サイバーレスキュー隊（J-CRAT）活動状況
[2021 年度下半期]

2022 年 7 月 15 日

サイバーレスキュー隊（J-CRAT）では、主に国家支援型（ステートスポンサード、ネイションバックド）[1]とされる攻撃者によるサイバー活動（標的型サイバー攻撃）、特にサイバーエスピオナージに対して、相談対応、レスキュー活動、公開情報の収集及びサイバースレットインテリジェンスの活用等を通じた情報収集等を行っている。

2021 年度下半期及び本活動状況報告の発出にいたる期間を通じたサイバー状況把握の結果、国際情勢の急激な変化の最中においても、我が国に対するサイバーエスピオナージは手口や標的を大きく変えることなく継続していることを確認している。また、ロシアによるウクライナ侵攻に際しては、破壊的・物理的なサイバー攻撃やサイバーエスピオナージが観測されると同時に、当隊でも以前より注視してきた国家的意志を背景としたと目されるサイバー空間上の情報活動（偽情報、インフルエンスオペレーション、マスキロフカ（情報偽装工作）など認知領域における活動）も、サイバー空間に関係する新たな脅威として注目を集めており、国家支援型のサイバー活動の一部としてサイバー状況把握に必要な領域であることが再認識された。

本活動報告で紹介するサイバー状況の報告が、我が国そして各組織及び個人に対する国家支援型サイバー活動に対する理解の一助となり、即応を目的とした情報の利活用に加え、中長期的な対抗策としての政府による利活用を前提とした情報共有の推進、ひいては我が国一丸となったサイバーセキュリティ活動の形成につながることを望む。

1　活動結果

年度毎の「標的型サイバー攻撃特別相談窓口」に対して寄せられた相談や情報提供の件数、緊急を要する事案に対してレスキュー支援を行った件数及びオンサイトでの支援件数を表 1 に示す。

表 1 J-CRAT 支援件数の推移

	2018 年度	2019 年度	2020 年度	2021 年度
相談・情報提供	413	392	406	375
リモートレスキュー	127	139	102	94
オンサイトレスキュー	31	20	17	9

※中長期に渡る 1 つの事案に対して複数回のオンサイト対応を要した場合も、1 件として集計

2021 年度に「標的型サイバー攻撃特別相談窓口」に対して寄せられた**相談・情報提供**は **375 件**であった。このうち、**リモートレスキュー支援**へ移行したものは **94 件**、うち**オンサイト支援**を行った事案数は **9 件**であった。

2　2021 年度下半期の活動を通じてみられた特徴的な事項

当隊では、脅威情報を認知領域や物理領域といったマルチドメインで複合的に把握することや、攻撃の背景を窺うに値する地政学的傾向、近隣諸国や同盟国、有志国の動向を重要視している。本項では、2021 年度下半期を中心に、当隊活動を通して把握した国家支援型サイバー活動のうち、特にサイバーエスピオ

[1] 公開情報などによれば、実際の活動は外国の軍及び情報機関、宣伝機関が直接、または下請のハッカー（Hack-For-Hire）や犯罪者（政府放任型サイバー犯罪グループ）を介して行われるとされる。

ナージを中心に特徴をいくつか特徴を述べる。

2.1 資源・エネルギー部門等を標的としたと目される攻撃活動

2022 年 4 月より、国内の資源・エネルギー部門に関係する組織や研究者、メディア関係者等を標的とする新たな攻撃を観測している。初期侵害の手口である標的型攻撃メールには、標的とされた人物の関係組織を装い、実在するイベントへの招待を打診する内容に不審ファイルへのリンクが記載された丁寧な文面が用いられた。リンク先に設置されたマルウェアは未知のダウンローダーであり、セキュリティベンダの報告[2]によると、このマルウェアは 2022 年 3 月に公開されたばかりの Go 言語バージョンで作成されている。

本攻撃キャンペーンの特徴を整理すると、丁寧なメール文面、独自のマルウェア開発、多段階の感染フローといった要素が抽出される。これらは、以前から散発的に観測されてきた、ある攻撃グループの攻撃（2020 年度上半期の活動状況報告 2.3 項で述べた攻撃等） と重複する部分が大きい。また、通信インフラの追跡調査から、一連の攻撃活動は遅くとも 2021 年 9 月頃には開始されており、国際・安全保障部門も標的としていたことが示唆されている。当隊では攻撃活動の更なる拡大を警戒すると同時に全容の把握に努めており、皆様からの情報提供にも期待している。些細と思われる情報であっても、是非当隊へ御連絡いただきたい。

2.2 安全保障、国際政治、外交、メディアを標的としたと目される攻撃活動

LODEINFO と呼ばれる諜報用マルウェアを用いた攻撃が 2019 年 12 月以来継続しており、本報告期間中も、従来の標的とされる分野（安全保障、国際政治、外交、メディア）に対する標的型攻撃メールが観測され続けた。攻撃メールは組織／個人のメールアドレスを問わず送付されており、入念にカスタマイズされた文面を信じて、マルウェアの同梱された添付ファイルを開いてしまうケースが後を絶たない。

マルウェア感染へ誘導する具体的な手口に新規性は無く、無害なメールによる事前のやり取りや、標的の所属するコミュニティでしか知り得ないイベント情報等をメールの題材に用いるなどして標的の信用を得たうえで悪意あるメールを送りつける、といった標的型攻撃メールに典型的な騙しの技法が使い続けられている。

本報告期間に見られた特徴として、悪意あるメールが送付される数週間～数カ月も前に無害なメールが送られていたケースが複数見られた点を挙げる。無害メールの内容は自己紹介や時候の挨拶であり、その送信元メールアドレスは後の悪意あるメール送付にも使用された。期間を空けて無害メールが送付された目的が、例えばメール到達性のチェックなのか、返信等のリアクションから信頼度を計るためなのか定かでは無いが、背景には攻撃の成功率を高めるための長期的な計画があることが示唆され、まさに高度な持続的脅威（Advanced Persistent Threat; 通称 APT）と言えるだろう。

2.3 中国国内の日本企業従業員を標的としたと目される攻撃活動

2021 年 10 月から 11 月にかけて、オンラインの無料ウイルス判定サービス上に、中国国内の日本企業従業員を狙ったとみられるマルウェアファイル群がアップロードされた。ファイル名は簡体字（主に中華人民共和国で使用されている中国語の字体）で、賃金や監査に関する資料を装った文書ファイルである。当隊にてこれらを調査したところ、2018 年から 2020 年にかけて BlackTech が日本国内の組織を攻撃した際に使用した検体の属性値と複数の一致が見られた。2021 年 7 月には日本企業の中国拠点に対して BlackTech によるとみられる攻撃が観測されたという状況も踏まえて、本報告期間にも同様の攻撃が行われたものと推定する。

なお、中国の大手セキュリティベンダ系列の企業が同じマルウェアファイルに対する解析報告をブログで公開している[3]。中国のサイバーセキュリティ業界では、2018 年頃より BlackTech を”黑凤梨” または“T-

[2] ショートカットと ISO ファイルを悪用する攻撃キャンペーン
https://security.macnica.co.jp/blog/2022/05/iso.html

[3] 瑞星：BlackTech 组织对国内企业 APT 攻击分析
http://it.rising.com.cn/anquan/19843.html

APT-03”などと呼称し、その標的は中国を含む東アジア一帯と解説されている。これらの主張に関しては帰属の曖昧化を図った情報戦の試みである可能性も排除せず、各国のセキュリティベンダ等がどのような記事を発信するのか、その方向性にも目を向けている。

2.4 潜在の懸念される A41APT による侵害

セキュリティベンダの報告によると[4] [5]、少なくとも本報告期間の中頃（2021 年 12 月頃）まで攻撃が続いていたとされている。正規の Web サービスと同じポートで通信するリスニング型のバックドアが新たに投入され、アクセスログからの検知が困難とのことから、かつての Winnti マルウェア感染のような長期感染に気が付けていない被害組織が潜在していることを懸念している。

A41APT の従来の侵入手口は、インターネット境界に設置された機器の脆弱性を突く「ネットワーク貫通型」とよばれる手法が使われていると報告されており、主に海外拠点などのセキュリティ対策が不十分な組織を入口として、組織全体へ侵害を拡大（横移動、ラテラルムーブメント）していくものとされている。そのような事例に心当たりのある組織においては、サイバーエスピオナージに係るサイバー状況把握のため、不完全な情報や、古い情報でも構わないので当隊との情報共有に是非御協力をいただき、国のサイバー状況把握の一助にご協力いただきたい。

2.5 中小企業の従業員に対するソーシャルエンジニアリング

2021 年後半に国内の先端技術情報を扱う中小企業の従業員を標的としたソーシャルエンジニアリングが行われたことを観測した。当該従業員の私的な SNS アカウントに対して好待遇の求人情報をもちかけて、最終的に諜報用マルウェアに感染させようとする手口から、Lazarus によるとされる「Operation DreamJob」攻撃キャンペーンの一環であると推測している。

類似の事案は 2020 年中頃に国内の大手製造業でも存在したといわれているが、今期の事例のように機微な情報を扱う企業であればその規模を問わず標的となり得るという点で、国内の先端技術情報を扱う事業者においては、技術情報窃取のリスクへの認識を新たにする必要があると考える。

なお、本件を踏まえ、組織が取るべき対策としては、①従業員が私的に利用する SNS に関しても、SNS 上で経歴、所属企業、肩書き、職務内容、他者との関係を外部公開しない等の内容を含むガイドライン等を定めること、②SNS を通じた求職活動、いわゆる「ソーシャルリクルーティング」を装ったサイバー諜報活動という手口が存在することを、セキュリティ研修等を通じて定期的に周知し、注意喚起を実施すること等が考えられる。

2.6 国内の北朝鮮有識者を標的としたと目される諜報活動

2022 年 2 月、国内の北朝鮮有識者に対する、北朝鮮による日本人拉致問題をテーマとした標的型攻撃メールを観測した。メール本文は、国内の北朝鮮問題関係組織を詐称してアンケートへの回答を依頼する内容で、本文中に記載された URL リンクから正規 Web メールサービスを通して悪意ある文書ファイルがダウンロードされる手口が用いられた。

本攻撃の痕跡情報を公開情報と照合すると、同時期に韓国のセキュリティベンダのブログ [6]で公開された韓国メディアの職員に対する標的型攻撃の特徴とも一致したことから、地域・言語を問わず北朝鮮問題の関係者個人を狙う攻撃キャンペーンの一環であると考えられる。これまでに観測された我が国組織／個人への攻撃範囲は限られているものの、周辺国への攻撃動向にも注意を払い、警戒を続ける必要があると考える。

---

[4] 「Earth Tengshe」によるマルウェア「SigLoader」を用いた攻撃キャンペーンで観測された新たなペイロード
https://blog.trendmicro.co.jp/archives/29842

[5] 標的型攻撃の実態と対策アプローチ 第 6 版 日本を狙うサイバーエスピオナージの動向 2021 年度
https://www.macnica.co.jp/business/security/2022/report_02.html

[6] 워드문서 이용한 APT 공격 시도 (External 연결 + VBA 매크로)
https://asec.ahnlab.com/ko/30980/

3 我が国を取り巻くサイバー攻撃グループ

本項では、我が国周辺国を中心に、本報告期間の情報収集を通じてみられた国家支援型サイバー活動として報じられている情報の中から特徴的な動向の一部を紹介する。公開情報として報告されている攻撃グループの属性を地域毎に分類したこれらの脅威情報は、日本国内への影響度を判断してリスク管理、危機管理につなげていくべきと考えている。直接の影響が少ないと思える脅威情報であっても、現地法人や海外支店などの海外拠点が被害に巻き込まれるだけでなく、それらを介して国内まで侵害を受ける可能性は考慮すべきと考える。

3.1 中国に関係するサイバー攻撃グループ

国内外における中国の関与が疑われるサイバー諜報活動に目を向けると、APT41（WINNTI）、APT10、Mustang Panda、Tonto といった旧知の攻撃グループから新たに識別された攻撃グループまで幅広く報告されている。ここでは、ウクライナ侵攻に関係した活動及びその他の特筆すべき活動について抽出して述べる。

ロシアによるウクライナ侵攻開始（2022 年 2 月）と時期を同じくして、Mustang Panda が欧州諸国（ロシアを含む）の組織に対し、EU やウクライナ政府の公式文書を偽装したファイルを用いたフィッシングメール攻撃を行ったとするセキュリティベンダの報告がある[7]。同攻撃グループについては、遅くとも 2020 年以降、継続的に欧州の外交機関を標的とした活動を継続しており、侵攻の勃発によりその活動が活発化したとの見方もある [8]。Mustang Panda についてはセキュリティベンダ各社から様々なレポートが公開されており、複数の言語圏にまたがる攻撃グループとされているため、その活動が日本へ直接、または間接的に及ばないか注視している。その他、2022 年 3 月にウクライナ政府機関（CERT-UA）が警告を発した[9]不審な文書ファイルについて、米国のセキュリティベンダが中国に関連する攻撃グループによるものと判断するブログを公開している[10]。

2021 年 12 月に公表された Java のゼロデイ脆弱性 Log4Shell は、サイバークライム・サイバーエスピオナージを問わず世界中の攻撃グループに使用され、その影響も世界に及んだ。セキュリティベンダのブログによると[11]、APT41 は遅くとも 2021 年 5 月以降に米国州政府等を標的にインターネット境界の脆弱性を悪用した様々な攻撃を仕掛け続けていたところ、Log4Shell が公表されるとその数時間後にはこれを悪用して政府機関や重要産業部門を新たに侵害したと報じられている。近年、こうした「ネットワーク貫通型」攻撃を初動とする APT は増えており、標的型攻撃メールと比較して事案の把握が難しいだけでなく、その実態を被害組織が認識するのが困難であり、また認識されたものを当隊と共有する機会も少ないことは、サイバー状況把握を確実に実行していくための課題だと考えている。

2021 年 11 月、台湾の金融機関や証券会社に対するデータ窃取及びクレデンシャルスタッフィング攻撃が行われ、不正取引に起因してオンライン取引が停止する事件が発生した。セキュリティベンダの報告によると[12]、攻撃に使用された通信インフラの一部は、数年前の APT10 の活動と疑われる攻撃のものと同一であり、その他複数の攻撃手口（TTPs）の一致から APT10 の関与が疑われている。但し本件は、当隊の把握している国内組織に対する APT10 の初動 TTPs や被害者像とは異なる部分が大きいため、帰属については慎重な判断が必要と考える。攻撃の目的についても、金銭的動機なのか、あるいは台湾金融業界

---

[7] Mustang Panda deploys a new wave of malware targeting Europe
http://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html

[8] The Good, the Bad, and the Web Bug: TA416 Increases Operational Tempo Against European Governments as Conflict in Ukraine Escalates
https://www.proofpoint.com/jp/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european

[9] Кібератака групи UAC-0026 з використанням шкідливої програми HeaderTip (CERT-UA#4244)
https://cert.gov.ua/article/38097

[10] Chinese Threat Actor Scarab Targeting Ukraine
https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/

[11] Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments
https://www.mandiant.com/resources/apt41-us-state-governments

[12] Operation Cache Panda - Chinese APT10 Targets Taiwan
https://cyware.com/news/operation-cache-panda-chinese-apt10-targets-taiwan-9619edf7

の信用を失墜させることなのか、現段階での判断は難いため今後の状況把握が必要となる。

その他、ガバメントマルウェアを用いた治安活動を実施しているとも言われている LuoYu と呼ばれる攻撃グループが新たに識別されている[13]。報告によると、国内組織の中国拠点や中国国内の組織を標的としてサイバー諜報活動を展開しており、2021 年 4 月以降に活動が観測されている。初期侵入の手口の一つとして、正規ツールのアップデーターを通じたマルウェア感染が疑われており、攻撃者はインターネット経路上の機器にアクセス可能な存在と疑われる点には注意が必要である。このような、他国の治安に関するサイバー活動に対して、当隊がどのような立場で、どのように言及すべきかは新しい課題であり、脅威認識の共有という観点でも新たな時代の到来を感じさせるものである。

その他、中国が関係するディスインフォメーションに関しては、2021 年 12 月に開催された民主主義サミット等を標的にした活動についてのレポートが公開されている[14]。レポートによると、中国のプロパガンダエコシステムは、ニュース配信、学術レポート配信、パネルディスカッションの開催、漫画・動画の公開、SNS への投稿と拡散、海外メディアや外国人インフルエンサー等との提携等で構成されており、英語圏の視聴者を対象とした影響力工作が展開されたと主張されている。また、このような国家を背景とするソーシャルネット空間の工作活動として、日本語を用いることで標的国家に対し間接的な情報操作が行われているとする情報もある。サイバー空間の脅威認識として、このような活動も注視する必要性が高まっていると判断している。

3.2 ロシアに関係するサイバー攻撃グループ

当隊では本報告期間中、ロシアに関係するサイバー攻撃グループによる、国内での明らかなサイバー諜報活動を示唆する公開情報は把握していない。我が国を含む地域を対象とした活動としては、2021 年以降に APT29 が欧州、北米南米及びアジアの外交組織に対して大規模なフィッシングキャンペーンを継続的に実施しているとするセキュリティベンダのブログが公開されているが[15]、我が国へ直接実施されたとする公開情報には触れていない。

一方、ロシア軍によるウクライナ侵攻に伴い、ウクライナ及び NATO 加盟国に対する活動は活発化している。CERT-UA によると、侵攻直前の 1 月に数十件の政府系 Web サイトが侵害を受けて、改ざんや破壊の被害を受けたとされる[16]。さらに、1 月から 2 月にかけて、ウクライナ政府、軍、金融機関に対する DDoS が行われ、侵攻直前のタイミングで行われたウクライナの衛星インターネット網への攻撃は欧州全域のシステムに影響を及ぼしたとされている[17]。米国、EU、英国及びその同盟国はこれらの攻撃についてロシア政府が関与しているとして非難声明を出している[18]。軍事侵攻の開始後も、ウクライナ政府やメディア部門に対する破壊活動とデータ窃取作戦、原子力部門に対するデータ窃取作戦が続き、これらの作戦に関与した攻撃グループとして、GRU の配下とされる APT28、Sandworm 及び未定義のグループが挙げられている[17]。

影響力工作の観点では、軍事侵攻の開始前に、米国、英国当局側がロシアによる軍事侵攻と偽旗作戦を警告し、ロシア当局側は偽情報と否定する応酬が見られた。侵攻に際して生じた民間人の被害に関しては、ロシア当局は概ね一貫してウクライナ軍側に責任があるとする一方的な主張を展開し、軍事侵攻についてはウクライナ国内の一部市民を守るための特別な軍事作戦であるとの正当化を繰り返した。侵攻をロ

---

[13] LuoYu: 新型 WinDealer を用いた日本を狙う 2021 年のスパイ活動
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_7_leon-niwa-ishimaru_jp.pdf

[14] China's Narrative War on Democracy – Recorded Future Report
https://www.recordedfuture.com/chinas-narrative-war-democracy/

[15] Trello From the Other Side: Tracking APT29 Phishing Campaigns
https://www.mandiant.com/resources/tracking-apt29-phishing-campaigns

[16] Фрагмент дослідження кібератак 14.01.2022
https://cert.gov.ua/article/18101

[17] Special Report: Ukraine　An overview of Russia's cyberattack activity in Ukraine
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[18] Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion
https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion

シアが正当化する根拠の一つとも考えられる、ウクライナ生物研究所への米国の関与に関する偽情報を分析した公開情報によると[19]、2022 年 1 月以降、ソーシャルネットワーク、ロシア国内のブログサイト、ロシア国営 TV のドキュメンタリー番組、他国のジャーナリストの発言、主に米国向けの陰謀論の投稿サイト等を通じて、米国が生物兵器を製造しているとの偽情報が配信され続けたとされている。ロシア国内の世論を統制する動きとしては、2022 年 3 月、ロシア政府はロシア軍に関する偽情報を広めた場合の罰則を定めた法案を成立させている[20]。

ハクティビストグループの活動については、Killnet と呼ばれる親ロシアのグループが、西側諸国の政府機関、インフラ施設に対する DDoS 攻撃を活発に繰り返しているとの報道が続いている。ウクライナの支援、ロシア制裁の立場を表明した組織は、ロシア政府に属する攻撃者やハクティビスト、ロシア国内に基盤を持つと考えられるランサムウェア攻撃グループなどから将来的に報復を受けるリスクが考えられる[21]。現時点で日本の組織、企業に対する攻撃報告には接していないが、この先攻撃対象とされる可能性を否定することはできない。ファイブアイズ各国の情報機関からロシア政府に属する攻撃者やハクティビストの攻撃を緩和するためのアドバイザリが発行されているので参考にしていただきたい[22]。

日本企業も被害に遭っているランサムウェア攻撃グループ Conti は、ウクライナ侵攻の支持表明とその撤回、それに伴う内部対立と情報リークを引き起こした結果、2022 年 5 月に解散することを表明したが、グループの名前を変えて活動は継続するものと考えられている[23]。リークされた情報からは Conti の上層部とロシア連邦保安庁（FSB）の間に何らかの関係があったことが示唆されており[24]、攻撃者グループの保護（活動の黙認）の見返りとして、所属を隠した代理攻撃者として活動する、あるいは情報を融通しあうといった何らかの互助関係があった可能性も指摘されている。

また、ロシアを中心に集団安全保障条約（CSTO）を構成する国におけるサイバー連携や、サイバー活動の帰属を報じるものもあり、特に 2022 年 5 月には CSTO 設立 20 周年を迎えたことや、ロシアも参加している多国間協力組織である上海協力機構（CSO）の活動動向など関連する国際関係に関する情勢把握や関係性への注視も、国家支援型サイバー活動の把握においては必要であると感じられる。

3.3 北朝鮮に関係するサイバー攻撃グループ

当隊では、2.5 項で述べたように Lazarus に関係するとみられる攻撃グループの国内を対象とした活動（Operation DreamJob）を観測している。この活動に関しては複数のセキュリベンダからも報告されており[25][26][27]、国や地域を問わず、防衛、メディア、IT、化学といった部門に属する企業の従業員が標的とされている。個人の SNS を介して悪意ある文書ファイルを送り込むという侵害の手口に大きな変化は見られないが、セキュリティソフトに検出されにくい独自のツールの開発・使用が続いているとみられる。国連安保理北朝鮮制裁委員会専門家パネルの報告書によると、北朝鮮が極超音速滑空機の設計資料等の兵器開

---

[19] Russian State-Sponsored Amplification of Bio Lab Disinformation Amid War in Ukraine
https://www.recordedfuture.com/russian-state-sponsored-amplification-bio-lab-disinformation-amid-war-ukraine/

[20] 外国メディアの活動停止拡大 ロシア「偽情報」処罰法で
https://www.jiji.com/jc/article?k=2022030600335&g=int

[21] Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation
https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation

[22] Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

[23] DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape

[24] Conti Leaks: Examining the Panama Papers of Ransomware
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html

[25] Countering threats from North Korea
https://blog.google/threat-analysis-group/countering-threats-north-korea/

[26] Lazarus Targets Chemical Sector
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical

[27] New Malware of Lazarus Threat Actor Group Exploiting INITECH Process
https://asec.ahnlab.com/en/33801/

発に必要な技術情報をサイバー攻撃により入手していることが指摘されており[28][29]、Lazarus によるこれらの分野を標的とした活動は今後も継続するものと考えられる。なお、国内の宇宙・防衛産業の中には、標的となり得る先端技術開発を行う中小企業も少なくない。不審なソーシャルリクルーティングが見られた場合は、是非当隊まで情報提供いただきたい。

Kimsuky の関与が疑われる活動は、セキュリティベンダより繰り返し報告されている [30][31][32][33]。主に外交、安全保障、国際関係部門が標的とされ、スピアフィッシングメールを介して独自のマルウェアを展開する手口は従来通りである。

2020 年頃を境に、攻撃ツールや攻撃に関わる通信インフラが北朝鮮へと帰属される攻撃例を報じる記事が増加傾向にある。被害はセンセーショナルに報道されるが、その後の具体的な調査がなされていないような事例があれば、帰属の追及の観点で見直しをかけることも検討し、サイバー状況把握を高める必要があると判断している。

3.4 その他リージョンに関係するサイバー攻撃グループ

本項で紹介する事例は、当隊の注目したトピックの一部である。これらのリージョンで活動する日本企業は直接、または間接的に影響を受ける可能性がありうる。各地における脅威認識のあり方や、参考情報などをお持ちであれば、是非当隊との意見交換などを通じてサイバー状況把握に協力頂きたい。

3.4.1 イラン

イランが関与するとみられる APT 攻撃グループとして、少なくとも APT35、MuddyWater、TA456 の活動が報告されている。当隊が特に着目したイベントとして、2022 年 1 月、米国サイバーコマンドは、自身のニュースサイトを通して MuddyWater をイランの公的な諜報機関である情報省（MOIS）の下部組織であると公言している[34]。続く 2 月には、米国 CISA の警告として MuddyWater をイラン政府の支援を受けた（Iranian government-sponsored）APT 攻撃グループと表現したうえで、攻撃緩和策のアドバイザリを公開している[35]。同報告によると、MuddyWater は 2018 年頃より MOIS の活動を支援し、窃取したデータは政府に提供するとともに、他の攻撃グループと共有できる立ち位置にあるとされている。

3.4.2 インド

インドが関与するとみられる APT 攻撃グループとして、少なくとも Patchwork（別称 Viceroy Tiger, Hangover, White Elephant, 等）、SideWinder の活動が報告されている。

2021 年 11 月頃より行われた Patchwork の活動では、パキスタンの分子医学や生科学の研究を行う大学の研究者が標的とされたと報じられており[36]、同攻撃グループによる研究者を標的とする活動の観測は初とされている。

---

[28] 北、サイバー攻撃で極超音速ミサイルの技術窃取か…国連パネル指摘
https://www.yomiuri.co.jp/world/20220403-OYT1T50024

[29] S/2022/132 - Security Council Report
https://undocs.org/S/2022/132

[30] 병·의료원 건강검진 증명서 발급으로 위장한 北 연계공격 등장
https://blog.alyac.co.kr/4536

[31] 2021 년 김수키 그룹은 어떻게 움직였나
https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=31442

[32] North Korea-related Hangul Word Processor (HWP) File Being Distributed
https://asec.ahnlab.com/en/30324/

[33] North Korean attackers use malicious blogs to deliver malware to high-profile South Korean targets
http://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html

[34] Iranian intel cyber suite of malware uses open source tools
https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/

[35] Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a

[36] Patchwork APT caught in its own web
https://blog.malwarebytes.com/threat-intelligence/2022/01/patchwork-apt-caught-in-its-own-web/

SideWinder は 2020 年 4 月以降、パキスタン、バングラデシュ及びその他の南アジア地域を対象に、従来標的としてきた軍事、法執行機関だけでなく、新たに航空や IT といった先端産業部門等へと活動を拡大している可能性があるとの発表資料がある[37]。

3.4.3 パキスタン

パキスタンが関与するとみられる APT 攻撃グループ APT36（別称 Mythic Leopard, Transparent Tribe）は、2021 年 6 月以降、インドの安全保障及び軍関係者を標的とする継続的な活動を実施していると報じられており[38]、直近の変化として、攻撃手口として、正規組織やファイル共有サービスの偽装 Web サイトを使用し、ソーシャルエンジニアリングに注力している点が挙げられている。

3.4.4 ベトナム

ベトナムが関与するとされる攻撃グループ Ocean Lotus（APT32）は、2012 年頃より近隣諸国や米国等を標的として活動しているとされている。本報告期間中、西側諸国のセキュリティベンダ等からの、同グループの活動に関する公開情報は確認していない。

2021 年 6 月に公表された英国の民間研究機関が公表したレポートによると[39]、APT32 を政府に結び付いたグループとし、比較的高度なサイバー攻撃を開始する可能性があると評価されている。

3.4.5 中南米

El Machete は、主に中南米で活動しているスペイン語話者の APT 攻撃グループとされている。セキュリティベンダのレポートによると[40]、同グループは 2010 年頃より、ニカラグア、ベネズエラの、政府、金融部門を主な標的として活動している。2022 年 3 月にはニカラグアの金融機関を狙い、ロシアによるウクライナ侵攻をテーマとするスピアフィッシングメール攻撃を展開したと報じられている。

4 活動を通しての所感

中国湖北省武漢市を発端とした新型コロナウイルスの蔓延に伴うロックダウンやウクライナ侵攻勃発の混乱にも左右されず、我が国に対する国家支援型と推定されるサイバー活動は継続的に発生している。このような長期にわたる持続的な脅威の継続の背後には国家自身、または国家的な支援（ステートスポンサード）があると考えられており、当隊はその状況把握に努めてきた。その際、適正な対策にもつながるためにも、サイバーセキュリティの観点だけでなく、攻撃主体の目的や意図に対する見解の理解を得るべく、相手の行動原理、動機、技術力、組織構造の把握、さらには安全保障や国際関係など地政学や社会的歴史、民俗学にいたるまで情報収集に努めている。

例えば、中国武漢市は、2017 年頃より「国家网络安全人才」（国家的サイバーセキュリティ人材）を育成するための基地建設を開始し[41]、産業・教育・防衛・政府、各々のセクターが共同で環境の整備を進めてきた。2021 年 12 月には、サイバーセキュリティ人材育成の教育モデルが確立したとされ、第二弾以降の研究開発・産業化計画も公表されている[42]。この一連の流れで創設された組織・施設の地理的関係、人の流れ、出資企業の部門、教育カリキュラム、セキュリティイベントの内容等を収集整理していくと、中国のサイバーエコシステムの輪郭が見えてくるだろう。

---

[37] SideWinder Uncoils to Strike
https://www.blackhat.com/asia-22/briefings/schedule/#sidewinder-uncoils-to-strike-26513

[38] Transparent Tribe campaign uses new bespoke malware to target Indian government officials
https://blog.talosintelligence.com/2022/03/transparent-tribe-new-campaign.html

[39] CYBER CAPABILITIES AND NATIONAL POWER: A Net Assessment
https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-three

[40] State-sponsored Attack Groups Capitalise on Russia Ukraine War for Cyber Espionage
https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

[41] 市人民政府关于支持国家网络安全人才与创新基地发展若干政策的通知 2017-03-03 11:27
http://czj.wuhan.gov.cn/FBJD/ZCWJ/GFWJ/202004/t20200424_1122744.html

[42] 武漢投資環境の概要 概要五大産業拠点
http://japanese.wuhan.gov.cn/wh_rywz09_2021/wh_rywz091_2021/202112/t20211201_1864050.shtml

他方、こうしたサイバー活動の様々な痕跡を、ナレッジとして蓄積・分析することで 2 項に述べたような攻撃グループの活動の把握につなげていくことがサイバー状況把握において重要である。分析を重ねると、攻撃グループ間に共通する特定のローダーや通信インフラ等が見つかることがあり、攻撃組織間の関係やインフラ基盤の存在把握にまで発展できることもある。

当隊としては、サイバー空間における安心・安全実現の観点において、国家支援型と推測されるサイバーエスピオナージへの対応に加え、その関連領域としての認知領域作戦、国家放任型と推測されるサイバークライム活動の概況を含めた幅広い脅威情報の収集、情報提供などの活動を引き続き進めていくことで、国家レベルでのサイバー空間における状況把握（サイバードメインアウェアネス[43]）を高めることに努めていく所存である。

関係者の皆様には本稿をご活用いただくとともに、当隊の活動改善のためのご指摘やご教示をいただければ幸甚である。

サイバーレスキュー隊（J-CRAT）活動状況［2021 年度下半期］
https://www.ipa.go.jp/security/J-CRAT/index.html

2022 年 7 月 15 日
独立行政法人情報処理推進機構

https://www.ipa.go.jp/

[43] サイバー状況把握を意味する用語として Cyber Situational Awareness も用いられているが、当隊ではサイバー空間およびサイバー空間と関わる物理空間、認知空間における事象の把握という観点から Cyber "Domain" Awareness と表記する。なお Domain Awareness には海洋の Maritime、宇宙の Space といった概念も存在する。