AhnLab

eBook

威胁行为者分类体系与命名法

系统化分类和命名威胁行为者是现代网络安全中的一项非常重要的任务。要有效应对日益复杂的网络攻击，必须先准确理解和分析威胁行为者。鉴于这一需求，AhnLab开发了新的威胁行为者分类和命名法，并建立了三个阶段的威胁行为管理体系。

AhnLab的新方法旨在完善现有分类体系的不足，同时实现更灵活、更准确的威胁分析。该体系的特点在于承认信息的不确定性，并加以管理，同时能够持续反映对威胁行为者变化。此外，通过三个阶段威胁行为管理法，提供了可以系统分析从单个攻击到长期活动的框架。

接下来，将详细介绍威胁行为者命名的重要性与挑战、AhnLab新开发的分类体系，以及如何通过这一体系实现威胁信息的高效管理和分类。

1. 威胁行为者命名的重要性与挑战

在网络安全领域，不同组织之间的交换威胁行为者信息并非易事，因为各组织的情况和利益关系不同。各组织通常基于各自角度收集、识别和分析的信息对威胁行为者进行命名和信息交换。幸运的是，这种交换威胁行为者信息的文化一直得以维系，并成为当今全球网络威胁情报的基石。

对威胁行为者进行命名和管理，能够带来以下好处：

- **易于识别和分类：**通过为威胁行为者赋予唯一名称，可以轻松识别和分类不同的威胁行为者。
- **促进信息共享和沟通：**在安全社区内讨论特定威胁行为者时，使用唯一名称可以实现更清晰、更高效的沟通。
- **增强威胁情报：**将每个威胁行为者的特性、战术和技术与其名称关联记录，能够建立更具体和精确的威胁情报。
- **制定有效的威胁响应策略：**根据特定名称识别威胁行为者的模式和行为，可以更轻松地制定针对该组织的定制型响应策略。
- **保持研究和分析的一致性：**安全研究人员使用一致的名称和描述威胁行为者，有助于研究结果的对比和整合。
- **提高威胁严重性的认知：**提高对具有特定名称的威胁行为者的存在感和危害性的认知，从而推动组织内的安全意识提升。

尽管命名有诸多优势，但也面临一些挑战：

- **信息可见性差异：**各网络安全组织对威胁行为者所能获取的信息和可见性是有限的，并且组织之间存在差异。
- **名称重复：**同一威胁行为者可能有多个名称，或者多个威胁行为者可能使用相同的名称。
- **不准确信息的传播风险：**如果未经充分分析就使用其他组织命名的威胁行为者名称，可能导致不准确信息被生成并传播。

因此，网络安全组织需要充分认识到信息交流的重要性，明确管理和分享威胁行为者的信息，并为持续优化这些过程而努力。

2.AhnLab 的威胁行为者命名体系

为解决上述挑战，AhnLab 开发了一套新的威胁行为者命名体系。该命名体系在补充现有网络安全行业分类方式的基础上，充分考虑了威胁行为者相关情报的不确定性，使其能够以更加灵活的方式进行管理。该体系在设计时考虑到威胁行为者可能以多种形态存在，包括具有国家背景的 APT 组织、幕后国家尚未明确的 APT 组织，以及网络犯罪团伙、勒索软件组织和黑客行动主义者（Hacktivist）等。

AhnLab 的命名体系根据威胁行为者的识别阶段，将其分为 Larva（幼虫） 和 Arthropod（节肢动物）两个阶段。这一概念源自于生物的升值过程：幼虫在早期形态相似，但随着时间推移会逐渐演变为不同的节肢动物。这一比喻直观地体现了在持续分析过程中，威胁行为者真实身份逐步被揭示的过程。

2-1. Larva（幼虫）：未识别的威胁行为者

Larva 指的是在归属信息尚未确认的初期阶段、身份未知的威胁行为者。所有威胁行为者在首次被发现时，都会被归类为 Larva 进行管理，直至获得更多归属信息并完成进一步识别。

类别	名称	名称中文含义	威胁行为者类型
未识别威胁行为者	Larva	幼虫	未识别的威胁行为者

【表1】未识别的威胁行为者命名体系

未识别的威胁行为者将被赋予“Larva-YY###”形式的识别编号。其中，“YY”表示检测年份，“###”表示该年度的检测顺序。例如，“Larva-26001”表示 2026 年首次发现的、尚未被识别归属的威胁行为者。

Larva 属于后文所述“威胁行为三阶段管理体系”中的第一阶段，是 Incident（单个攻击事件）级别及以上赋予的固定名称。随后，通过进一步分析与信息收集，一旦确认其归属于某个特定威胁组织，则会与相应的 Arthropod（已识别威胁行为者）命名进行关联。

【图1】AhnLab 威胁行为者命名流程

2-2.节肢动物（Arthropod）：已识别的威胁行为者

当获取关于 Larva 的充分归属信息后，将根据其与特定国家或组织的关联性，将其连接至相应的 Arthropod 命名。 Arthropod 大致可分为“国家背景的威胁行为者”和“非国家威胁行为者”。

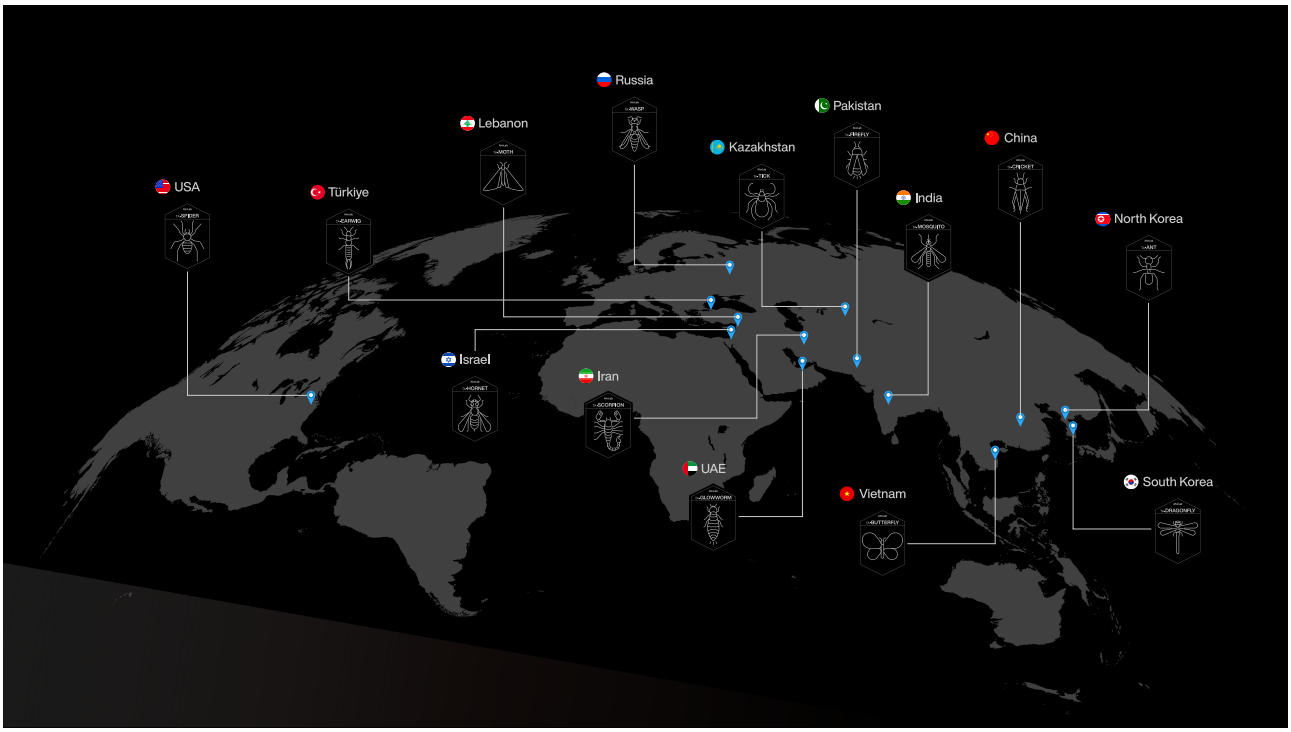
国家背景威胁行为者

国家背景威胁行为者根据各国家所对应的 Arthropod 名称进行区分。例如，推测为朝鲜背景的威胁行为者被命名为 Ant（蚂蚁），而与中国相关的威胁行为者则命名为 Cricket（蟋蟀）。另一方面，若某威胁行为者呈现出高级持续性威胁（APT）的特征，但其幕后国家尚未被明确识别，则将其归入 Mantis（螳螂）类别。

当出现新的信息时，与 Arthropod 的关联关系可随时进行修订（新增、变更或删除）。例如，若某攻击组织最初识别为朝鲜背景，并被归类为 Ant。但在进一步分析后若确认为其实际与中国相关，则与该 Larva 关联的 Arthropod 也将从 Ant 调整为 Cricket。

类别	名称	名称中文含义	威胁行为者类型
国家背景威胁行为者	Mantis	螳螂	幕后国家未确认的 APT
	Ant	蚂蚁	推测为朝鲜背景
	Cricket	蟋蟀	推测为中国背景
	Dragonfly	蜻蜓	推测为韩国背景
	Butterfly	蝴蝶	推测为越南背景
	Firefly	萤火虫	推测为巴基斯坦背景
	Mosquito	蚊子	推测为印度背景
	Tick	蜱虫	推测为哈萨克斯坦背景
	Wasp	黄蜂	推测为俄罗斯背景
	Spider	蜘蛛	推测为美国背景
	Scorpion	蝎子	推测为伊朗背景
	Hornet	大黄蜂	推测为以色列背景
	Moth	飞蛾	推测为黎巴嫩背景
	Glowworm	荧光虫	推测为阿联酋背景
	Earwig	蠼螋	推测为土耳其背景

【表2】国家背景威胁行为者代表命名



【图2】全球威胁行为者分布

由于国家背景威胁行为者并非单一组织，而可能由多个不同的攻击组织组成，因此为了对其进行识别和区分，采用“TA 前缀 + Modifier + Arthropod”的命名结构。该命名方式既保持了国家层面的代表性，又能够更加清晰地区分同一国家内部不同威胁行为者的特征与差异。

AhnLab 对部分威胁行为者按照如下方式命名并进行管理：

- **TA-GiantAnt：**被称为 Lazarus 的朝鲜背景攻击组织
- **TA-RedAnt：**被称为 RedEyes 的朝鲜背景攻击组织
- **TA-ShadowCricket：**被称为 ShadowForce 的中国背景攻击组织

Larva 的幕后国家信息一旦被确认，便会与该国家对应的威胁行为者命名进行关联；若通过进一步分析识别或确定了具体的攻击组织，则会进一步与该攻击组织的名称建立关联。

非国家背景威胁行为者

网络犯罪组织、勒索软件组织以及黑客行动主义者（Hacktivist）等，也可能与某些国家存在一定关联。然而，在对这些威胁行为者进行分类时，相比国家背景，其活动目的与攻击类型更为重要。因此，非国家背景的威胁行为者将如【表3】所属，根据其主要活动目的与攻击特征进行分类并加以管理。

类别	名称	名称中文含义	威胁行为者类型
非国家背景威胁行为者	Beetle	甲虫	网络犯罪组织
	Tarantula	狼蛛	勒索软件组织
	Cicada	蝉	黑客行动主义者组织

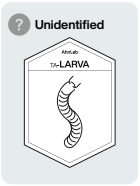
【表3】非国家背景威胁行为者命名

非国家背景威胁行为者数量庞大，且其中部分组织会自行使用特定名称，因此为每个对象单独赋予唯一名称方面存在一定局限。因此，对非国家背景威胁行为者采用不同于国家背景威胁行为者的命名规则。非国家背景威胁行为者的命名采用“TA 前缀 + Arthropod + YY + ###”的结构。

例如：TA-Beetle-25001

这种方式基于“年份（YY）”与“识别编号（###）”进行系统化分类，使得大量非国家背景威胁行为者能够被更高效地追踪和管理。

Unidentified



Nation-State

Non-Nation-State

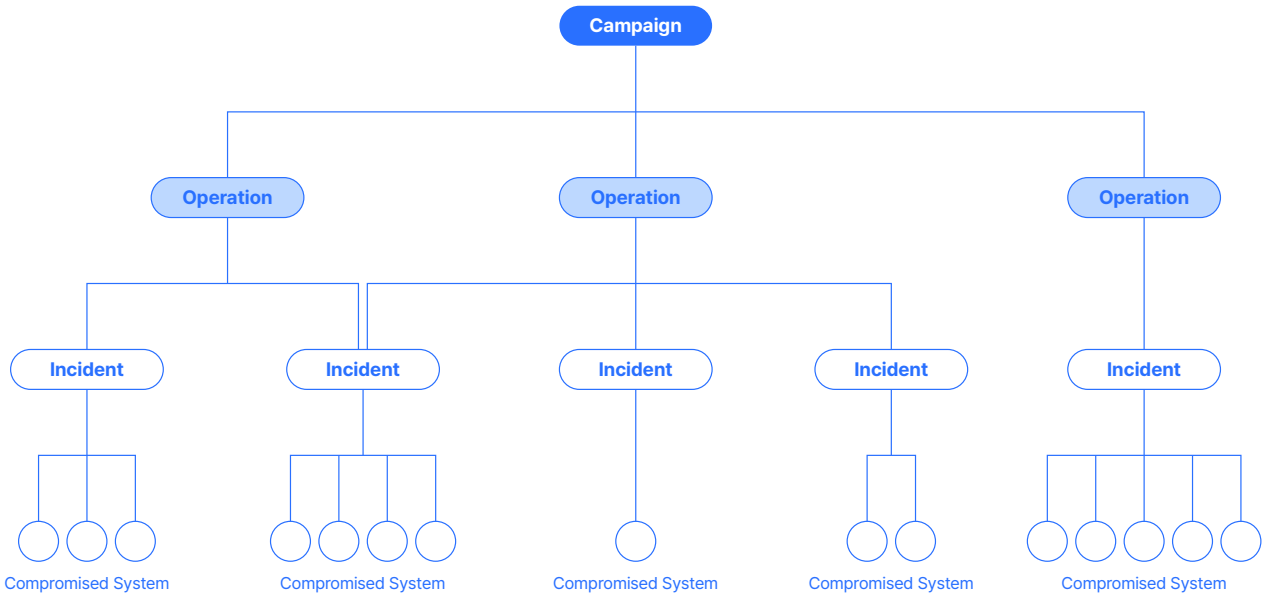
【图3】威胁行为者图标与命名

3.三阶段威胁行为管理体系

AhnLab 定义的三阶段威胁行为管理体系以网络威胁的层级为基础，由 Incident（单个攻击事件）→ Operation（攻击活动）→ Campaign（长期且具有组织的攻击活动）构成。该体系在各阶段对多种威胁要素进行综合管理，并提供了一套能够从单个攻击事件到长期攻击活动（Campaign）进行系统化分析的框架。

类别	名称	名称中文含义	说明
第一阶段	Incident	单个攻击事件	已确认受害者或受害组织的单个攻击事件
第二阶段	Operation	攻击活动	由多个 Incident 组成的一个攻击活动单元
第三阶段	Campaign	长期且具有组织的攻击活动	由两个以上 Operation 构成，持续时间至少数个月至一年以上的攻击活动

【表4】三阶段威胁行为管理体系



【图4】三个阶段威胁行为管理体系关系图

#1. Incident: 单个攻击事件

Incident指的是已确认受害者或受侵害组织的单个攻击事件。每个Incident都会被赋予唯一的管理编号“INC-YYMMDD-###”，其含义为“INC（入侵事件）-YYMMDD（年月日）-###（顺序）”。对于Incident，重点在于分析事件的特性、入侵范围、使用的攻击手法等，以了解该事件具有什么特点。通过这一阶段，可以准确识别单个攻击事件，并为构建更高层次的Operation奠定基础。

#2. Operation: 攻击活动

Operation是将多个事件组成一个攻击活动的单位。重点在于综合分析攻击的特点、目标和使用的技术，以找出各事件之间的关联性，并了解攻击活动的模式和意图。Operation的名称格式为“OP-YYMMDD-###”，其结构与Incident的名称结构相同。

在Operation分析中会考虑各种因素，主要项目如下：

- **Goal:** 攻击者的最终目标
- **Target:** 攻击对象（组织、行业领域、地区等）
- **Malware:** 所使用的恶意代码种类和特点
- **Tool:** 攻击中使用的工具和软件
- **Vulnerability:** 被利用的漏洞
- **Technique:** 攻击技术和战术
- **Infrastructure:** 攻击中使用的基础设施（C&C服务器、代理等）

通过对这些多种因素进行综合分析，可以识别各Operation的固有特点和模式，从而更准确地追踪威胁行为者的活动。

从分析威胁行为者的角度来看，在分析的初始阶段，Operation被视为由未识别的威胁行为者Larva执行的。由于在分析开始时威胁行为者的归属信息不明确，因此以Larva命名进行管理，应对信息不确定性。之后，当获得更可靠的信息时，可以将威胁行为者与Arthropod关联起来。

在Operation阶段，重要的一点是一个攻击活动中可能涉及多个威胁行为者。在本体系中，考虑到网络攻击可能基于多个威胁行为者之间的合作，因此允许Larva关联到多个Arthropod。从实际攻击案例来看，个人、受雇威胁行为者或威胁团体常常为了共同的目标进行合作。

#3. Campaign: 长期且组织化的攻击活动

Campaign是指长期且有组织的攻击活动，包括持续至少几个月到一年以上的攻击活动。Campaign由两个或多个Operation组成，并在长时间内利用多种攻击技术以实现长期目标。对于这样的Campaign，也是在经过长期分析后定义其名称。

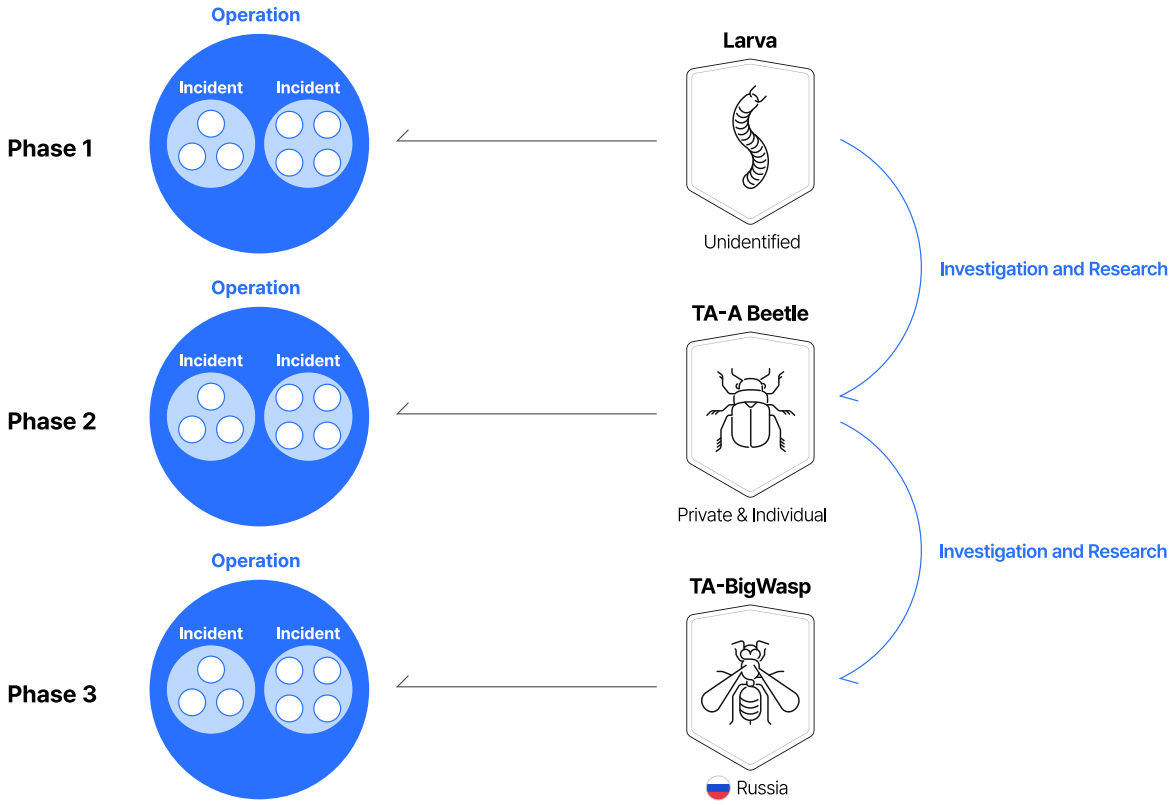
在分析Campaign时，重点分析涉及多个Operation以实现长期目标的攻击活动，而不是单一攻击活动。此阶段的目标是了解攻击者的最终目的和长期战略。为此，会对多个威胁行为者长期合作或独立活动的案例进行分析。

3-1. 威胁行为者与威胁活动的相关关系

接下来，将探讨在本体系中威胁行为者与威胁活动的相关关系。

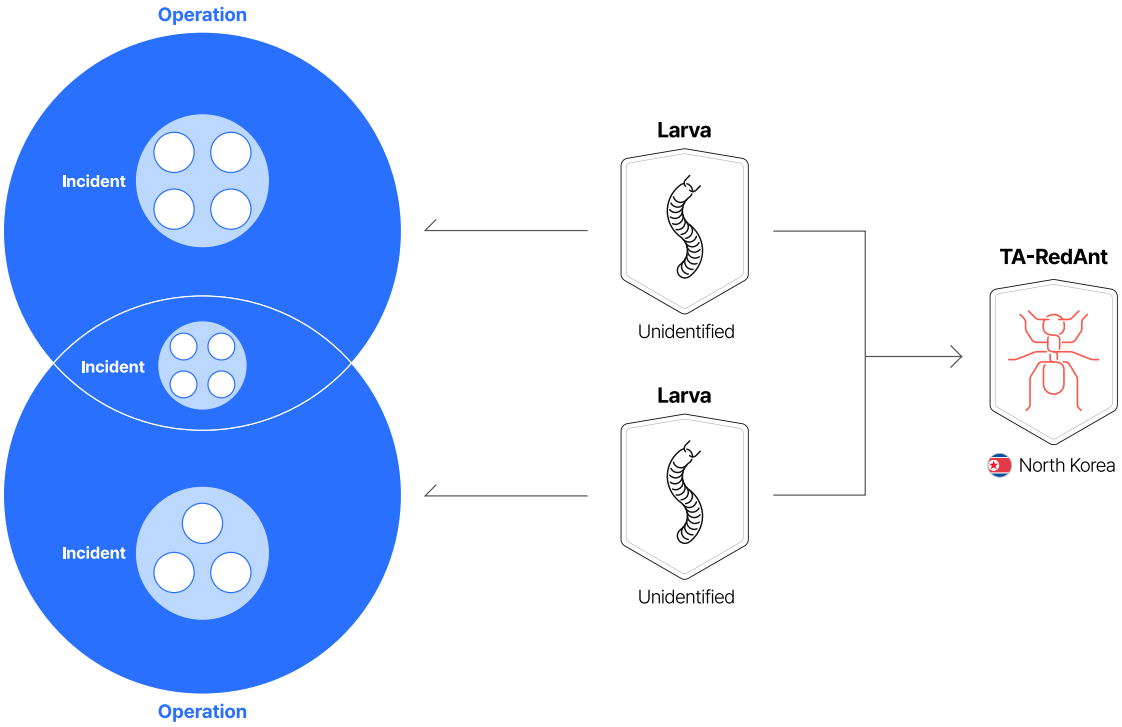
在威胁活动中，Operation是Incident的集合，初期可以认为攻击是由未确认的威胁行为者Larva执行的。之后，通过内部调查或执法机构、调查机构确认的信息识别Larva的身份，并根据其特性将其关联到相应Arthropod。如果在后续调查中发现Operation的实际主体或背景与预期不同，或者确认了其他威胁行为者的介入，则会更改或增加关联的Arthropod。

例如，从【图5】可以看到，最初被命名为Larva的威胁行为者经过调查被识别为个人威胁行为者，并命名为“TA-FireBeetle”。但是，经过进一步研究，发现该威胁行为者疑似具有俄罗斯背景，因此重新命名为包含Wasp意义的“TA-BigWasp”。



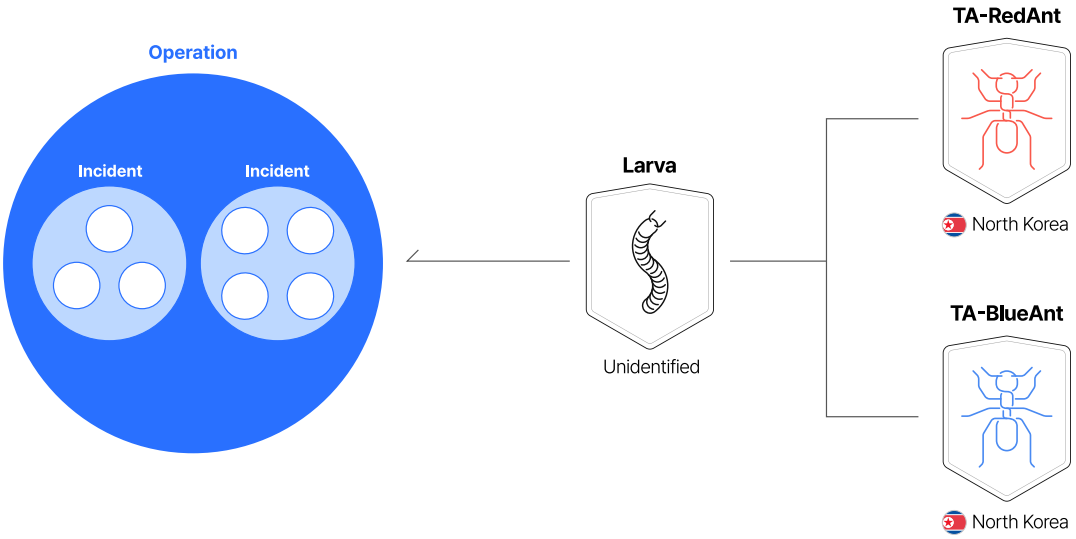
【图5】威胁行为结构与命名连接的变化

此外，对近期网络威胁行为的分析表明，一个威胁行为者可能执行多个独立的Operation。起初，各Operation被认为是由单独的Larva执行的，但经过调查，如果是同一威胁行为者所为，这些Larva将连接到同一个Arthropod。例如，如果一个被认为可能具有朝鲜背景的单一威胁行为组织同时进行网络间谍活动和利用勒索软件寻求经济利益的活动，其结构将如图6所示。



【图6】单一威胁行为者执行多个Operation时的结构

相反，也有多个威胁行为者共同参与一个Operation的情况。近期，包括恶意代码开发者、网络犯罪组织和具有国家背景的威胁行为者在内的各种攻击者都非常活跃。网络攻击演变为RaaS（Ransomware-as-a-Service，勒索软件即服务）等复杂结构，攻击者之间的合作和联系变得更加频繁。这样就形成了在单一Operation中多个Arthropod合作的结构。【图7】显示了一个最初被识别为单一威胁行为者所为的Operation，经过进一步调查，发现是两个不同的疑似具有朝鲜背景的威胁行为者的攻击。因此，根据威胁行为者的特征，将其分别重新命名为“TA-RedAnt”和“TA-BlueAnt”，同时也不排除识别出其他威胁行为者的可能性。



【图7】多个威胁行为者执行单一Operation时的结构

4. 威胁行为和行为者管理体系特点总结

如上所述，AhnLab重新定义了威胁行为者命名法和三个阶段威胁行为管理体系。这两个体系的主要特点如下：

- **管理信息不确定性：**所有执行攻击的威胁行为者由于其身份最初未得到确认，因此被归类为Larva进行管理。一旦获得更多信息并明确身份，就会连接到相应Arthropod。
- **防止信息失真：**该体系通过赋予信息可信度（Confidence）和权重（Weight）来评估和管理信息的可靠性。
- **反映威胁行为者的变化：**通过Larva和Arthropod之间的灵活连接，持续追踪威胁行为者的变化。
- **考虑多个威胁行为者的参与：**考虑到了在一个Operation或Campaign中可能有多个威胁行为者同时参与。
- **应用威胁情报框架：**参考MITRE ATT&CK、Lockheed Martin Cyber Kill Chain（洛克希德·马丁网络杀伤链）、入侵分析钻石模型（Diamond Model of Intrusion Analysis）等网络威胁情报（CTI）框架来构建分析体系。

5. 结语

AhnLab建立的威胁行为和行为者分类体系基于准确性、灵活性和可靠性。这有助于组织了解网络威胁的复杂性并快速响应不断变化的威胁环境。通过该体系，将能够密切追踪威胁行为者的活动，并制定更有效的响应策略。未来，AhnLab计划持续完善和发展这一分类体系，以提供更精确、更可靠的威胁情报。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区新镇路1699弄E栋303室
https://www.ahnlab.com/cn | cn.sales@ahnlab.com
电话： +86 10 8260 0932（北京）| +86 21 6095 6780（上海）