サイバーレスキュー隊（J-CRAT） 活動状況
[2019 年度上半期]

2019 年 11 月 29 日

1　活動結果

2019 年 4 月～2019 年 9 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（上半期）
相談件数	519	412	413	221
レスキュー支援数	123	144	127	80
オンサイト支援数	17	27	31	18

※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 **221 件**であった。このうち、**レスキュー支援**へ移行したものは **80 件**、うち**オンサイト支援**を行った事案数は **18 件**であった。

2　2019 年度上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とみられる攻撃者によるサイバーエスピオナージ（サイバー諜報活動）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、セキュリティ対策への手がかりとなることを望む。

2.1 標的型サイバー攻撃の動向

2018 年 12 月に米国司法省が中国を拠点とするサイバー攻撃グループ（APT10）に所属するとみられる人物 2 名を起訴し [1]、即座にわが国も攻撃活動を非難する談話を公表している[2]。当隊の把握している範囲限りではあるが、これ以降の同グループによるわが国に対するサイバーエスピオナージはみられず、セキュリティベンダ等の公開情報からも、同グループによるとみられる国内の活動情報は現在まで収集されていない。

当隊の発足(2014 年 7 月)以来、APT10 は活動の観測頻度の高いグループの一つであり、今期のように活動が低減し続けたのは初めてである。この変化には、米国及びわが国などからのネーミングアンドシェーミング（非難）の効果が作用したともいえよう。

一方で、少なくとも数年間以上継続して活動している他の攻撃グループについては、当隊が直接的・間

[1] Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information
https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
[2] 中国を拠点とする APT10 といわれるグループによるサイバー攻撃について
https://www.mofa.go.jp/mofaj/press/danwa/page4_004594.html

接的に得た情報から、インフラ、化学、シンクタンク、メディアといった分野への標的型攻撃メール[3]による攻撃を今期も断続的に確認している。地理的には特に、中国の現地法人や、わが国と中国との合弁会社に対する活動が活発であったと判断している。攻撃の初期段階に、マルウェアを埋め込んだ画像形式ファイルをダウンロードする新たなツールが展開されるなど技術的な多様性も増えており、これらの攻撃グループの活動は今後も活発化していくであろうと判断している。

攻撃メールのテーマとしては、昨今の米中貿易戦争といわれる状況にある中で、米中両国の貿易問題、韓国との輸出管理問題といった経済問題や、それに関連する先端技術などの時事問題を用いたものが複数確認されている。これらの経済動向や関連製品の技術に直接・間接的に関わる組織においては、動向把握のためにサイバー諜報活動を受けていないか注意するとともに、何か不審な点を感じた場合は当隊へ相談いただきたい。また、既にこうした攻撃に関する情報を持っている企業には、事後のタイミングでも、部分的な情報でも構わないので、より正確なサイバー状況把握をおこなうために、お手数でもぜひ当隊へコンタクトいただきたい。

2.2 昨年行われた複数の学術組織に対する攻撃の継続調査

前期より継続して、学術組織の技術情報を狙ったとみられる事案群の対応を行っている。

攻撃開始時期は 2018 年の春頃と思われるが、事案対応はその約 1 年後、外部機関からの指摘により、ある学術組織から不審な通信が出ていることが発覚したことから始まった。当初は標的型攻撃メールからの感染を疑い調査を行ったが、不審なメールの痕跡は発見されなかった。そこで、発見されたマルウェアの一つが、市販のクラウドストレージサービスのアップデート実行ファイルと同じファイル名であることに着目して通信ログやディスク等の調査を進めていくと、そのダウンロード元はクラウドストレージサービスの正規サーバではない、侵害された別のサーバであることが分った。感染経路については、セキュリティベンダよりネットワーク機器への中間者攻撃の可能性も報告されているが[4]、断定はできていない。

この攻撃手口を被害組織の視点で考えた場合、このような侵攻パターンは、サイバーエスピオナージだけでなく、ランサムウェアやマイニングツールの設置など、さまざまな動機に基づく攻撃者にも悪用される可能性も高いと考えられるため、注意いただきたい。特に、「スタンドアロン」「クローズドネットワーク」なので安心と考えられているシステムにおいても、今一度、外部接続に対するセキュリティ制御を有効にしているか、そもそも外部接続経路は本当に存在しないのか、再確認を行っていただきたい。

その後、本事案の調査を通じて得られた多くの痕跡情報を基に、相談を受けた多数の学術組織等と協力してレスキュー支援を進めたところ、他の複数の組織からも同時期、同様の攻撃痕跡を発見している。本レスキュー活動は、標的とされた可能性のある多くの組織や、具体的な対処を行う機関と連携できたことで、一つの事案の痕跡を辿って攻撃の全体像が見えてきた一例である。

なお、この攻撃グループは、同時期に複数の学術組織への標的型攻撃メールも展開していたことから、様々な手口を用いて極めて執拗に、特定分野の技術情報を窃取することを目的としたキャンペーンを展開していた可能性を考えている。

2.3 攻撃者の目的に即した人物をピンポイントで狙うフィッシング攻撃

過去に繰り返しサイバーエスピオナージを受けてきた組織において、役員とシステム管理者に標的を絞った標的型攻撃メールの事例が見られた。

その手口は、標的組織の公開コンテンツを紹介するメールの文面に張られたリンクをクリックすると、組織の本物の Web ページをコピーした画像の上に偽のログイン画面を表示した不正サイトが開き、認証情報を入力すると正規サイトのトップページへ遷移するという典型的なフィッシング攻撃であった。

---

[3] 本活動報告では、標的型攻撃メールを、ランサムウェアやバンキングトロージャン、一般的なフィッシングメール、ビジネスメール詐欺（BEC）などサイバークライムやマルウェア SPAM ではなく、秘密裏に侵攻し情報を窃取することなどを目的とした「サイバーエスピオナージ」に関わる攻撃を指すものとする。

[4] Plead malware distributed via MitM attacks at router level, misusing ASUS WebStorage
https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

攻撃者の目的が「メールを窃取して内容から状況を把握すること、宛先や内容から人間関係を把握すること、及び、他組織を攻撃するための橋頭堡を確立すること。」であった場合、その達成手段は必ずしもマルウェアを用いた手口が必須ではないことに注意を払う必要がある。すなわち、標的型攻撃メールはもちろんのこと、ソーシャルエンジニアリングなど「サイバーエスピオナージと並行して行われる人間による活動」、あるいはそれらを組み合わせた活動についても、同様の注意やリスク管理が必要であり、セキュリティ部門だけでなく経営層を含めた組織全体で理解し、備えることが大切である。

2.4 高度な技術力を持つ攻撃グループの動向

2019 年 8 月に、セキュリティベンダが APT41、WINNTI と呼ばれる攻撃グループを特定している[5]。ステートスポンサードと思われる同グループは、日本を含む各国の、医療、ハイテク、通信、教育、ゲーム、旅行、報道などの業界を標的として、2013 年頃よりサイバーエスピオナージを開始しているとされる。当隊ではこのグループによる最近の国内活動について、これ以上の情報を得られていない。

しかし、このグループは極めて活発であり、その侵入手口はサプライチェーン攻撃、Web サーバ経由、認証情報窃取、標的型攻撃メール、正規のリモートアクセスツールなど極めて多様であることに加えて、使用するバックドアは検出がより困難なものであることから、国内には既に攻撃を受けている潜在的な感染組織、また実際に対処中や対処が終わった組織があるとみている。

同グループの標的とされている先端技術等を扱う組織におかれては、仮に攻撃を検知しておらず、平時という認識であっても、標的型サイバー攻撃の感染調査を健康診断として行うことを推奨する。そのようなレスキュー対応も可能なため、お気軽に当隊へご連絡いただきたい。

また、この攻撃者の活動に対して対処中、対処が終わった組織においては、お手数ではあるが、正確なサイバー状況把握のために当隊へもご連絡いただきたい。

3 活動を通しての所感

当隊がレスキュー支援の対象とする組織は、1 名のシステム管理者がセキュリティ管理を兼務するまたは、専任のシステム担当者もいない小規模な組織から、組織全体のセキュリティを運用管理する CSIRT 部門を有する大企業まで様々である。それぞれのセキュリティ対応組織に規模の違いはあるものの、サイバーエスピオナージへの対応に関しては経験値による成熟度の違いや変化を感じている。

初めてサイバーエスピオナージを経験する組織は、その対応をウイルス対策ソフトによる隔離や駆除、及び感染端末の初期化といった、一般的なマルウェア感染と同等の処置で済ませようとする傾向がある。しかし、標的型サイバー攻撃においては、攻撃ツールがウイルス対策ソフトで検出できないことや、攻撃者の横展開活動により感染範囲が拡大していることもある。当隊は、レスキュー支援を通じてこうした標的型サイバー攻撃の特徴を説明して理解いただき、少なくとも証拠保全を行うことにより後々の原因調査や被害推定に役立つこと等、状況に応じた対策の助言を行っている。

一方、過去にレスキュー支援を行い攻撃の脅威を理解いただいた組織においては、繰り返し攻撃を受けた場合は当隊へ直ちに連絡をいただく、また、先回りして保全や注意喚起を出すなどの対応を実施している様子である。さらに次の段階として、標的型サイバー攻撃の対応計画を見直したい、簡易調査を自身で行えるようにしたい、外部組織との脅威情報の連携を行いたい、過去の攻撃情報だがわが国のサイバー状況把握のために攻撃者の活動痕跡を活用していただきたい、といった積極的な相談をいただくケースも増えている。

一般に、セキュリティインシデント対応に求められる役割は幅広く、組織運営、対応方針の管理、マルウェア分析、インシデント対応、システムの診断、脅威情報の収集と活用、外部連携など多岐にわたる。サイバーエスピオナージのインシデント対応力を向上させるために、インシデントの対応方針へ各組織に適した「サイバーエスピオナージを受けた場合のアクション」を加えていただきたい。当隊のレスキュー支援では、こうした対応力を向上していただくことも念頭に活動を行っており、攻撃を未経験の組織に対しても必要に

[5] APT41: A Dual Espionage and Cyber Crime Operation
https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html

応じて施策等の助言も行っているので、是非活用していただきたい。

そして、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を成熟させて外部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。すなわち、各組織でのサイバーセキュリティに加え、ナショナル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、他国に対して、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る。

IPA では政府機関の一員としてわが国に対するサイバー脅威の状況把握活動を強化しており、各組織、各個人において、万一の被害を受けた場合だけでなく、攻撃が失敗に終わった場合であっても、我が国に対する情報活動の痕跡を収集させていただきたく、是非 J-CRAT へ連絡いただきたい。

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。