AhnLab

eBook

脅威アクター分類システムと命名法

脅威アクターを体系的に分類し命名することは、現代のサイバーセキュリティにおいて非常に重要な課題です。高度化するサイバー攻撃に効果的に対応するためには、脅威アクターに対する正確な理解と分析が先行する必要があるためです。アンラボは、このような必要性を認識し、脅威アクターに対する新たな分類および命名法と、脅威行為を3段階で管理するシステムを開発しました。

アンラボの新たなアプローチは、従来の分類システムの限界を補完すると同時に、より柔軟かつ正確な脅威分析を目標としています。本システムの特徴は、情報の不確実性を認め、これを管理する方式と脅威アクターの変化を持続的に反映できるようにすることです。また、3段階の脅威行為管理法によって、個別の攻撃から長期的な攻撃キャンペーンまで、体系的に分析できるフレームワークを提示します。

脅威アクター命名の重要性と課題、アンラボの新たな脅威アクター分類システム、そして具体的な脅威情報の管理と分類方式まで、アンラボが新しく考案した脅威アクター分類システムと命名法をご紹介します。

1. 脅威アクター命名の重要性と課題

サイバーセキュリティ組織間の脅威アクターに関する情報交流は、各組織の状況や利害関係が異なるため、簡単な課題ではありません。組織は各自の観点から収集、把握および分析した情報をもとに脅威アクターを命名して情報を公開することで交流しており、幸いにもこのような脅威アクター情報の交流文化はうまく維持され、今日のグローバルサイバー脅威インテリジェンスの基礎的役割を担っています。

脅威アクターを命名して管理すると、以下のようなメリットがあります。

- **識別および分類の容易性:** 脅威アクターに固有名称を付与することで、各アクターを容易に識別、分類することができます。
- **情報共有およびコミュニケーションの向上:** セキュリティのコミュニティ内で特定の脅威アクターについて議論する際、固有名称を使用すればより明確で効率的な意思疎通ができます。
- **脅威インテリジェンスの強化:** 各脅威アクターの特性、戦術、技術などを名前と関連付けて記録・分析し、より具体的かつ高精度な脅威インテリジェンスを構築できます。
- **効果的な脅威対応戦略の策定:** 特定の名称により識別された脅威アクターのパターンと行動を把握し、当該グループに合わせたカスタマイズ型対応戦略の策定が容易になります。
- **研究および分析の一貫性維持:** セキュリティ研究者が同じ脅威アクターに対して一貫した名称を使用することにより、研究結果の比較と統合が容易になります。
- **脅威の深刻性に対する認識の向上:** 特定の名称を持つ脅威アクターの存在感と危険性に対する認識を高め、組織内のセキュリティ意識向上に役立ちます。

ただし、脅威アクターの命名には以下のような課題も残されています。

- **情報可視性の差:** 各サイバーセキュリティ組織が脅威アクターについて確保できる情報と可視性は限定的であり、組織別の差も存在します。
- **名称の重複:** 同じ脅威アクターに複数の名称が付与される、または複数の脅威アクターが同じ名称で呼ばれるケースが発生することがあります。
- **不正確な情報伝播のリスク:** 十分な分析を行わず、他の組織が付与した名称を無分別に使用すると、脅威アクターに対する不正確な情報が生成され伝播するリスクがあります。

したがって、サイバーセキュリティ組織は情報交流の重要性を認識し、脅威アクターに関する情報を明確に管理して提供しなければならず、これを継続するために努力する必要があります。

2. アンラボの脅威アクター命名法

アンラボは、これらの課題を解決するために新たな脅威情報管理システムを開発しました。脅威アクターの命名法は、従来サイバーセキュリティ業界において使用されていた方式を補完し、情報の不確実性を反映して柔軟に管理できるように設計しました。脅威アクターは国家関与のAPTグループだけでなく、国家が識別されていないAPTグループ、サイバー犯罪者、ランサムウェアグループ、ハクティビストグループなど様々な形態で存在し得ることを考慮して構成しました。

アンラボの新規命名法を基準に、脅威アクターは大きな枠組みでLarva（幼虫）とArthropod（節足動物）に区分されます。これは、幼虫が初期には似た姿をしていても、時間の経過とともにそれぞれ異なる節足動物へと変化する過程に着想を得た概念で、分析の進展に伴い脅威アクターの実体が徐々に明らかになる様子を直感的に表現しています。

2-1. Larva（幼虫）：識別されていない脅威アクター

Larvaは、正体が識別されていない身元不詳の攻撃者を意味します。すべての脅威アクターは最初に確認された時、追加の帰属情報が確認されるまでLarvaから始まり管理されます。

区分	名称	意味	説明
識別されていない脅威アクター	Larva	幼虫	識別されていない脅威アクター

[表1] 識別されていない脅威アクターの命名法

Larvaの名称を付与した脅威アクターは「Larva-YY###」形式の管理番号に基づいて表記されます。「YY」は検知年度、「###」はその年の検知順序を意味します。例えば、「Larva-26001」は2026年に初めて確認された識別されていない脅威アクターを意味します。

Larvaは後述する「脅威行為の3段階管理法」のうち、1段階に該当する「Incident（個別の攻撃事件）」単位以上で付与される脅威アクター名称です。さらなる分析により帰属情報が確認されると、識別された脅威アクターを意味するArthropodに結びつけます。

[図1] アンラボの脅威アクター名称付与のプロセス

2-2. Arthropod（節足動物）: 識別された脅威アクター

Larva に関する十分な帰属情報が確保されると、特定の国または組織との関連性を考慮し、該当する Arthropod の名称に結びつけます。Arthropodは、大きく国家関与の脅威アクターと非国家の脅威アクターに区分されます。

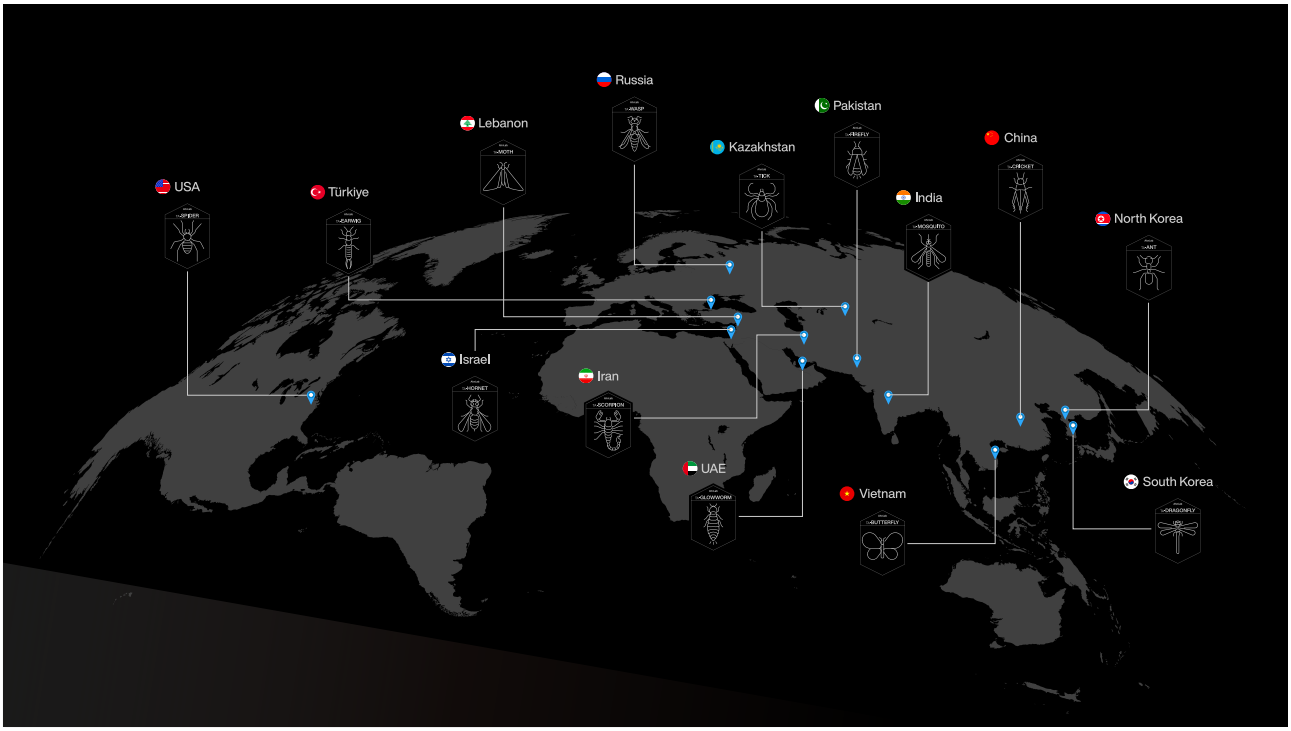
国家関与の脅威アクター

国家関与の脅威アクターは、国ごとに固有の Arthropod 名称を使用して区分します。例えば、北朝鮮の関与が推定される脅威アクターは Ant（アリ）、中国と関連する脅威アクターは Cricket（コオロギ）と命名します。一方、高度化した持続的脅威（APT）の特性を示すが、背後の国家が明確に特定されていない場合には、Mantis（カマキリ）として分類されます。一方、高度な持続的脅威（APT）の特性を示しながらも、関与国家が明確に特定されていない場合には Mantis（カマキリ）として分類されます。

Arthropod への結びつきは流動的であり、新たな情報が確認されるといつでも修正(追加、変更、削除)されることがあります。例えば、北朝鮮の脅威アクターと識別されていた攻撃グループが、さらなる分析によって中国の脅威アクターと判明した場合、Larva と結びついた Arthropod も Ant から Cricket に変更されることがあります。

区分	名称	意味	説明
国家関与の脅威アクター	Mantis	カマキリ	国家関与が確認されていない APT
	Ant	アリ	北朝鮮の関与を推定
	Cricket	コオロギ	中国の関与を推定
	Dragonfly	トンボ	韓国の関与を推定
	Butterfly	蝶	ベトナムの関与を推定
	Firefly	ホタル	パキスタンの関与を推定
	Mosquito	蚊	インドの関与を推定
	Tick	ダニ	カザフスタンの関与を推定
	Wasp	スズメバチ	ロシアの関与を推定
	Spider	蜘蛛	アメリカの関与を推定
	Scorpion	サソリ	イランの関与を推定
	Hornet	スズメバチ	イスラエルの関与を推定
	Moth	ガ	レバノンの関与を推定
	Glowworm	ホタル	アラブ首長国連邦の関与を推定
	Earwig	ハサミムシ	トルコの関与を推定

[表2] 国家関与の脅威アクターの代表名称



[図2] 世界中の脅威アクター分布

国家関与の脅威アクターは、単一のグループではなく複数のグループとして存在する可能性があります。これらを識別し区別するために、TA接頭辞+Modifier+Arthropod　のような命名構造を採用しています。この方式は、国家単位での代表性を維持しつつ、同一国家内に存在する多様な脅威アクターの特性や違いをより明確に識別できるよう設計されています。

アンラボは一部の脅威アクターに対して、次のように名称を付与し管理しています。

- **TA-GiantAnt:** Lazarusとして知られる北朝鮮系攻撃グループ
- **TA-RedAnt:** RedEyesとして知られる北朝鮮系攻撃グループ
- **TA-ShadowCricket:** ShadowForceとして知られる中国系攻撃グループ

Larvaの関与国家情報が確認されると、該当する国家の脅威アクター名称に結び付けられ、さらなる追加分析によって特定の攻撃グループまで識別または指定された場合には、そのグループ名に結び付けられます。

非国家の脅威アクター

サイバー犯罪者、ランサムウェアグループ、ハクティビストも特定の国と関連している可能性がありますが、これらの分類においては、国家との関連性よりも活動目的や攻撃の種類がより重要な基準となります。これに基づき、非国家脅威アクターは[表３]のように主な活動目的と攻撃の特性に基づいて分類・管理します。

区分	名称	意味	説明
非国家の脅威アクター	Beetle	カブトムシ	サイバー犯罪組織
	Tarantula	タランチュラ	ランサムウェアグループ
	Cicada	セミ	ハクティビストグループ

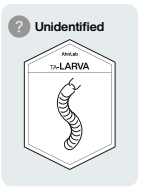
[表3] 非国家脅威アクターの名称

非国家の脅威アクターは数が膨大であり、なかには自ら名称を用いるものも存在するため、個別に固有名を付与するには限界があります。したがって、国家関与の脅威アクターとは異なる命名規則を適用します。
非国家の脅威アクターの名称は、TA接頭辞+Arthropod+YY+###の構造に従います。

例) TA-Beetle-25001

この方式は、年度（YY）と識別番号（###）に基づく体系的な分類を可能にし、多数の非国家脅威アクターを効率的に追跡・管理できるようにしています。

Unidentified



Nation-State

Non-Nation-State

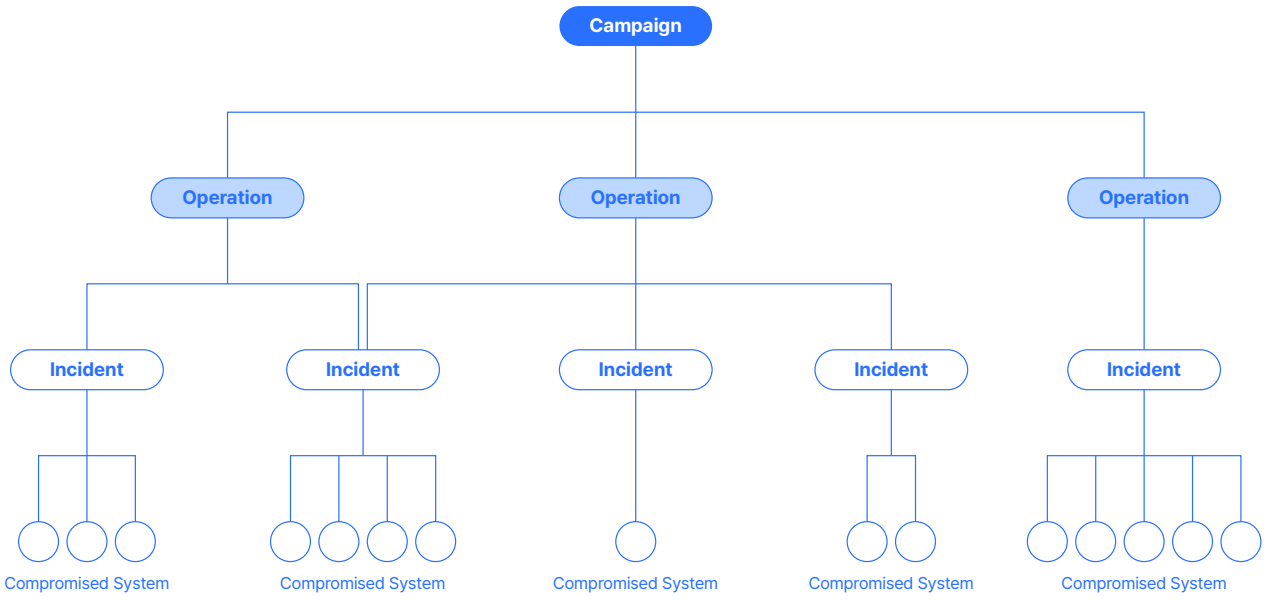
[図3] 脅威アクターのアイコンと名称

3. 3段階の脅威行為管理システム

アンラボが定義した3段階の脅威行為管理システムは、サイバー脅威のレベルを基準に　Incident（個別の侵害事件）→Operation（攻撃活動）→Campaign（長期的かつ組織的な攻撃活動）」で構成されています。各段階において様々な脅威要素を総合的に管理し、個別の攻撃から長期的な攻撃キャンペーンまで、体系的に分析できるフレームワークを提示します。

区分	名称	意味	説明
第1段階	Incident	個別の侵害事件	被害者や被害を受けた組織が確認された個別の攻撃事件
第2段階	Operation	攻撃活動	複数の Incident を一つの攻撃活動として構成した単位
第3段階	Campaign	長期的かつ組織的な攻撃活動	二つ以上の Operation で構成され、長期的な目標を達成するために長い期間にわたり様々なの攻撃手法

[表4] 3段階の脅威行為管理システム



[図4] 3段階の脅威行為管理システム関係図

#1. Incident: 個別の攻撃事件

Incidentは、被害者や被害を受けた組織が確認された個別の攻撃事件を意味します。各Incidentには固有の管理番号「INC-YYMMDD-###」を付与しますが、意味を紐解くと「INC(侵害事件)-YYMMDD(年月日)-###(順序)」と解釈されます。Incidentについては事件の特性、被害範囲、使用された技術などに関する分析を実施し、当該事例がどのような特徴を持つのかを把握することに重点を置いています。これによって、単体の攻撃事件を正確に識別し、上位段階であるOperationを構成する基礎を構築することができます。

#2. Operation: 攻撃活動

Operation は、複数の Incident を一つの攻撃活動として構成した単位です。攻撃の特徴、目標、使用された技術などを総合的に分析し、複数の事件同士の関連性を把握して攻撃活動のパターンと意図を理解することに重点を置きます。Operation の名称は「OP-YYMMDD-###」で付与されますが、その構造は Incident の名称構造と同じです。

Operation の分析には様々な要素を考慮しますが、主な項目は以下の通りです。

- **Goal:** 攻撃者の究極的な目標
- **Target:** 攻撃対象(組織、産業分野、地域等)
- **Malware:** 使用されたマルウェアの種類と特徴
- **Tool:** 攻撃に利用されたツールとソフトウェア
- **Vulnerability:** 悪用された脆弱性
- **Technique:** 攻撃の手法と戦術
- **Infrastructure:** 攻撃に使用されたインフラ(C&C サーバー、プロキシ等)

このように、様々な要素を総合的に分析することで、各 Operation の固有の特性とパターンを識別し、脅威アクターの活動をより正確に追跡することができます。

脅威アクター分析の観点から見ると、分析の初期段階では Operation が識別されていない脅威アクターである Larva により行われたものと見なします。これは、分析を開始した時点では脅威アクターの帰属情報が明確でないため、Larva と命名して管理し、情報の不確実性に対処するものです。その後、より確実な情報が追加されると脅威アクターを Arthropod に結びつけることができます。

Operation 段階において重要な点は、一つの攻撃活動に複数の脅威アクターが関与し得るという点です。本システムではサイバー攻撃が複数の脅威アクター同士の協力の下で行われる可能性を考慮し、Larva に複数の Arthropod が結びつくようにしました。実際の攻撃事例を見ても、個人、雇われた脅威アクター、または脅威グループが共通の目標を持って協力するケースが多いです。

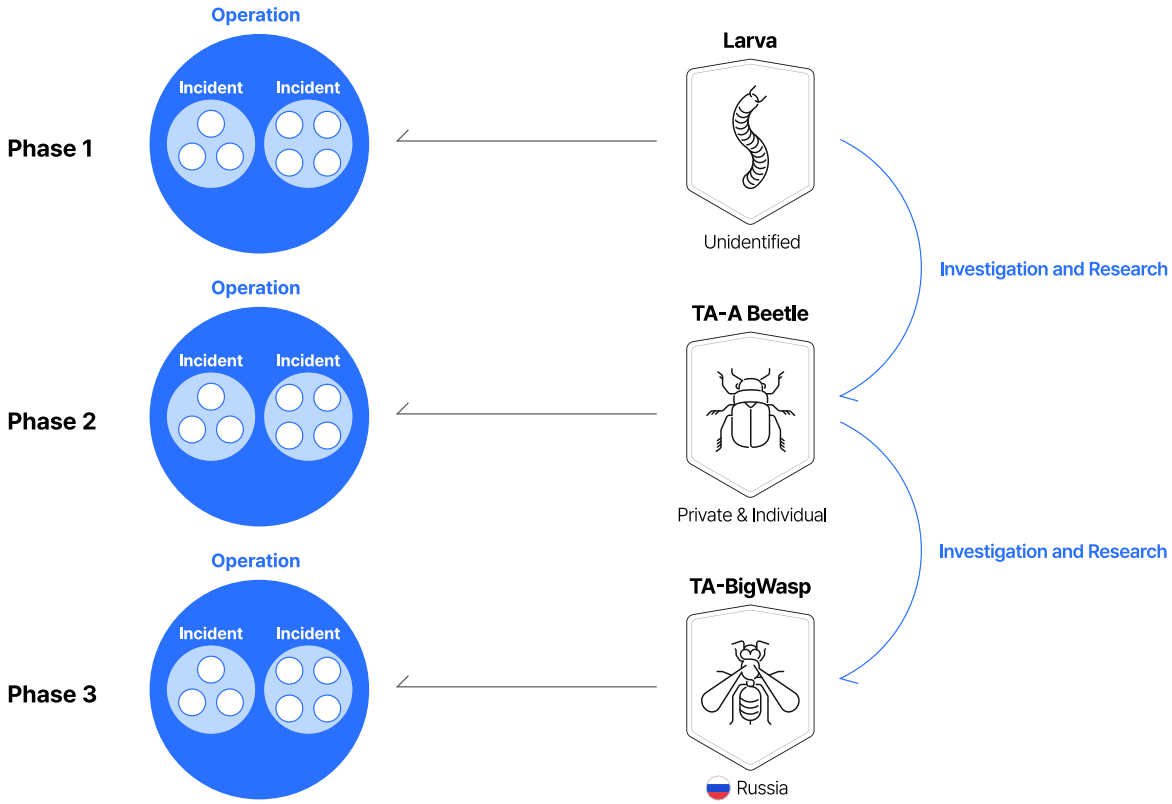
#3. Campaign: 長期的かつ組織的な攻撃活動

Campaign は長期的かつ組織的な攻撃活動であり、最短で数か月から1年以上続いた攻撃活動を含みます。Campaign は二つ以上の Operation で構成され、長期的な目標を達成するために長い期間にわたり様々なの攻撃手法を活用します。このような Campaign についても、長期的な分析の後に名称を定義します。

Campaign の分析では、単体の攻撃活動ではなく、長期的な目標を達成するために複数の Operation が連携した攻撃活動を分析することに重点を置きます。この段階は、攻撃者の究極的な目的と長期的な戦略を把握することが目標です。このために、複数の脅威アクターが長期間にわたり協力する、または独立的に活動を行った事例を分析します。

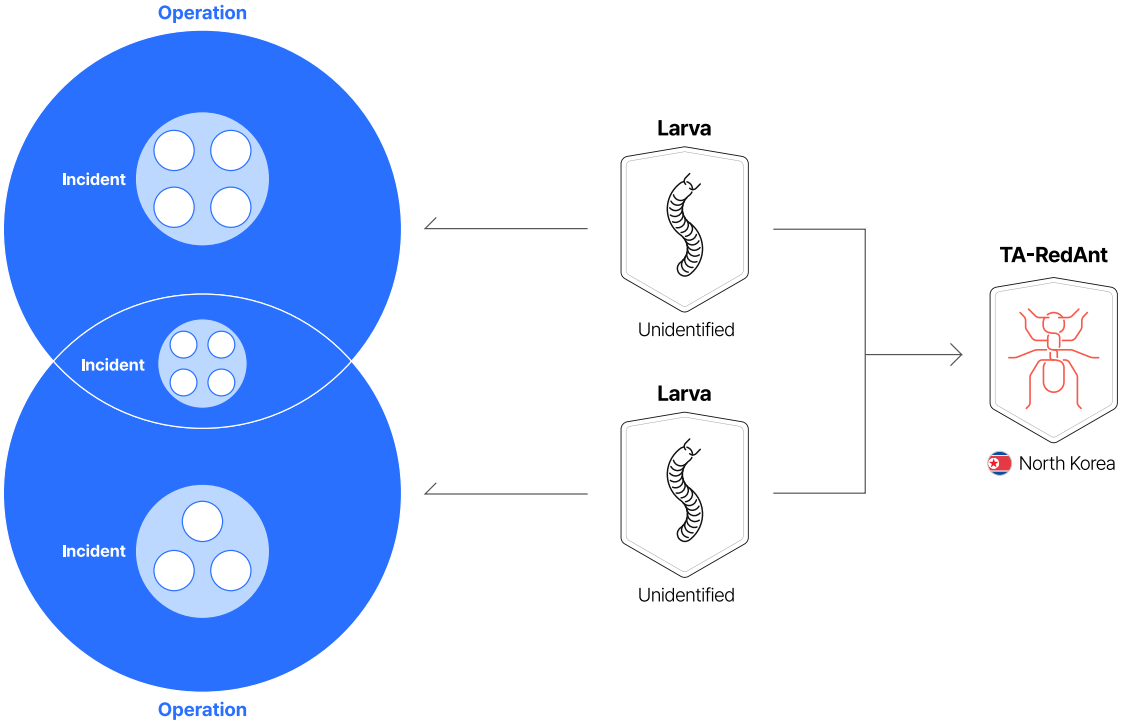
3-1. 脅威アクターと脅威活動の相関関係

次に、本システムにおいて脅威アクターと脅威活動がどのような相関関係を形成するのかを見ていきます。脅威活動において、Operation は Incident の集合であり、初期段階では未確認の脅威アクターである Larva が攻撃を遂行するものと見なします。その後、自社の調査と、法執行機関または捜査機関が確認した情報を通じて Larva の正体が識別されると、特性に一致する Arthropod へ結びつけます。万が一、後続調査で Operation の実際の主体や背景が異なっていたことが明らかになる、または他の脅威アクターの介入が確認された場合、Arthropod の結びつきが変更または追加されます。
例えば、[図5]を見ると、当初は Larva で名称を付与した脅威アクターは、調査の結果個人の脅威アクターと識別され「TA-FireBeetle」と命名されました。しかし、その後のさらなる研究によってロシアの関与が推定される脅威アクターであることが明らかになり、名称の結びつきを Wasp の意味が含まれた「TA-BigWasp」に変更しました。



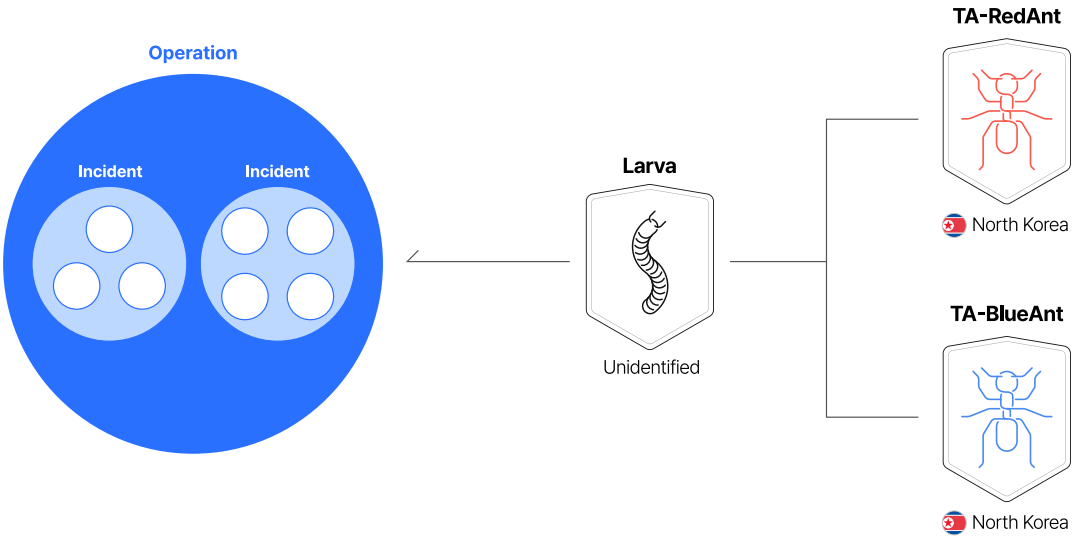
[図5] 脅威行為の構造と名称の結びつきの変化

また、最近のサイバー脅威行為を分析してみると、一つの脅威アクターが複数の独立したOperationを遂行するケースが存在します。このとき、最初は各Operationを個々のLarvaが遂行したものと見なしますが、調査の結果同じ脅威アクターの仕業であることが判明すると、これらのLarvaが同じArthropodに結びつきます。例えば、北朝鮮の関与が推定される単体の脅威行為の組織がサイバースパイ活動とランサムウェアを利用した金銭的利益の追求活動を同時に遂行した場合、その構造は[図6]のようになります。



[図6] 単体の脅威アクターが複数のOperationを遂行したときの構造

逆に、一つのOperationに複数の脅威アクターが共同で参加するケースも存在します。最近ではマルウェア開発者、サイバー犯罪組織、国が関与する脅威アクターなど、様々な攻撃者が活動しており、サイバー攻撃がRaaS(Ransomware-as-a-Service)などの複雑な構造へと高度化したことで、攻撃者同士の協力や連携がより活発化しています。この場合は、単体のOperationに複数のArthropodが協力する構造となります。[図7]は、最初に単体の脅威アクターの仕業と識別されていたOperationが追加調査の結果、二つの異なる北朝鮮の関与が推定される脅威アクターの攻撃であることが判明したケースです。したがって、脅威アクターの特徴を考慮してそれぞれ「TA-RedAnt」、「TA-BlueAnt」という名称に結びつけ、別の脅威アクターが新たに識別される可能性も残しておきます。



[図7] 一つの Operation に複数の脅威アクターが協力するときの構造

4. 脅威行為および脅威アクター管理システムの特徴の要約

上記のように、アンラボは脅威アクターの命名法と3段階の脅威行為管理システムを新たに定義しました。これらのシステムの主な特徴をまとめると、以下の通りです。

- **情報の不確実性の管理:** 攻撃を遂行したすべての脅威アクターは、最初は正体が確認されていないため、Larva から管理を開始します。追加情報を確保して正体が明確になると、該当する Arthropod に結びつけます。
- **情報の歪曲防止:** 本システムは、情報に信頼度(Confidence)と加重値(Weight)を付与し、情報の信頼性を評価・管理します。
- **脅威アクターの変化の反映:** Larva と Arthropod 間の柔軟な結びつきを通して、脅威アクターの変化を持続的に追跡します。
- **複数の脅威アクターの関与を考慮:** 一つの Operation または Campaign に複数の脅威アクターが同時に関与する可能性を認めます。
- **脅威インテリジェンス・フレームワークの適用:** MITRE ATT&CK、Lockheed Martin Cyber Kill Chain、Diamond Model of Intrusion Analysis などのサイバー脅威インテリジェンス(CTI)フレームワークを参照し、分析システムを構築します。

5. 結び

アンラボが確立した脅威行為および脅威アクター分類システムは、正確性、柔軟性、信頼性に基づいています。これにより、組織がサイバー脅威の複雑さを理解し、変化する脅威環境に迅速に対応できるようにサポートします。本システムを通じて、脅威アクターの活動を綿密に追跡し、より効果的な対応戦略を策定できるものと期待しています。今後アンラボは、この分類システムを持続的に改善・発展させ、より高精度で信頼できる脅威インテリジェンスを提供する計画です。

AhnLab

東京都港区芝4丁目13-2 田町フロントビル3階 〒108-0014
URL: www.ahnlab.com / jp Mail: jp.sales@ahnlab.com
Tel: 03-6453-8315