サイバーレスキュー隊（J-CRAT） 活動状況
[2020 年度上半期]

2020 年 12 月 1 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、レスキュー活動、及び情報収集を行っている。本報告の期間において、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を実施したところ、件数としての増加傾向は見られていない。しかし攻撃の手口は、従来多用された標的型攻撃メール（スピアフィッシングメール）だけでなく、攻撃把握の比較的困難なネットワーク貫通型へシフトしている可能性や、当隊との情報共有の接点が確立できていない特定セグメントが被害を受けている可能性があることを考慮する必要がある。

多様化するステートスポンサードとされるサイバー攻撃に対抗するためには、個々の組織による戦術的な活動を共有して積み重ね、またそれをオペレーショナルに、そして戦略的に活用することで、わが国一丸となったサイバーセキュリティ活動を形成していくことが重要であり、当隊は各組織の情報共有を支援すべく幅広い活動を行っている。

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、ひいてはわが国におけるサイバーセキュリティの一助となることを望む。

1　活動結果

本報告の期間に、「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 上期
相談・情報提供	412	413	392	205
リモートレスキュー	144	127	139	45
オンサイトレスキュー	27	31	20	5

※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

「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・情報提供件数**は **205 件**であった。このうち、**レスキュー支援**へ移行したものは **45 件**、うち**オンサイト支援**を行った事案数は **5 件**であった。

2　2020 年度上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攻撃キャンペーンの継続

2019 年下期の活動レポートでも紹介したが、2019 年 12 月中旬から観測されていた LODEINFO と呼ばれる諜報用マルウェアを用いた攻撃を、2020 年 8 月まで断続的に確認している。攻撃は、安全保障、外交、メディアに関係する人物へのスピアフィッシングメールが中心であり、標的とされた分野や初期侵入の手口に大きな変化は見られなかった。マルウェアの構造は段階的に変化しており、画面キャプチャ機能やキーロ

[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、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。

ガー機能が追加された他に、悪意あるコードの一部をテキストデータの保存サイトから読み込む方式も見られた。

これまでの事案対応から得られた侵入痕跡の調査を進めたところ、攻撃者は対象のコンピュータ環境を調査したのち、個人のプライベート環境であれば認証情報の窃取とドキュメントファイルの収集をコマンドの手入力で行い、組織環境であれば認証システムの侵害から横展開（ラテラルムーブ）を行うなど、攻撃対象の状況把握を実施した上で具体的な行動を選択していることが確認された。このように侵入後の行動にはある程度規則性がみられることから、攻撃者は明確な目的を持ち、作業マニュアルを準備して組織活動している可能性が垣間見える。

コマンドが手入力されているが故に、スピアフィッシングメールの添付ファイルからマルウェアに感染した場合、攻撃者に侵入されてからデータが外部へ転送されるまでには相応の時間がかかることがある。また、近年の傾向に違わず、攻撃者の指令環境（C2 サーバ）が通信可能にある状態はごく短時間であり、一日に数回程度しか攻撃活動が行われない状況も確認している。

視点を変えれば、標的型攻撃メールの添付ファイルやリンクを介して不審なドキュメント（デコイファイル）を開いた場合の初動対応として、マクロの起動やボタン押下など不自然な指示が書かれている、添付ファイルの内容がメールに沿わない、不自然な日本語、または白紙や読めない文字の羅列であるといった不審点に気が付き、直ちにネットワークから切り離すことができれば、情報の窃取を水際で阻止することに一定の効果がある。

2.2 インターネットを介して内部システムへ接続する装置に対する侵入事例

当隊ではこれまで「ネットワーク貫通型」攻撃と呼称して、SSL VPN 製品や Web サーバなどネットワーク境界に接する機器に対し、脆弱性や設定不備を悪用して侵入したり、何らかの方法で得た認証情報（ユーザー名とパスワードなど）を使って不正アクセスしたりする手口を、スピアフィッシングメールやソーシャルエンジニアリングとは異なるサイバーエスピオナージにおける初期侵入の脅威として注意を促してきた。

本報告の期間において、従来様々な業種への攻撃を行ってきた既知の攻撃グループが、国内企業の海外拠点に設置された SSL VPN 製品の既知の脆弱性を突いて侵入し、遠隔操作機能を持つ未知のバックドアが設置された攻撃の事例を確認している。バックドアは侵入時点ではウイルス対策ソフトの検知を逃れていたこと、正規プログラムの一部に紛れ込み DLL ハイジャッキングで起動するよう設置されていたことから、初期段階での発見は困難だったと思われる。

この攻撃グループによるネットワーク貫通型攻撃は遅くとも 2017 年頃より行われているとされており、セキュリティ施策の比較的甘い海外拠点から侵入する手口も継続的に確認していることから、初期侵入の手口として今後も注意が必要である。

ネットワーク貫通型攻撃の対策としては、従来の繰り返しとなるが、自組織でインターネットに公開している製品やサービスを、海外拠点を含めて漏れなく把握し、最新のパッチを適用することで、攻撃者を利する状態を回避するといった基本的な予防策を続けることや、ログイン情報が窃取されることを前提に多要素認証、多段階認証、アクセス元制限などを導入する、侵入を前提に自組織のネットワークセグメントを分割する等して重要情報へのアクセスを防止するといった技術的な対策が求められる。また、「自組織の認証という仕掛け（シングルサインオン、認証連携など）がどのような状態にあるかを適切に把握する」といった運用上の見直しも、当隊の事案対応ではしばしば助言の中心となっている。

上述の事案とは別に、日本固有の資産管理ソフトウェアの脆弱性が突かれて数年前に侵入されていた事案の対応において、諜報用マルウェアが対策パッチの公開前に設置されていたことが判明している。このようなゼロデイ攻撃成功の可能性を考慮すると、緊急や重大な脆弱性の場合は、パッチを適用するだけでなく、脆弱性の悪用され始めた時期に遡って不審な通信の有無を確認する等の対策を合わせて行う運用も検討いただきたい。

2.3 国際問題の関係者を狙ったとみられる攻撃

安全保障や国際問題、外交問題を扱う組織に所属する研究者をピンポイントで狙った標的型攻撃メールが複数観測された。メールの内容は、実在するメディアを騙り何らかの資料と称してマルウェア付きドキュメントを送るという、過去の攻撃でも繰り返し使われてきた手口である。特徴としては、未知のマルウェアが使用されたこと、マルウェアは多段階のダウンロードを繰り返して最終的に諜報用マルウェアに感染させる仕組みであることが挙げられる。

メールの文体やマルウェア種別が 2.1 項、2.2 項に報告した攻撃と異なることから、当隊ではこれらとは別の攻撃グループによるものと推測しているが、判断にはより多くの事例が必要である。

2.4 ソーシャルネットワークなどサイバードメインにおける人間関係を悪用した攻撃

主に仕事の関係を構築することに利用されるソーシャルネットワークの場をもちいて、攻撃対象へ侵入する攻撃 Operation DreamJob [2]、Operation In(ter)ception [3], Operation North Star [4] がセキュリティベンダより公開された。

公開情報によると、このオペレーションの主な標的は韓国・米国に関係する航空宇宙産業と防衛産業であり、標的とする従業員に対するメールまたは SNS を介して厚遇の求人情報を持ちかけてコンタクトし、最終的に情報収集を目的としたマルウェアに感染させる手口を使用する。マルウェアの特性から、北朝鮮に帰属する攻撃グループが関係するとされている。

攻撃者が SNS を用いて情報収集を行うことを踏まえると、真の標的とされた人物の SNS 上に関係者として表示される人物も、攻撃の連鎖を成功させるために標的とされることも想定される。上述の重要産業に属する日本人が攻撃対象となる可能性は十分に考えられる。

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することは、攻撃者のサイバー偵察活動を支援する結果となることがある。組織が取るべき対策としては、個人利用の SNS に関してもガイドラインを定めること、攻撃者からサイバー偵察や接触を受ける危険性を含めて周知することが求められる。その他のリスクの観点から、自組織のセキュリティインシデントが発生した際に、インシデント対応状況、ネットワーク構成やサイバーセキュリティ関連の情報を個人利用の SNS から漏洩させないための社内規定などが有効となるケースも考えられる。

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。本項では今期に見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

当隊では少なくとも BlackTech、及び LODEINFO マルウェアを使用する攻撃グループの国内活動を本報告の期間内に観測した。その他、APT31、APT41、及び MustangPanda 等と呼ばれる攻撃グループによる台湾や香港、ASEAN 諸国等に対する活動がセキュリティベンダ等から報告されている。

米国司法省は 2020 年 9 月に APT41 のメンバーとみられる中国人 5 名のハッカーと、APT41 に協力したとされるマレーシア人 2 名を起訴した。起訴状によると、米国、台湾、日本を含む 100 以上の組織及び個人

---

[2] Operation ‘Dream Job’ Widespread North Korean Espionage Campaign
https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf

[3] Operation In(ter)ception: Aerospace and military companies in the crosshairs of cyberspies
https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/

[4] Operation (노스 스타) North Star A Job Offer That’s Too Good to be True?
https://mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/

にサイバー攻撃を行ったとされている。起訴されたうち 3 名は、中国国内に存在する企業の幹部とみられており、その表向きの業務は侵入テスト、攻撃の監視、マルウェアの検出といった一般的なセキュリティベンダのものとされている。中国の攻撃グループの実態は軍・政府機関からサイバーエスピオナージを委託された請負会社であるという主張は前々から存在したが、今回の起訴状はその裏付けを追加するものと言える。

また、9 月に公表されたセキュリティベンダのレポートによると、2020 年 3 月以降、米国大統領選挙に関係する組織に対して APT31 による数千件の攻撃が検出され、約 150 件の侵害が発生したと報告されている [5]。

なお、7 月には米国の戦略国際問題研究所（CSIS）から、日本に対する中国共産党のインフルエンスオペレーション（印象操作や偽情報による情報操作など）に関するレポートが公開されている [6]。日本では現状サイバー空間を使ったそのような脅威についての情報が比較的少ないが、サイバーセキュリティの視点においても、サイバー空間における脅威として今後このような認知領域や物理領域の脅威を複合的に扱う、マルチドメインオペレーションが重要となるであろう。

3.2 ロシアに関係するサイバー攻撃グループ

公開情報によると、ロシア連邦軍参謀本部情報総局（GRU）に関係するとされる Sandworm、ロシア連邦保安庁（FSB）やロシア対外情報庁（SVR）に関係するとされる Gamaredon Group、所属不明の Energetic Bear による活動等が各国でみられている。

2020 年 5 月に、米国国家安全保障局(NSA)は Sandworm によるメールサーバの脆弱性を突いた攻撃の注意喚起を行い[7]、8 月には米国国務省が、ロシア政府の偽情報作戦を担う 7 つの組織に関するレポートを公表し、COVID-19 に関する偽情報の拡散が行われたと指摘している[8]。10 月には Sandworm のメンバーとみられるロシア人 6 名が米国司法省に起訴されており、欧州の政府機関・政党への攻撃、NotPetya を用いた破壊行為、2018 年平昌冬季オリンピックに関する攻撃を行ったとされている。

9 月に公表されたセキュリティベンダのレポートによると、2020 年 3 月から 9 月の期間に、米国大統領選挙に関係する、米国、欧州の 200 以上の組織に対して APT28 による攻撃が行われたと報告されている[5]。

10 月に英国政府は、GRU が東京オリンピック・パラリンピックの関係者に対するサイバー偵察を実施したと公表している。サイバーキルチェーンにおける偵察とは標的組織へ侵入するための偵察行為であり、公開された組織や個人の情報から標的型攻撃メールを送る標的を定めたり、標的組織のサーバに脆弱性が無いかを調査したりする行為が含まれる。

なお、2020 年 8 月以降、日本を含む世界各地の企業に対し、Fancy Bear (APT28)、Cozy Bear (APT29) を名乗る攻撃者が、「金銭を支払わなければ DDoS 攻撃を行う」という趣旨の脅迫文を送りつけ、実際に DDoS 攻撃を行う事例が増加傾向にあるが、実際の攻撃者は APT28、APT29 を騙る別グループと考えられている。本報告の期間中に、当隊でも本件に関する複数の相談や情報提供を受け付けている。

3.3 北朝鮮に関係するサイバー攻撃グループ

2019 年 9 月から 2020 年 8 月頃にかけて、APT37 と呼ばれるグループによる、各国の防衛・航空宇宙関

---

[5] New cyberattacks targeting U.S. elections
https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/

[6] China's Influence in Japan
https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200722_Stewart_GEC_FINAL_v2%20UPDATED.pdf

[7] Exim Mail Transfer Agent Actively Exploited by Russian GRU Cyber Actors
https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2196511/exim-mail-transfer-agent-actively-exploited-by-russian-gru-cyber-actors/About-Us/EEO-Diversity/Employee-Resource-Groups/

[8] GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem
https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

連企業を狙ったサイバーエスピオナージオペレーションが報告されている。

また、北朝鮮のステートスポンサードとされる攻撃グループの一部は、破壊工作やエスピオナージだけでなく、金銭目的の活動も行っているのが特徴の一つである。米国政府は 2020 年 8 月に、BeagleBoyz と呼ばれる攻撃グループが、2020 年 2 月以降に日本を含む数十ヵ国の ATM を狙った攻撃を仕掛けていると報告している[9]。

攻撃グループやマルウェアに対する各セキュリティベンダの呼称は様々であり、情報収集活動においては公開レポートに記載された別称などを頼りに関係を整理する必要がある。また、攻撃グループのスポンサーとされる軍、情報機関といった構図を整理するためには、サイバー領域以外の知見からの解釈と相違がないか確認するといった多面的な理解が必要となる。サイバーセキュリティのコンテキストにおいて、収集すべき情報量は今後ますます増えていくと考えている。

4 活動を通しての所感

ステートスポンサードとされる攻撃グループによるサイバー空間における活動は、従来のセキュリティ対策では侵入時の活動が検知され難く、活動後に痕跡を消去することがあるため、攻撃を受けたことに気づけないケースや、侵入から数か月～数年が経過した後になって外部機関からの通報やウイルス定義ファイルの更新のタイミング等を契機に発覚するケースも多々ある。当隊の活動においても、現在進行中の攻撃に対処する他に、数か月以上前に攻撃を受けて既に攻撃者が立ち去ったとみられる組織の攻撃痕跡を調査し、影響範囲の推定や以後の対策に関する助言を行うケースがあり、2.2 項や 2.3 項に挙げた事例の一部もこれに該当する。

当隊の主な活動は、標的型サイバー攻撃を受けた組織の初動対応支援であり、レスキュー支援を通じて標的型サイバー攻撃の理解を深めていただくとともに、後々の調査や根本対策に役立てるための、セキュリティインシデント対応全般への助言を行っている。その他、サイバーエスピオナージに該当するか分からないメールや痕跡情報を情報共有いただき、当隊の知見と照合することや、サイバーエスピオナージの被害に不安を持つ組織に対しての簡易的な調査を行いその結果をお伝えすることも活動範囲としている。

これらの活動の根幹として、当隊自身の事案対応を通じて情報共有いただいたインディケータ情報はもちろんの事、セキュリティベンダやリサーチャが公開しているインディケータ情報やマルウェア解析事例、最新のマルウェア動向等を収集し続けている。その中でも、現在進行中の事案から得られる鮮度の高い情報は、注意喚起への活用の点や、攻撃者の活動目的や帰属の推定材料を多く得られる点からも特に貴重であるため、インシデント発生時から情報共有していただける組織を増やしていくことが大切と考えている。一方で、攻撃を受けて一定期間が経った後の情報であっても、サイバー状況把握の視点では極めて重要であることに変わりはない。

これまでに当隊とコンタクトできていないセグメントの組織や、初動対応から根本対策まで自組織で完結できる力を持つため当隊を必要としないと考えている組織においても、上述の視点で当隊を活用できる可能性があれば、有事・平時にかかわらず当隊へ一度ご相談いただきたい。

サイバー攻撃グループの動向把握の視点では、本報告の期間では過去と比較し、他国政府やセキュリティベンダから、中国、ロシア、北朝鮮、イラン、ベトナム、インド、パキスタンに帰属するとされるサイバー攻撃グループに関する注意喚起、起訴状、活動に関するレポートが多数公表されたと感じている。

3 項でも述べたように、公開情報はその存在を把握し、確実な収集と格納を行い、将来的な分析の基礎情報とする必要がある。また、その真偽判断の材料として、サイバー領域以外の知見についても同様に把握、収集、格納、分析といったサイクルを行う必要があると考えている。

---

[9] FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks
https://us-cert.cisa.gov/ncas/alerts/aa20-239a

以前より繰り返し述べているように、ステートスポンサードの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報連相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ていくことで、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脅威状況把握を高めることが重要であろう。

そのためには、今現在だけでなく過去に遡って把握されていない攻撃を発見すること、推定される攻撃者像については国内のみならず海外での活動まで追跡すること、及び攻撃の理由を推察するために国際情勢や地政学的な背景情報を蓄積することも必要となるだろう。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進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。

本報告は、その内容に関する有用性、正確性、知的財産権の不侵害等の一切について、執筆者及び執筆者が所属する組織が如何なる保証をするものでもありません。また、本資料の読者が、本資料内の情報の利用によって損害を被った場合も、執筆者及び執筆者が所属する組織が如何なる責任を負うものでもありません。