サイバーレスキュー隊（J-CRAT） 活動状況
[2020 年度下半期]

2021 年 6 月 25 日

サイバーレスキュー隊（J-CRAT）では、主にステートスポンサード（国家支援型）[1]とされる攻撃者による標的型サイバー攻撃、特にサイバーエスピオナージに関する相談受付、レスキュー活動、及び情報収集を行っている。

本報告の期間における当隊の活動、当隊への情報共有、公開情報の収集、サイバースレットインテリジェンスの活用等によるサイバー状況把握等から、攻撃の把握が比較的困難なネットワーク貫通型攻撃の拡大と、従来国内では報告の少なかったステートスポンサードの活発化、といった情勢の変化が認められており、既成概念にとらわれず柔軟な対応が求められている。

本活動報告で紹介するサイバー状況の報告が、各組織及び個人に対するサイバー諜報活動に対する理解の一助となり、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促進、ひいてはわ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

	2017 年度	2018 年度	2019 年度	2020 年度
相談・情報提供	412	413	392	406
リモートレスキュー	144	127	139	102
オンサイトレスキュー	27	31	20	17

※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

今年度に「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 **406 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 **102 件**、うち**オンサイト支援**を行った事案数は **17 件**であった。

2　2020 年度下半期の活動を通じてみられた特徴的な事項

2.1　2019 年 12 月から観測され始めた標的型攻撃メールの連鎖が継続

本報告期間も、2019 年 12 月中旬から観測されている LODEINFO と呼ばれる諜報用マルウェアを用いた攻撃が継続している。標的とされる分野に変化はなく、安全保障、国際政治、外交、メディアに関係する人物に対する標的型攻撃メールが観測され続けている。侵害を受けた人物のメールアドレスを踏み台として、新たな攻撃対象へ標的型攻撃メールが送付されるケースと推定されるものもあり、攻撃の連鎖が断ち切れていない状況である。

[1] State-Sponsored: ネイションバックド（Nation-Backed）と呼ばれることもある。実際の活動は、敵対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）を介して行われるとされる。

本攻撃に関して新たに判明した攻撃手口のバリエーションとして、メールのやり取りを続けて最終的にマルウェアが送付される手法もみられている。具体的には、最初に送付される標的型攻撃メールでは関係者を装った日程調整、原稿の評価、取材の依頼といったテーマの無害なメールが送付され、攻撃対象が返信した場合は資料と称して不正なマクロを含むオフィスファイルが送付される、といった流れである。

やり取り型とも呼ばれるこの手口は従来の標的型攻撃メールの典型的なパターンの一つであり、攻撃対象を信用させたうえでマルウェアを送り付けるため、攻撃の成功率が高まる傾向があると考えられる。今期に観測されたやり取り型のメール文面には、過去に APT10 とされる攻撃グループが用いた文書構成や言い回しがそのまま流用されている箇所がみられている。この点は、今回の攻撃グループが APT10 に関する情報要求や、サイバー諜報活動における過去の資源（文面など）を利用可能な組織であることを強く示唆している。

マルウェア LODEINFO には機能の大幅な変更はみられないものの、細かなバージョンアップが続いており、セキュリティ対策ソフトウェアによるリアルタイム検出をすり抜ける可能性が考えられる。標的となり得る組織、個人においては、不審なファイルに接する機会を減らし（フリーメールや送信元詐称メールの識別、添付ファイルのプレビュー制限等）、不審なファイルを開いた際のアプリケーションからの注意（コンテンツ有効化の確認）に気を払い、セキュリティ対策ソフトウェアの最新の定義ファイルによるフルスキャンを定期的に行うことが、被害拡大の防止策の一つになり得ると考える。

2.2 新たなネットワーク貫通型の攻撃オペレーションの発覚

本報告期間の初頭、国内の複数の企業を標的とした侵害事案の情報提供を受けた。その後公開されたリサーチャやセキュリティベンダの情報[2][3][4]によると、2019 年 3 月頃より、企業の海外拠点における SSL-VPN 製品から侵入されたものと報告されている。特徴として、侵入後に設置されたバックドアには攻撃グループのオリジナルと思われる未知のマルウェアが使用されていたこと、バックドアは正規の実行ファイルから多段階の呼出し処理を経て起動する仕組みであったこと、侵害活動後にイベントログの削除といった痕跡消去が行われていたことが挙げられるため、検出が難しいとされている。攻撃グループの帰属に関しては、複数の攻撃手口（TTPs）の類似性、及び同時に発見されたマルウェアの種別等から、APT10 並びに BlackTech と呼ばれる攻撃グループの関与が指摘されている。

当隊へもいくつかの情報提供はあったが、攻撃の全体像を把握するには判断材料が不足している状況である。攻撃対象となり得る組織との更なる情報共有体制の構築を行い、サイバー状況把握と有効な対策の助言を行えるよう努めていく。

また、本オペレーションにおける着目点の一つとして、標的型攻撃メールが侵入経路として使われたという情報は得られていない。当隊では、ネットワーク貫通型と呼称する、ネットワーク境界に設置された装置からの侵入であると分類している。

攻撃側の視点で考えると、標的型攻撃メール攻撃を行う場合、標的とする組織や個人のメールアドレスを入手することで実行可能となり、ピンポイントの攻撃が比較的容易である。一方で、ネットワーク貫通型攻撃を行う場合、侵入の可否は標的組織の使用するネットワーク製品の種類、アカウント設定不備の有無、及び脆弱性対策の状況等に依存する。よって、標的組織は予め厳密に指定されているわけではなく、偵察段階で侵入可能な組織をリストアップしたうえで、情報要求に関連する分野の企業や組織（例えば防衛、航空宇宙、製造技術、政治経済、等）との照合を行い、複数の標的組織が選定されているとも考えられる。

従って、ある組織に対するネットワーク貫通型攻撃が観測された場合、その組織の属する分野はもとより、

---

[2] A41APT case
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_jp.pdf

[3] Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage

[4] APT10：A41APT の活動内で発見された高度なマルチレイヤー型ローダー「Ecipekac」
https://blog.kaspersky.co.jp/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/30393/

さまざまな組織に対する攻撃が既に広範囲に行われているとみなして警戒する必要があると考えられる。類似の事例として、過去にみられたBlackTechによるネットワーク貫通型攻撃では、全国で数十もの関係組織が同時期に標的とされた事案もある。ネットワーク貫通型攻撃は分野横断的に行われるという特性を各組織が理解し、攻撃情報の迅速な共有網を構築することは、有効な対抗策の一つとなり得るだろう。

なお、情報共有にあたっては、暫定的・戦術的な対応として利活用可能な痕跡情報（IOCs）だけではなく、中長期的に、戦略的に利活用可能な各種痕跡、メタデータを意識し、可能な限り「あるがまま」の情報を共有していくことが重要であり、わが国の情報共有体制の発展における課題でもあると考えている。

2.3 北朝鮮に関係した複数の攻撃オペレーション

2020 年 11 月に、北朝鮮内のイベントや脱北者をテーマに用いた不審ファイルが観測された。事案対応より得られた特徴を公開情報と照合すると、脱北者やその支援団体をテーマとする同種の攻撃は遅くとも2020 年 3 月頃よりみられており、この攻撃を北朝鮮に紐づく攻撃グループに関連付けるセキュリティベンダの報告 [5] もある。北朝鮮に紐づく攻撃グループの呼称と分類については諸説ある中で、脱北者、人権団体、朝鮮半島の統一に関わる組織・個人の情報収集を目的とするグループもあるとされている。

この攻撃の経路は特徴的であり、水飲み場攻撃に近い手口が用いられたとみている。攻撃者は、北朝鮮関係の情報を扱うサイトに類似するドメインを作成し、その Web ページ上にニュースサイトのコンテンツを流用するなどしたコンテンツを作成し、北朝鮮情勢に興味関心を持つ人物を誘導して不審ファイルをダウンロードさせたと考えられる。一般的な”水飲み場攻撃”は正規 Web サイトが侵害されて不正なリダイレクトやダウンロードが行われる攻撃を意味するのに対し、本事案では攻撃者が作成したとみられる Web ページが用いられた点が異なる。攻撃者は、標的とする人物が Web ページへアクセスするようになったことを確認したうえで、マルウェアを設置したとも考えられる。

さらに、上述の攻撃と同時期より、わが国の安全保障や北朝鮮関係の有識者に対する執拗なフィッシングメールが継続的に観測されている。フィッシングメールのテーマには、プロバイダからの各種通知（アカウントの変更連絡、アカウントロックの警告、新サービスの提案等）が用いられ、メール本文中には偽のアカウント／パスワード入力ページへのリンクが記載されている。この手口は広く一般に拡散しているフィッシングメールと全く同じであるため、サイバー諜報活動かどうかの見極めが難しいケースであるが、攻撃に用いられたインフラの照合から、前節で述べた不審ファイルを用いた攻撃と同じ攻撃グループによるものである可能性が高いと判断している。また、フィッシングに用いられたドメインの追跡調査からは、日本及び韓国を中心とする複数のプロバイダを偽装した名称が発見されていることから、両国の有識者を狙った攻撃が潜んでいるものとみて、当攻撃活動の観測を継続している。

その他、公開情報によると、北朝鮮に紐づく攻撃グループによる日本の組織を狙った攻撃が行われたとされており[6]、独自のマルウェアが複数使用されていること、国内向けの偽装サイトが用意されていることといった特徴がみられる。当隊はこの攻撃に関する事案を直接扱っていないが、マルウェアの調査や他の情報ソースとの突合せから、遅くとも 2020 年 7 月以前より攻撃が行われていたとみて、関連情報の収集に努めている。

これらの攻撃で使われたツールやインフラは、サイバースレットインテリジェンスの観点より、特定国からのステートスポンサード攻撃と推察可能なものもあるが、サイバー以外も含めた情報活動全体の把握が困難であるため、現時点での判断は難しいと考えている。

---

[5] Kimsuky が利用している KGH スパイウェアスイートの内部解析
https://www.cybereason.co.jp/blog/cyberattack/5373/

[6] 日本の組織を狙った攻撃グループ Lazarus による攻撃オペレーション
https://blogs.jpcert.or.jp/ja/2021/03/Lazarus_malware3.html

3　わが国を取り巻くサイバー攻撃グループ

当隊では、わが国に対するサイバーエスピオナージにつながる恐れのある攻撃グループの動向を把握することを重要と考え、ステートスポンサードとされるさまざまな攻撃グループの情報を集めてサイバー状況把握へ活用することを検討している。本項では今期にみられた特徴的な動向の一部を紹介する。

3.1　中国に関係するサイバー攻撃グループ

当隊では、2.1 項及び 2.2 項で述べたように、APT10、BlackTech に関係すると考えられる攻撃グループの国内活動の観測を継続している。その他、公開情報によると、HAFNIUM と呼ばれる攻撃グループによるネットワーク貫通型攻撃を使った、主に米国に対する攻撃が報告されている。

2021 年 3 月、米国の大手ソフトウェア会社は HAFNIUM と呼称される未知の攻撃グループによる、グループウェア製品に対するゼロデイ攻撃を公表した[7]。攻撃は 2021 年 1 月より開始され、医療、教育、防衛、政策、NGO、その他多数の分野が標的となったとされている。HAFNIUM は、攻撃の手口と被害組織の特徴から、中国のステートスポンサードと評価されている。また、翌週に公開された他社の公開情報[8]によると、本攻撃で使用された脆弱性（CVE-2021-26855 他）の更新プログラムが公表された前後のタイミングで、Tick、Tonto、Winnti Group（APT41）を含む複数の攻撃グループが一斉に、全世界のサーバに対する脆弱性スキャンを行ったとされている。

2020 年 4 月、警視庁は、国内組織に対するサイバー攻撃に関与したとして、中国共産党員で、国営の情報通信企業でシステムエンジニアをしていた男を書類送検したと報道された[9]。攻撃の手口から、中国人民解放軍の 61419 部隊の配下にある”Tick”と呼ばれる攻撃グループが関与したとされている。本報道に対し、中国外交部は定例記者会見を通じて『サイバー空間は仮想性が強く、追跡が難しく、関係者は多様である。サイバーインシデントの調査と評価は十分な証拠に基づいて行うべきであり、不当な推測を行うべきでない』との見解を述べた[10]。同様の見解は、上述の HAFNIUM に関しても述べられている。

3.2　ロシアに関係するサイバー攻撃グループ

当隊では、本報告期間中に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サイバー諜報活動像を把握していない。一方、公開情報によると、今期も APT28 系列及び APT29 系列とされる攻撃者グループの国外活動が公表されている。

2021 年 4 月、米国政府は英国とともに、2020 年に発覚した SolarWinds 社の IT 監視・管理ツールを悪用した攻撃をロシア対外情報庁によるものと正式に発表し、サイバー活動を支援したとされるロシアの組織及び個人に制裁を行った[11]。この攻撃は、2020 年 3 月に開始され、SolarWinds 社製品のアップデートを通じたサプライチェーン攻撃により、米国政府機関や大手 IT 企業を含む最大で 18,000 件が影響を受けたとされている。侵害が発覚したのは 2020 年 12 月であり、長期に渡り攻撃を受け続けていた可能性が考えられる。一方で、ロシア政府は本件への関与を繰り返し否定している。

その他、2020 年を通じて、APT28 が全世界の政府関係組織、防衛産業を標的として、ブルートフォース

---

[7] HAFNIUM targeting Exchange Servers with 0-day exploits
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

[8] Exchange servers under siege from at least 10 APT groups
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

[9] JAXA 攻撃「背景に中国軍」 警察庁長官が初めて言及
https://www.asahi.com/articles/ASP4Q5WXZP4QUTIL012.html

[10] 2021 年 4 月 20 日外交部发言人汪文斌主持例行记者会
https://www.fmprc.gov.cn/web/fyrbt_673021/jzhsl_673025/t1870105.shtml

[11] Treasury Sanctions Russia with Sweeping New Sanctions Authority
https://home.treasury.gov/news/press-releases/jy0127

攻撃とシンプルな標的型攻撃メールによる攻撃を仕掛けているとの報告もある[12]。

なお、本報告期間には、米国の大統領選、英国の欧州連合離脱、中国湖北省武漢市を発端とした新型コロナウイルスによる被害拡大などのトピックスに対し、ロシアによる情報窃取活動や情報操作（インフルエンスオペレーション、認知領域活動）が報じられた。これらの平時、またはグレーゾーン事態におけるロシアの活動は一般に「ハイブリッド戦」ともよばれ、これからのサイバー空間の使われ方において重要な理解となるため、日本に対する攻撃を明確に把握できない中でも、どのような活動が、どのように実施され、どのように報じられたか把握する必要があると考える。

3.3 北朝鮮に関係するサイバー攻撃グループ

北朝鮮に関係するとされる活動については、主に Kimsuky (Belvet Chollima, Thallium, 他) と呼ばれるグループ、Lazarus(HiddenCobra, Labyrinth Chollima, ZINC, 他) と呼ばれるグループの活動が報告されている。

Kimsuky による韓国を標的とした攻撃は遅くとも 2013 年頃より継続しているとされており、今期も 2020 年 11 月から 2021 年 2 月にかけて、米国大統領選や北朝鮮の党大会に関するテーマの標的型攻撃メールの存在が報告されている[13]。

2021 年 1 月、世界中のセキュリティ研究者やセキュリティ企業の従業員に対し、同業者等を装い SNS でのやり取りを介してマルウェアに感染させようとする攻撃が観測されたと報告された [14]。防衛産業の職員に対する接触の報告も継続しており、標的の嗜好を意識したサイバー空間での接触（ソーシャルエンジニアリング）が拡大傾向にあると考えられる。

2021 年 2 月、米国司法省は北朝鮮の偵察総局（RGB）に関係するとされる 3 名を起訴した[15]。起訴状によると、2014 年のソニーピクチャーズに対する攻撃から、2020 年 9 月までの金融関係組織への不正アクセス、WannaCry の開発、暗号通貨関係の不正アプリといった幅広い活動が対象となっている。これらの活動は、起訴対象の 3 名及び特定できていない他のハッカーにより実行されたとされている。また、これらの活動を行った組織は起訴状に含まれる IOCs から Lazarus グループを指すものと考えられる。

4 活動を通しての所感

APT10 を始めとする中国に帰属するとみられる攻撃グループの活動が、手口の大きな変化無しに継続していることから、現在行われている連鎖的な標的型攻撃メールとネットワーク貫通型攻撃をもって、攻撃者の目的が達成されている状況となっていることを危惧している。

また、今期に扱ったネットワーク貫通型攻撃の事案は、何れも侵害を受けて相当の時間が経過した後に発覚したケースである。攻撃の発見という観点では、標的型攻撃メールの痕跡は攻撃の成否に関わらずメールという目に見え易い形で残るのに対し、ネットワーク貫通型攻撃の初期の侵入痕跡は主にネットワーク機器や Web サーバ上に設置される Webshell 等のバックドアであるため、検出を逃れた場合は目につきにくい。また、もし検出できた場合でも、Webshell は様々なサイバー犯罪に用いられるため、サイバー諜報活動によるものか否かの判断が難しいことから、侵害の発覚していないケースや、侵害事案がサイバー諜報活動と認識されていないケースが相当数あると考えられる。

---

[12] Pawn Storm's Lack of Sophistication as a Strategy
https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html

[13] 탈륨 조직, 통일부 월간북한동향 문서 사칭 공격 수행
https://blog.alyac.co.kr/3601

[14] ZINC attacks against security researchers
https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/

[15] Indicted - Department of Justice
https://www.justice.gov/usao-cdca/press-release/file/1367721/download

手口によらず、一度侵害を受けた組織は、リモートログイン用の認証情報を窃取された後に正規の認証情報を使用されて繰り返し侵害を受けるケースもある。この場合、攻撃者はバックドアを使用せずに侵害活動を行うことで検出を逃れることが多く、EDR 製品等の内部対策で検出できない限り、発覚が遅れるケースが多い。

これらの問題や、本報告の 2.1 項、2.2 項で述べた攻撃とその対策については、2021 年 5 月に公開されたセキュリティベンダのレポート[16]でも言及されている。マクロ機能の組織内統制によるマルウェア実行の抑止、EDR 製品の監視対象外となる不審なリモート接続端末の検出、Forensic State Analysis (FSA) を用いた侵害調査を通したセキュリティレベルの底上げ、といった対策観点は、当隊も賛同するところである。

FSA とは、エンドポイント上のある瞬間の状態を収集・分析し、侵害の痕跡を洗い出す調査である。具体的には、自動起動設定、プログラムの設置場所・実行履歴、レジストリ、プロセスツリー情報等を収集し、異常を発見していく。EDR に代表される行動分析と比較すると潜在的なバックドアの検出に優れており、侵害を受けている可能性を前提に、予防的に実施されることもある。

自組織の採用しているセキュリティシステムの特長を改めて理解し、その弱点を補完する施策が考えられているかを見直すことが、根本的な対策強化となり得るだろう。

以下、従来の報告からの繰り返しとなるが、ステートスポンサード、ネイションバックドといわれるサイバー領域における敵対的活動に対抗していくためには、各組織がインシデント対応と脅威情報の共有ネットワークを成熟させるとともに、政府関係機関との連携力を強化し、わが国としての対応力を高めていくことが必要不可欠である。そしてその先に、ナショナルサイバーセキュリティの観点で、そのような活動の痕跡を収集して共有し、同盟国・有志国と連携して様々な手段と能力を活用できるよう、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)を高めることが重要であると考えている。

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、ソーシャルネットワーク等を使用する他国からのインフルエンスオペレーションについても、標的型サイバー攻撃対策の関連領域として、幅広く脅威情報の収集などの活動を引き続き進めていく。

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。

[16] 標的型攻撃の実態と対策アプローチ 第 5 版
https://www.macnica.net/pdf/mpressioncss_ta_report_2020_5.pdf