サイバーレスキュー隊（J-CRAT） 活動状況
[2019 年度下半期]

2020 年 6 月 24 日

1　活動結果

2019 年 4 月～2020 年 3 月に、「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

	2016 年度	2017 年度	2018 年度	2019 年度
相談件数	519	412	413	392
レスキュー支援数	123	144	127	139
オンサイト支援数	17	27	31	20

※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**相談件数**は **392 件**であった。このうち、**レスキュー支援**へ移行したものは **139 件**、うち**オンサイト支援**を行った事案数は **20 件**であった。

オンサイト支援においては、被害組織が長期間の侵害を受けていた攻撃痕跡に気づき、果敢にも当隊へ情報提供や相談をいただけたことで、攻撃活動の全容を共有し、わが国へのサイバーエスピオナージ（サイバー諜報活動）を把握するうえで貴重な知見を得ることができた事例が複数あった。

2　2019 年度下半期の活動を通じてみられた特徴的な事項など

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）とみられる攻撃者によるサイバーエスピオナージに対する相談やレスキュー活動、情報収集を行っている。本活動報告で紹介するサイバーエスピオナージの状況が、わが国、各組織、及び各個人におけるセキュリティ対策への手がかりとなることを望む。

2.1　12 月から観測され始めた攻撃キャンペーン

2019 年 12 月中旬から下旬にかけて、外交政策や安全保障政策、経済政策といった分野、特に米中関係の問題を扱う組織や人物に対する標的型攻撃メールによるサイバーエスピオナージを確認した。攻撃メールのテーマには、時候の挨拶、年末の事務処理、会議やフォーラムへの申し込みといった受信者にとって日常的に添付ファイルつきメールとして受信し易い事柄が用いられ、添付されたドキュメントファイルのマクロを有効化すると未知のマルウェアに感染する仕組みとなっていた。プライベート利用の端末が感染し、メールやブラウザ情報（ID やパスワード）を窃取されたうえで、さらに別種のバックドアが設置された事例や、組織管理の端末が感染し、管理サーバへの水平展開を試みられた事例も確認されている。

中国国内で、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に関する報道が激化していた 2020 年 1 月から 2 月にかけては、前記の攻撃を確認できる情報を入手できない期間が続いたが、3 月中旬以降に再び攻撃は活発化しており、本報告の執筆時点では台湾の蔡総統政権二期目が始まり、また中国の全人代開催時期の前後（5 月末現在）も攻撃が継続していることを確認している。直近では、新型コ

ロナウイルスや履歴書などの一般的なテーマを用いる他に、感染した組織から窃取されたとみられる文書やメールが新たなスピアフィッシングメールに悪用されて、受信者に関わりの深いテーマや差出人を模したメールにより関連組織の特定人物が連鎖的に狙われる事例も観測されており、攻撃は深化し拡大傾向にあると言える。また、マルウェアに感染させるトリックについても、単にマクロを有効化させるだけでなく、マクロボタンを押下させるといった、サンドボックスによる自動解析での判別を妨害する手法を取り入れたことを確認している。

今回行われている攻撃の手口やマルウェアには、従来の攻撃と比較して特別に目新しい点が見られるわけではなく、2005 年以来からの普遍的な傾向に違わず、攻撃メールの内容や添付ファイルには不自然で粗雑な点が多い。それでも、一部の組織からの情報窃取を許している現状に鑑みて、スピアフィッシングメールの連鎖により攻撃対象となった人物自体を攻撃側に加担させてしまう方式は依然としてサイバーエスピオナージの手段として有効であり、システム的に入口・出口・内部対策だけでは完全な未然防止が難しいことを裏付けている。

当隊では連鎖的な被害を抑止・低減するために、被害組織の追跡、攻撃インフラ・攻撃ツールの調査と情報共有、公開情報の収集いった活動を継続している。

攻撃グループの帰属を示唆する公開情報としては、今回使用された未知のマルウェアには中国国家安全部（MSS）が関与しているといわれる APT10 が以前に使用したマルウェア"ANEL"との、コードレベルの類点を指摘するレポートがある[1]。

今回の攻撃資源にはある特定の地域や言語を匂わせる文字列が多用されているが、安易な偽旗工作である可能性も否定できず、攻撃の全体的な嗜好からは、過去から継続した攻撃と見ることもできると当隊では判断している。

2.2 VPN 装置の脆弱性からの侵入事例

2019 年 8 月中旬、複数の SSL VPN 製品の、既知の脆弱性に関するエクスプロイトコードが公開されたことで、攻撃が世界的に広まった。これらの脆弱性を悪用されると、攻撃者は遠隔から容易に標的システムへ侵攻でき、そこで任意のコマンドを実行し、任意のファイルを読み取ることが可能となる。このような攻撃を当隊では「ネットワーク貫通型」として 2018 年下期の活動レポートで取り上げており、サイバーエスピオナージにおいては、不審メール対策が回避される初期侵入の手口として今後も注意が必要である。

当隊では、10 月中旬に国内で VPN の脆弱性をついて侵入された事例を確認している。その事例では、攻撃者はリモートデスクトップ接続で内部ネットワークへ横展開して情報窃取を行い、その後の遠隔操作を可能にするためのバックドアを設置していた。

新型コロナウイルス対策に伴うリモートワーク導入で VPN などによる外部から社内への接続利用が広がるなか、VPN 装置などリモートアクセス環境は 24 時間稼働となることが多いこともあり、セキュリティパッチの更新が適時に行われていない傾向にあると考えられる。このため攻撃者の格好の標的となっていると推定できる。米国 CISA は、VPN、ネットーワークインフラ、リモート接続機器に最新のソフトウェアパッチをあてることの他に、ログイン情報を狙うフィッシングメールへの注意、ログレビューによる攻撃検出、復旧の準備、多要素認証の導入などを推奨している[2]。

攻撃者は SHODAN や Censys といった検索サービスを悪用し、または使い捨ての活動環境から通信先全体をスキャンするなどして脆弱性の対象となる機器を容易に特定し、攻撃を仕掛けることができる。対策としては、外部のスキャンサービスからの接続を拒否する設定や、通信可能な IP アドレスレンジを絞っておくなど、Layer3（IP 層）における ACL なども有効だと考えられる。運用面では、自組織の外部公開している製品やサービスを、同検索サービス等を利用して漏れなく把握し、脆弱性対策情報データベース等を活用して

[1] 標的型攻撃の実態と対策アプローチ 第 4 版 日本を狙うサイバーエスピオナージの動向 2019 年度下期
https://www.macnica.net/mpressioncss/feature_06.html/

[2] Alert (AA20-073A) Enterprise VPN Security
https://www.us-cert.gov/ncas/alerts/aa20-073a

最新のパッチを適用するといった基本的対策を続けることが大切である。

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周辺諸国の攻撃グループの動向に着目している。本項ではその一部を紹介する。

3.1　朝鮮語話者に関係するサイバー攻撃グループ

当隊では、2016 年度以降 2019 年の上期まで、DarkHotel と呼ばれる攻撃グループの関与が疑われるスピアフィシングメールの国内事例を断続的に観測してきた。セキュリティ企業のレポートによると[3]、2019 年の秋頃、インターネットに接続されていない環境に対応したスパイウェアツールが発見されており、DarkHotel と呼ばれる攻撃グループの関与が示唆されている。このスパイウェアツールの情報収集を進めたところ、国内で使用された可能性のある関連ファイルの情報を発見しているが、実際の攻撃に使用されたかどうかの判断材料は得られていない。

DarkHotel の帰属は、韓国政府または北朝鮮、と議論が分かれているところであるが、朝鮮語話者・使用者に関係するのでは、といった点では共通している。朝鮮語話者や利用者の分布（たとえば中国の朝鮮族など）などを理解しないと、このような帰属の議論を評価するのは難しく、サイバーセキュリティにおいても、特にステートスポンサードとよばれる APT 攻撃などの理解において、サイバーセキュリティ以外の情報（地政学や情勢など人文科学領域の情報など）を知る必要がある所以である。

その他の着目情報として、中国のセキュリティ企業奇虎 360（Qihoo 360）は、DarkHotel が新型コロナウイルス対策に伴うリモートワークの増加に乗じて、数多くの中国政府、中国企業の VPN を攻撃し、医療技術、感染状況、データの窃取を試みているという主旨のブログを積極的に公開している[4]。

なお、近年、中国のセキュリティ企業は他国に倣い、各攻撃グループに独自の名称を定めており、奇虎 360 は APT-C-XX 、Tencent は T-APT-XX といった体系を用いている。DarkHotel には APT-C-06、及び T-APT-02 が割り当てられて活動が追跡されている。

3.2　中国に関係するサイバー攻撃グループ

中国政府への帰属が疑われる攻撃グループの中で、今期に活動が報告されているものとしては、APT23、APT41、Tick 、BlackTech、Mustang Panda に関するレポートがよく見られる。

これらの攻撃グループの実態は、中国人民解放軍戦略支援部隊網路系統部や中華人民共和国国家安全部といった軍・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可能性を指摘する報告もある[5]。また中国の軍事科学院軍事科学戦略部が発行した 2013 年度版戦略学[6]においては、「第三章　ネットワーク分野での軍事闘争の戦略的指導」で「軍の部隊」「軍が認めた活動（国家安全部や公安部）」「民間による活動」との分類がある。そのため、中国に帰属するといわれる攻撃グループについては、このような一般的なサイバーセキュリティでは扱われない情報も収集、検証し、その背景や活動目的を探る必要があると考えている。

当隊では発足以来、これらの攻撃グループによるものとみられる活動を間断なく調査し、被害を受けた組織からエビデンス情報提供の協力をいただきながら帰属を推定する材料を蓄積している。

---

[3] Ramsay: A cyber-espionage toolkit tailored for air-gapped networks
https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/

[4] 360 核心安全技术博客 APT Darkhotel attacks during coronavirus pandemic

[5] Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers
https://401trg.com/burning-umbrella/

[6] ISBN 978-7-80237-650-2, 军事科学出版社, 2013 年 12 月第 1 次印刷

なお、2019 年 6 月には米国ジェームスタウン財団の CHINA BRIEF 紙[7]で、「中国共産党による日本におけるインフルエンスオペレーション」の記事が発表されている。中国共産党が世界的なソーシャルネットワークから、ドメスティックなソーシャルネットワークまでを駆使し、サイバー空間を使ったステートスポンサードな情報活動を展開しているとした場合、サイバーセキュリティの観点で、それらをどのように警戒し、状況把握し、被害の未然防止や拡大防止を行うかを考えていかなければならないだろう。

3.3 北朝鮮に関係するサイバー攻撃グループ

北朝鮮政府への帰属が疑われる攻撃グループの分類や呼称はセキュリティ企業各社により異なるが、APT37、Kimusky、HIDDEN COBRA に関するレポートがよく見られる。グループの活動は遅くとも 2007 年頃よりみられており、その実態は、朝鮮人民軍偵察総局（RGB）121 局、204 局、110 研究室、91 号室、180 部隊といった組織によるサイバー諜報、資金獲得、破壊活動、情報操作であるとも言われている[8][9]。

先に述べたように、このような帰属が示唆される情報の真偽を判断するためには、対象国についての知見を増やし、検証可能とする必要があるため、サイバーセキュリティ以外の専門家との意見交換等も必要であると考えている。

なお、これらの攻撃グループの関与が疑われる攻撃において、国内組織が過去数年間侵害されて踏み台などに悪用された事例があったが、同事例では他の国に関係していると思われる別の攻撃グループの活動痕跡も同時に見つかっていた。このような場合、その組織を狙ったのか、または便利なリソースとして使われたのか判断は難しく、目的の推定を行うためにさらなる情報収集が必要である。

3.4 ロシアに関係するサイバー攻撃グループ

ロシア政府への帰属が疑われる攻撃グループの分類や呼称はセキュリティ企業各社により異なるが、APT28、APT29、Gamaredon、Turla、Sandworm に関するレポートがよく見られる。APT28 と Sandworm にはロシア連邦軍参謀本部情報総局（GRU/GU Unit 26165 や Unit 74455）と、APT29 にはロシア連邦保安庁（FSB）及びロシア対外情報庁（SVR)との繋がりがあるとも言われている [10][11]。

一部の攻撃グループの活動は遅くとも 2004 年頃より観測されており、主な標的は欧州および米国とされている。しかし、わが国と友好関係にある国を標的に含む攻撃キャンペーンにおいて日本国内の関係機関へのスピアフィッシングメールも観測されたとするレポートもあり、当隊でも注意を向けている[12]。

2016 年には米国民主党のメール流出により米国大統領選挙に影響を与えるなど、サイバー空間を使ったインフルエンスオペレーション、認知領域作戦への関与もみられる。こうした活動に対抗するためには、ある情報のソースを追跡して真偽を判断し、正しい情報を共有できる体制が必要になるだろう。

---

[7] A Preliminary Survey of CCP Influence Operations in Japan
https://jamestown.org/program/a-preliminary-survey-of-ccp-influence-operations-in-japan/

[8] 북한 사이버 전사 "평균 나이 20 세 영재"…20 년간 사이버전 준비
https://www.etnews.com/20171121000396

[9] North Korean Malicious Cyber Activity
https://www.us-cert.gov/northkorea

[10] FireEye M-TRENDS 2019
https://content.fireeye.com/m-trends/rpt-m-trends-2019

[11] INTERNATIONAL SECURITY AND ESTONIA 2018
https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

[12] 標的型攻撃グループ「Gamaredon」による日本への攻撃を初観測 | トレンドマイクロ セキュリティブログ
https://blog.trendmicro.co.jp/archives/24285

4　活動を通しての所感

ステートスポンサードとよばれる攻撃者による攻撃では、侵入フェーズで用いられる手口として、これまでのメールを使った手法から、ネットワーク機器の脆弱性の悪用、ソフトウェアの更新機能を悪用したサプライチェーン攻撃、SNS 等を介したモバイルマルウェア感染、といった話題が多く、徐々に多様化している印象を持つ。しかし、2.1 項でも述べたようにスピアフィッシングメールは、受信者をだまして攻撃に加担させ（感染させ）完全な防御が困難であるが故に、今後も警戒すべき攻撃手口の一つであり続けるだろう。その対策としては、適時の情報共有により攻撃の連鎖を断つ活動だけでなく、日本及び共通の被害リスクのある国が共に対処する必要性を感じている。

2020 年 1 月～3 月はレスキュー数、情報提供数ともに減少したが、この原因は攻撃自体の減少ではなく、新型コロナウイルスの拡大に伴う緊急事態宣言やリモートワーク導入等の混乱により、各組織における被害の検知力や情報共有が減少していた可能性もある。当隊の把握できていない被害がこの時期に拡大していないかを懸念している。各組織には、不審メールや不審通信の見落としが無いかを今一度確認いただき、心配な点があれば些細なことであっても、またこの期間に関わらず昔のものでも構わないので当隊へご連絡いただきたい。

海外拠点等におけるセキュリティ実装の差から組織のネットワークへ侵入される事例も継続している。一部の管理者権限が既に攻撃者に奪われていないかを確認するために、再度、組織内部の重要サーバへのアクセスログをチェックすることも必要だろう。このような確認を通して不審な侵入痕跡を発見した場合には遠慮なく当隊へ情報共有いただきたい。当隊の知見をフィードバックするとともにナショナルセキュリティの底上げにも貢献できると考えている。

以前より繰り返し述べているように、他国の政府機関が関係していると推定されるステートスポンサードのサイバーエスピオナージ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て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、サイバーエスピオナージ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、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。加えて、サイバー空間における安心安全の議論において、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コンテキストで対処する可能性も考慮し、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。