NET TANKEN LAB / RESEARCH REPORT

中国サイバー作戦 エコシステム

MISSION-001｜対日APT活動の歴史的構造と技術的特徴

調査対象：2020年より前に確認・報告・公表された、中国または中国系脅威アクターとの関連が指摘される対日APT活動。

編集方針：原報告書の主要な分析・事例・留保を保持し、読者向けに文章を再構成した要約編集版です。元PDFの文字欠落がある箇所は逐語復元せず、明瞭に確認できる情報のみを採用しています。

01 調査の目的と判断基準

本調査は、2019年12月31日までに活動が観測・報告された対日APT事案を中核に置き、2020年以降の政府発表・起訴・共同アドバイザリは、過去の活動を補強する証拠として区別して扱います。

中心的な観察は、中国に関連すると評価された対日サイバー活動が、単一の組織モデルでは説明できないことです。情報機関と民間企業の結び付き、軍部隊との関連が評価された活動、国家目的と金銭目的が混在する活動が並存しています。

■ 確認事実 インシデント対応、解析、起訴資料などから直接確認できる事象。

■ 政府評価 政府機関が公に示した帰属・評価。

■ 民間評価 セキュリティ企業・研究者による追跡・クラスタリング。

■ 状況証拠 標的選定、言語、活動時間、インフラなどの間接的な手掛かり。

■ 仮説・未確認 説明可能性はあるが、直接証拠がない、または公開資料で検証できない事項。

02 主要アクターの位置付け

■ APT10 / menuPass 日本を含むMSP顧客への侵害が焦点。米司法省の2018年起訴では、MSS天津市国家安全局、Huaying Haitai、個人ハッカーとの関係が具体的に主張されました。

■ Tick / BRONZE BUTLER 日本固有ソフトの脆弱性悪用など、対日特化が際立ちます。日本政府・警察は2021年、人民解放軍61419部隊との関係が高い可能性を評価しました。

■ BlackTech 2018〜2019年に日本でTSCookie、PLEAD、IconDownなどが観測され、後年の日米等の政府資料で中国政府関連アクターとして扱われました。

■ APT41 / Winnti関連 国家支援型の諜報と金銭目的活動が並行すると評価された例。Winnti全体をAPT41と同一視することは避けます。

■ APT16・APT17・APT12・Tonto Team 対日活動との接点はありますが、具体的な政府部署や個人への帰属の強度はそれぞれ異なります。

■ Icefog・Blue Termite 対日活動は重要ですが、中国国家機関との直接的な帰属根拠は弱く、比較対象として慎重に扱います。

03 対日活動の主な時系列

■ 2009〜2013年 IXESHE/APT12系、Icefog、Emdivi系などが東アジアや日本の組織を標的に活動。

■ 2013〜2015年 三四郎・一太郎など日本市場に特有のソフトウェアを狙う脆弱性悪用が観測されました。APT17による更新経路やDNS操作も重要です。

■ 2015〜2017年 Tickによる日本向け攻撃が拡大。2016年からSKYSEA Client ViewのCVE-2016-7836を未公開段階で悪用したと報告されています。

■ 2016〜2018年 APT10のOperation Cloud Hopper関連で、MSPを侵害して顧客環境へ展開するモデルが問題となりました。

■ 2018〜2019年 BlackTechの国内観測が継続。2018年には日本政府がAPT10による長期・広範な攻撃を非難しました。

04 技術的特徴：標的は日本の業務環境

特に重要なのは、日本国内で導入されるソフトウェアの事前研究です。三四郎（CVE-2014-0810）、一太郎（CVE-2013-5990、CVE-2014-7247）、SKYSEA Client View（CVE-2016-7836）が例に挙がります。

こうした攻撃は、無差別な脆弱性探索だけでは説明しにくく、日本市場・日本語環境・導入製品を調べた上での作戦を示唆します。一方、同一CVEの利用だけで別々の攻撃者を同一組織とみなすことはできません。

05 共通基盤と供給網への侵入

APT10によるMSP経由の横展開、APT17の更新サーバやDNS操作、BlackTechによるASUS WebStorage更新機能の悪用、Winnti/APT41関連のコード署名証明書やソフトウェア供給網への侵入は、信頼された中間経路が攻撃対象になることを示します。

共通するのは、最終標的を直接攻撃する代わりに、管理者権限、更新経路、委託先との信頼関係を利用する発想です。ただし、共通の指令系統が存在することを示す証拠とは区別します。

06 代表的な技術・ツール

■ APT10 ChChes、RedLeaves、PlugX、Poison Ivy、盗難認証情報、MSP経由の横展開。

■ Tick Daserf、Datper、NodeRAT、Mimikatz、PsExec、scheduled task、MS17-010関連の横展開。

■ BlackTech TSCookie、PLEAD、IconDown、更新機能の悪用。

■ APT17 Agtid、PlugX、McRAT、Htran、DNS・更新経路の操作。

■ Blue Termite Emdivi、認証情報収集、圧縮・持ち出し。

PlugX、Mimikatz、PsExecなどは複数の攻撃者が利用するため、ツールの一致だけで国家帰属や組織同一性を判断することはできません。

07 帰属評価の注意点

APT10は米司法省の起訴資料が人物・法人・政府部署の関係を具体的に示した重要例ですが、起訴上の主張と有罪認定は異なります。TickのPLA61419との関係は日本政府の評価に基づきます。BlackTechの国家関連評価は、2018〜2019年当時の公開技術観測と、後年の政府評価を分けて扱います。

中国語文字列、活動時間、中国所在IP、マルウェアやCVEの共有はいずれも補助的証拠です。外注、偽装、共有ツール、インフラの再利用など別の説明があり得ます。

08 2020年以降につながるエコシステム

APT10の天津MSSと民間企業、APT41関連のChengdu 404、APT40関連の海南MSSと企業、さらに2025年のi-Soon事件は、国家需要側と民間実行側が結び付く複数のモデルを比較する材料になります。

分析上は、①国家需要側、②実行・請負側、③能力供給側（ゼロデイやマルウェア等）、④アクセス供給側（侵害済みサイト、MSP、更新経路、盗難認証情報等）の四層に分けられます。ただし、この四層が一つの統合市場として機能していたという説明は仮説です。

09 次の調査で追跡すべき論点

■ 人物・法人の特定 TickとPLA61419を結ぶ公開チェーン、BlackTechの具体的な部署・人物の追跡。

■ 技術クラスタの再検証 日本のWinnti観測とAPT41の重なり、APT12/IXESHEの対応範囲。

■ 脆弱性供給網 一太郎CVE-2014-7247などの複数アクター間での近接利用と、開発者・仲介者の関係。

■ 帰属の保留 Blue Termite、Icefog、LODEINFOなどを、中国国家関連活動と短絡的に結び付けない検証。

■ 日本の被害範囲 個別組織名が非公開の事案について、業種・時期・侵入経路の一次資料を補完。

編集注記・原資料

本版は、提供された「中国サイバー作戦エコシステム MISSION-001 調査報告」（18ページ）を基にした読みやすさ優先の再編集版です。原資料にある詳細年表、全アクター別TTP表、IOC、参考文献一覧を網羅した完全復刻ではありません。元PDFには文字欠落が確認されるため、引用や正式公開には元原稿との照合を推奨します。