고도화된 지속적 위협(APT)의 특성을 보이지만 배후 국가가 명확히 식별되지 않은 경우에는 Mantis(사마귀)로 연결된다.

Arthropod로의 연결은 고정되지 않으며, 새로운 정보가 확인되면 언제든지 수정(추가, 변경, 삭제)될 수 있다. 예를 들어 북한 위협 행위자로 식별됐던 공격 그룹이 추가 분석을 통해 중국 위협 행위자로 밝혀지면, Larva와 연결된 Arthropod도 Ant에서 Cricket으로 변경된다.

구분	명칭	명칭 한글 의미	위협 행위자 유형
국가 배후 위협 행위자	Mantis	사마귀	배후 국가 미확인 APT
	Ant	개미	북한 배후 추정
	Cricket	귀뚜라미	중국 배후 추정
	Dragonfly	잠자리	한국 배후 추정
	Butterfly	나비	베트남 배후 추정
	Firefly	반딧불이	파키스탄 배후 추정
	Mosquito	모기	인도 배후 추정
	Tick	진드기	카자흐스탄 배후 추정
	Wasp	말벌	러시아 배후 추정
	Spider	거미	미국 배후 추정
	Scorpion	전갈	이란 배후 추정
	Hornet	장수말벌	이스라엘 배후 추정
	Moth	나방	레바논 배후 추정
	Glowworm	개똥벌레	아랍에미리트 배후 추정
	Earwig	집게벌레	튀르키예 배후 추정

[표 2] 국가 배후 위협 행위자 대표 명칭



[그림 2] 전 세계 위협 행위자 분포

국가 배후 위협 행위자는 단일 그룹이 아니라 다수로 존재할 수 있기 때문에, 이를 식별·구분하기 위해 TA 접두어 + Modifier + Arthropod 구조의 명명 체계를 사용한다. 이러한 방식은 국가 단위의 대표성을 유지하면서도, 동일 국가 내 다양한 위협 행위자의 특성과 차이를 명확히 식별할 수 있도록 설계됐다.

안랩은 일부 위협 행위자에 다음과 같이 이름을 부여해 관리하고 있다.

- **TA-GiantAnt** : Lazarus로 알려진 북한 배후 공격 그룹
- **TA-RedAnt** : RedEyes로 알려진 북한 배후 공격 그룹
- **TA-ShadowCricket** : ShadowForce로 알려진 중국 배후 공격 그룹

Larva의 배후 국가 정보가 확인되면 해당 국가의 위협 행위자 명칭으로 연결되고, 추가 분석을 통해 특정 공격 그룹까지 식별되거나 지정되면 해당 그룹명으로 연결된다.

B. 비국가 위협 행위자

사이버범죄자, 랜섬웨어 그룹, 해커비스트 역시 특정 국가와 연관될 수 있지만, 이들의 분류에서는 국가적 연계성보다 행위 유형이 더 중요한 기준이 된다. 비국가 위협 행위자는 [표 3]와 같이 주요 활동 목적과 공격 특성에 기반해 유형별로 구분하여 관리한다.

구분	명칭	명칭 한글 의미	위협 행위자 유형
비국가 위협 행위자	Beetle	딱정벌레	사이버 범죄 조직
	Tarantula	타란툴라	랜섬웨어 그룹
	Cicada	매미	해커비스트 그룹

[표 3] 비국가 위협 행위자 명칭

비국가 위협 행위자는 그 수가 방대하고, 일부는 스스로 명칭을 사용하기도 하므로 개별 고유 이름을 부여하는 데 한계가 있다. 따라서 국가 배후 위협 행위자와는 다른 명명 규칙을 적용한다.

비국가 위협 행위자의 명명은 TA 접두어 + Arthropod + YY + ### 구조를 따른다.

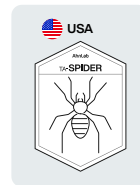
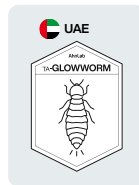
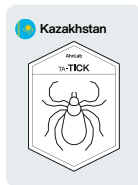
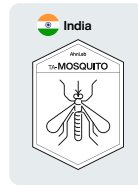
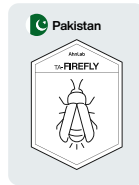
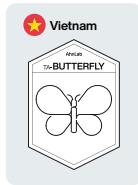
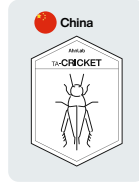
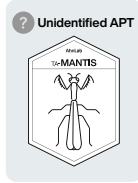
예) TA-Beetle-25001

이 방식은 연도(YY)와 식별 번호(###) 기반의 체계적 분류를 가능하게 하여, 다수의 비국가 위협 행위자를 효율적으로 추적·관리할 수 있도록 한다.

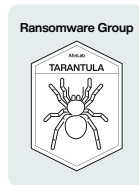
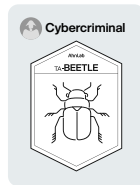
Unidentified



Nation-State



Non-Nation-State



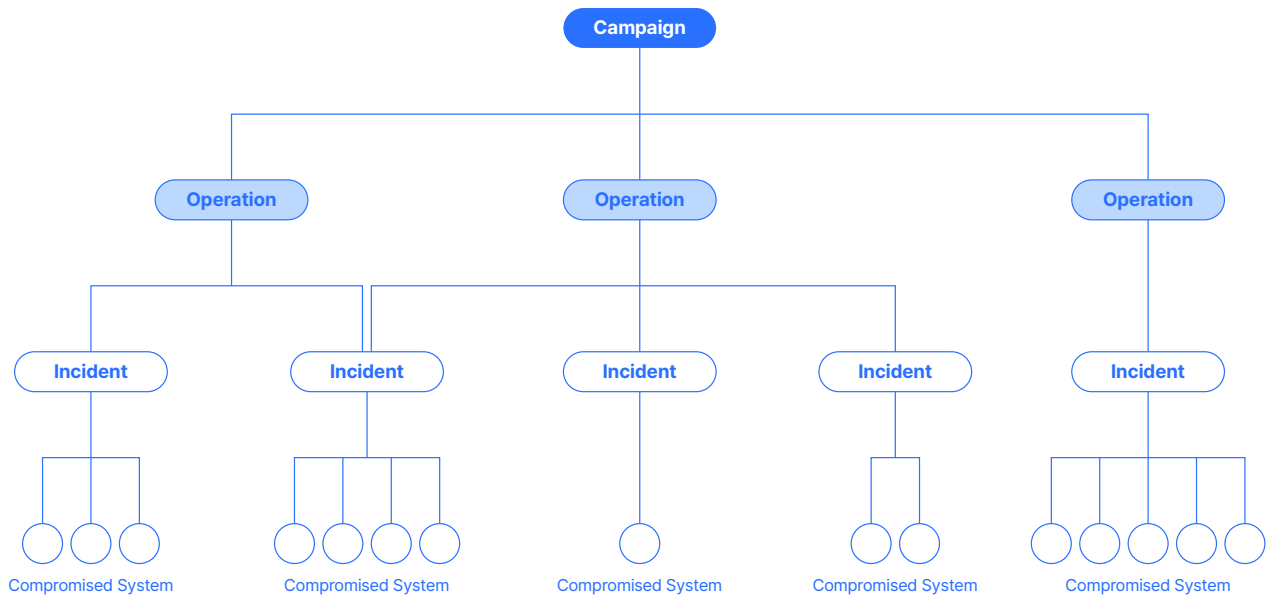
[그림 3] 위협 행위자 아이콘 및 명칭

3. 3단계 위협 행위 관리 체계

안랩이 정의한 3단계 위협 행위 관리 체계는 사이버 위협의 레벨을 기준으로 'Incident(개별 공격 사건) → Operation(공격 활동) → Campaign(장기적이고 조직적인 공격 활동)'으로 구성된다. 각 단계에서 다양한 위협 요소를 종합적으로 관리하며, 개별 공격부터 장기적인 캠페인까지 체계적으로 분석할 수 있는 프레임워크를 제시한다.

구분	명칭	명칭 한글 의미	설명
1단계	Incident	개별 공격 사건	피해자나 피해 조직이 확인된 개별 공격 사건
2단계	Operation	공격 활동	복수의 Incident를 하나의 공격 활동으로 구성한 단위
3단계	Campaign	장기적이고 조직적인 공격 활동	두 개 이상의 Operation으로 구성된 최소 수개월에서 1년 이상 지속된 공격 활동

[표 4] 3단계 위협 행위 관리 체계



[그림 4] 3단계 위협 행위 관리 체계 관계도

#1. Incident: 개별 공격 사건

Incident는 피해자나 피해 조직이 확인된 개별 공격 사건을 의미한다. 각 Incident는 고유 관리 번호 'INC-YYMMDD-###'를 부여하는데, 의미를 풀어보면 'INC(침해 사건)-YYMMDD(연월일)-###(순서)'로 해석된다. Incident 단계에서는 사건의 특성, 피해 범위, 사용된 기술 등에 관한 분석을 진행해 해당 사건이 어떤 특징을 갖는지 파악하는 데 중점을 둔다. 이를 통해, 단일 공격 사건을 정확하게 식별하고 상위 단계인 Operation을 구성하는 기초를 마련할 수 있다.

#2. Operation: 공격 활동

Operation은 복수의 Incident를 하나의 공격 활동으로 구성한 단위다. 공격의 특징, 목표, 사용된 기술 등을 종합적으로 분석해 여러 사건 간 연관성을 파악하고 공격 활동의 패턴과 의도를 이해하는 데 중점을 둔다. Operation의 명칭은 'OP-YYMMDD-###'로 부여되는데 구조는 Incident의 명칭 구조와 동일하다.

Operation 분석에는 다양한 요소들을 고려하는데, 주요 항목들은 다음과 같다.

- **Goal:** 공격자의 궁극적인 목표
- **Target:** 공격 대상 (조직, 산업 분야, 지역 등)
- **Malware:** 사용된 악성코드 종류와 특징
- **Tool:** 공격에 활용된 도구와 소프트웨어
- **Vulnerability:** 악용된 취약점
- **Technique:** 공격 기법과 전술
- **Infrastructure:** 공격에 사용된 인프라 (C&C 서버, 프록시 등)

이처럼 다양한 요소들을 종합적으로 분석함으로써, 각 Operation의 고유한 특성과 패턴을 식별하고 위협 행위자의 활동을 더욱 정확하게 추적할 수 있다.

위협 행위자 분석 관점에서 보면, 분석 초기 단계에는 Operation이 식별되지 않은 위협 행위자인 Larva에 의해 행해진 것으로 본다. 분석을 시작한 시점에는 위협 행위자의 귀속 정보가 명확하지 않기 때문에, Larva로 명명해 관리하여 정보의 불확실성에 대처하는 것이다. 이후, 보다 확실한 정보가 추가되면 위협 행위자를 Arthropod로 연결할 수 있다.

Operation 단계에서 중요한 점은 하나의 공격 활동에 여러 위협 행위자가 관여할 수 있다는 사실이다. 본 체계에서는 사이버 공격이 여러 위협 행위자 간 협력을 기반으로 이루어질 수 있음을 고려해 Larva에 여러 Arthropod가 연결될 수 있다. 실제 공격 사례들을 봐도 개인, 고용된 위협 행위자 혹은 위협 그룹들이 공통된 목표를 갖고 협력하는 경우가 많다.

#3. Campaign: 장기적이고 조직적인 공격 활동

Campaign은 장기적이고 조직적인 공격 활동으로 최소 수개월에서 1년 이상 지속된 공격 활동을 포함한다. Campaign은 두 개 이상의 Operation으로 구성되며, 장기적 목표를 달성하기 위해 오랜 기간에 걸쳐 여러 가지 공격 기법들을 활용한다. 이러한 Campaign에 대해서도 장기적인 분석 후 명칭을 정의한다.

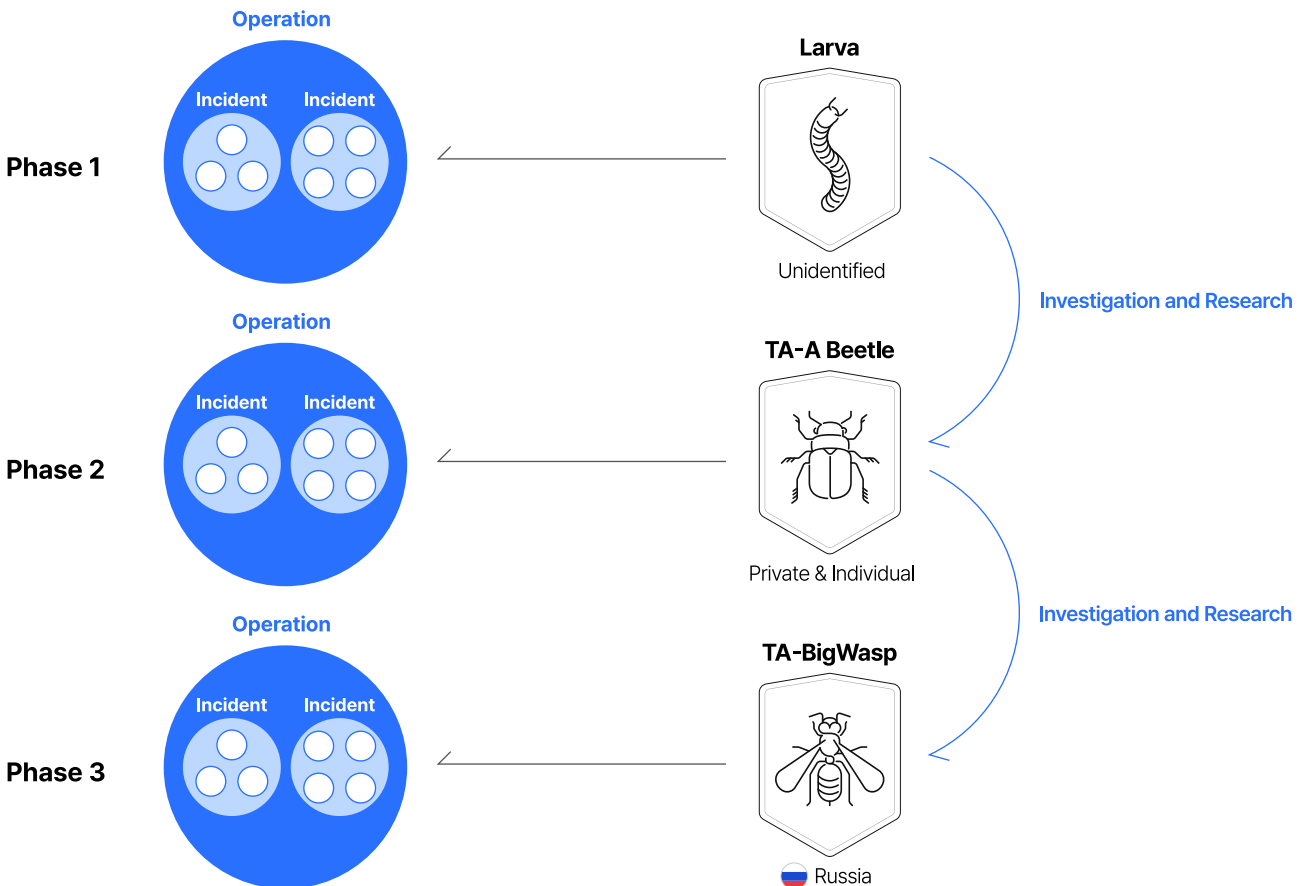
Campaign 분석 시, 단일 공격 활동이 아닌 장기적인 목표를 달성하기 위해 여러 Operation이 연계된 공격 활동을 분석하는 데 중점을 둔다. 이 단계는 공격자의 궁극적인 목적과 장기적인 전략을 파악하는 데 중점을 준다. 이를 위해, 여러 위협 행위자가 장기간에 걸쳐 협력하거나 독립적으로 활동한 사례를 분석한다.

3-1. 위협 행위자와 위협 활동의 연관 관계

다음으로, 본 체계에서 위협 행위자와 위협 활동이 어떤 연관 관계를 형성하는지 살펴보자.

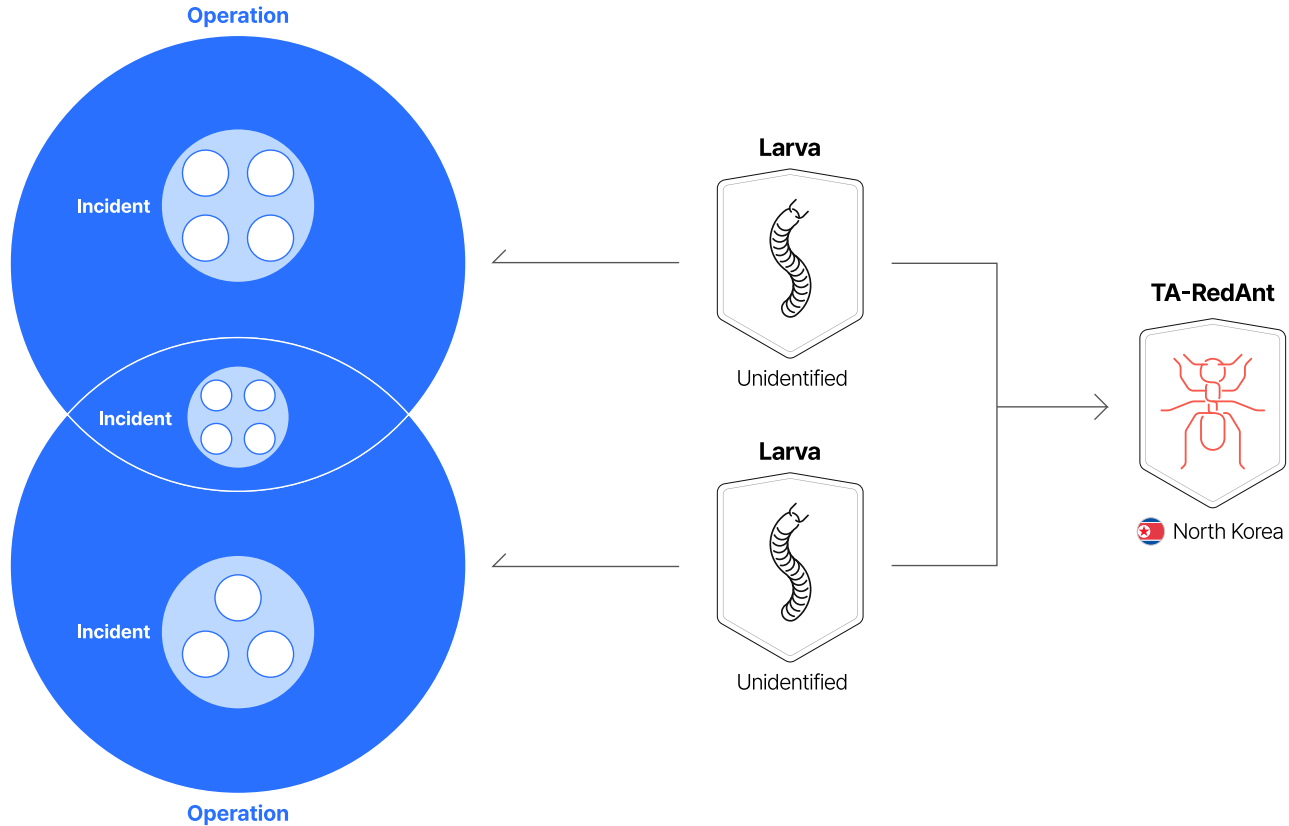
위협 활동에서 Operation은 Incident의 집합으로, 초기에는 미확인 위협 행위자인 Larva가 공격을 수행하는 것으로 본다. 이후 자체 조사, 법 집행 기관 혹은 수사 기관이 확인한 정보를 통해 Larva의 정체가 식별되면 특성에 부합하는 Arthropod로 연결된다. 만약, 후속 조사에서 Operation의 실제 주체나 배후가 다른 것으로 밝혀지거나 다른 위협 행위자의 개입이 확인된 경우, Arthropod 연결이 변경 혹은 추가된다.

예를 들어, [그림 5]를 보면 최초 Larva로 명칭을 부여했던 위협 행위자는 조사 결과 개인 위협 행위자로 식별되어 'TA-FireBeetle'로 명명했다. 하지만, 이후 추가적인 연구를 통해 러시아 배후로 추정되는 위협 행위자로 밝혀져 명칭 연결을 Wasp의 의미가 담긴 'TA-BigWasp'로 변경했다.



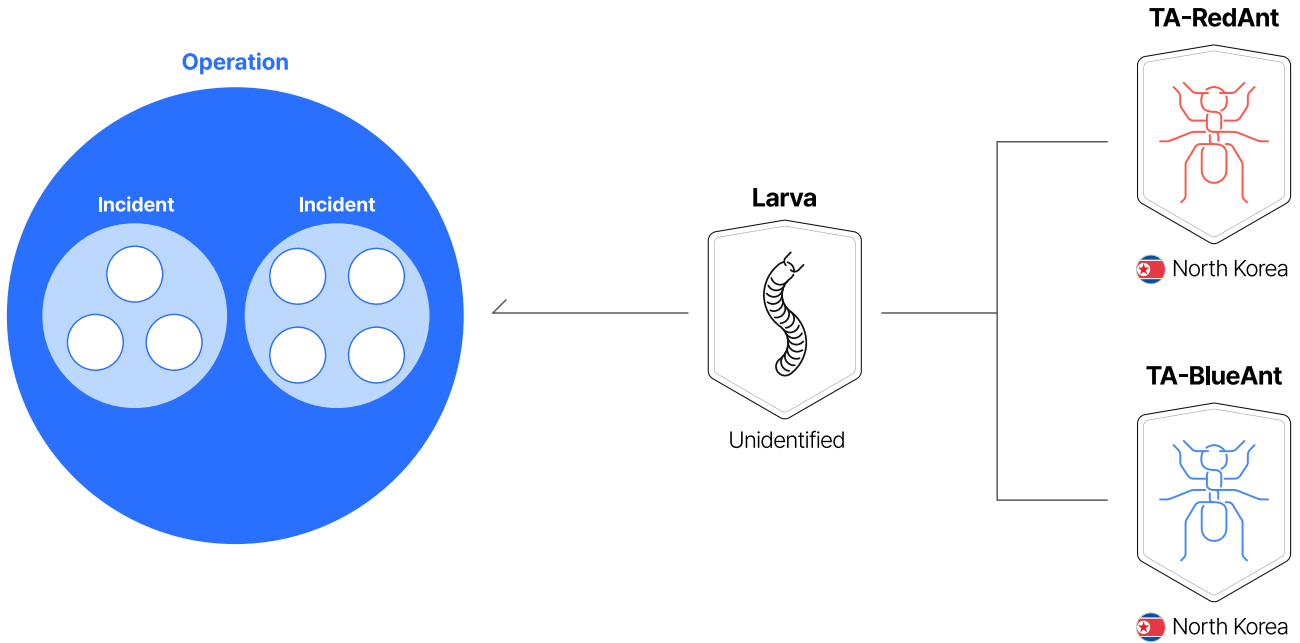
[그림 5] 위협 행위 구조와 명칭 연결의 변화

최근 사이버 위협 행위들을 분석해 보면 하나의 위협 행위자가 여러 독립적인 Operation을 수행하는 경우가 있다. 초기 분석 단계에서는 각 Operation을 개별 Larva가 수행한 것으로 보일 수 있으나, 추가 조사 결과 동일 위협 행위자의 활동으로 확인되면 이들 Larva가 동일한 Arthropod로 연결될 수 있다. 예를 들어, 북한 배후로 추정되는 단일 위협 행위 조직이 사이버 스파이 활동과 랜섬웨어를 이용한 금전적 이익 추구 활동을 동시에 수행했다면, 그 구조는 [그림 6]과 같다.



[그림 6] 단일 위협 행위자가 여러 Operation을 수행했을 때의 구조

반대로, 하나의 Operation에 여러 위협 행위자가 공동으로 참여하는 경우도 있다. 최근에는 악성코드 개발자, 사이버 범죄 조직, 국가 배후 위협 행위자 등 다양한 공격자들이 활동하고 있고, 사이버 공격이 RaaS (Ransomware-as-a-Service) 등 복잡한 구조로 고도화되면서, 공격자들 간 협력과 연계가 더욱 활발해지고 있다. 이때는 단일 Operation에 여러 Arthropod가 협력하는 구조가 된다. [그림 7]은 최초 단일 위협 행위자 소행으로 식별되었던 Operation이 추가 조사 결과 두 개의 서로 다른 북한 배후 추정 위협 행위자의 공격으로 밝혀진 경우다. 이에 따라, 위협 행위자들의 특징을 고려해 각각 'TA-RedAnt', 'TA-BlueAnt'라는 명칭으로 연결하며, 또 다른 위협 행위자가 식별될 가능성도 열어둔다.



[그림 7] 복수 위협 행위자가 단일 Operation을 수행했을 때의 구조

4. 위협 행위 및 행위자 관리 체계 특징 요약

위와 같이 안랩은 위협 행위자 명명법과 3단계 위협 행위 관리 체계를 새롭게 정의했다. 두 체계의 주요 특징을 정리하면 다음과 같다.

- **정보의 불확실성 관리:** 공격을 수행한 모든 위협 행위자는 최초에 정체가 확인되지 않기 때문에 Larva로 시작해 관리한다. 추가 정보를 확보하고 정체가 명확해지면, 해당하는 Arthropod로 연결된다.
- **정보의 왜곡 방지:** 본 체계는 정보에 신뢰도(Confidence)와 가중치(Weight)를 부여해 정보의 신뢰성을 평가하고 관리한다.
- **위협 행위자의 변화 반영:** Larva와 Arthropod 간 유연한 연결을 통해 위협 행위자의 변화를 지속적으로 추적한다.
- **여러 위협 행위자의 관여 고려:** 하나의 Operation 또는 Campaign에 여러 위협 행위자가 동시에 관여할 가능성을 인정한다.
- **위협 인텔리전스 프레임워크 적용:** MITRE ATT&CK, Lockheed Martin Cyber Kill Chain, Diamond Model of Intrusion Analysis 등의 사이버 위협 인텔리전스(CTI) 프레임워크를 참조해 분석 체계를 구축한다.

5. 맺음말

안랩이 수립한 위협 행위 및 행위자 분류 체계는 정확성, 유연성, 신뢰성을 기반으로 설계됐다. 이를 통해, 조직들이 사이버 위협의 복잡성을 보다 체계적으로 이해하고 변화하는 위협 환경에 신속하게 대응할 수 있도록 지원한다. 또한 이 체계는 위협 행위자의 활동을 체계적으로 추적하고 효과적인 대응 전략을 수립할 수 있을 것으로 기대한다. 향후 안랩은 이 분류 체계를 지속적으로 개선하고 발전시켜, 더욱 정교하고 신뢰할 수 있는 위협 인텔리전스를 제공할 계획이다.

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493

홈페이지: www.ahnlab.com

대표전화: 031-722-8000 팩스: 031-722-8901

© 2026 AhnLab, Inc. All rights reserved.