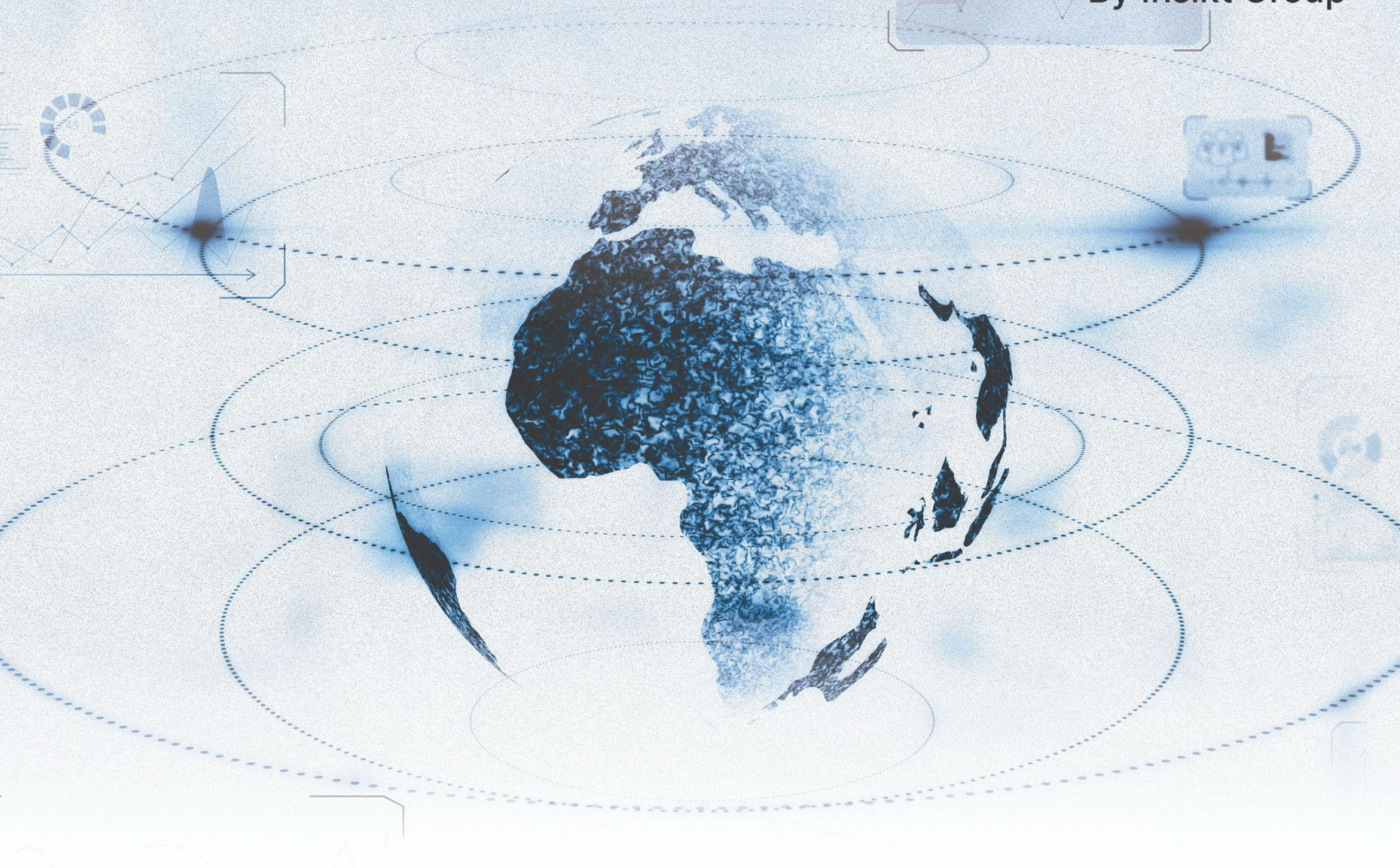
Recorded Future®

By Insikt Group®



世界のサイバー大国へと上り詰めた中国

CTA-CN-2023
0

要約

過去 5 年間にわたり、中国の国家支援型サイバー作戦は変化を遂げてきました。以前よりも成熟度とステルス性が向上し、より連係した脅威となっています。この新しい枠組みの具体例として挙げられるのが、外部公開されたセキュリティアプライアンスとネットワークアプライアンスのゼロデイ脆弱性および既知の脆弱性の活発な悪用です。同時に、運用上のセキュリティの重視、侵入活動の証拠の最小化、攻撃者の追跡の阻害も確認されています。追跡の阻害には、大規模な匿名ネットワークや「環境寄生型（Living Off the Land）」技術が使われています。

このような変化が確認されており、これらは内的要因と外的要因の双方から影響を受けていると考えられます。内的要因としては、中国の軍の大規模な再編や、中国国内での脆弱性に関する規制の変化が挙げられます。外的要因としては、西側諸国の政府や脅威インテリジェンスコミュニティによるレポートや情報公開が挙げられます。中国の国家支援型サイバー作戦が進化し、ステルス性と運用上のセキュリティが強化されたことにより、標的とされる組織、政府、サイバーセキュリティコミュニティにとっては、より複雑で困難な状況が生じています。

中国はサイバー作戦を利用して経済スパイ活動を行っています。以前はさまざまな商業上の知的財産（IP）を盗み出していましたが、進化を経て的を絞った戦略をとるようになり、戦略、経済、地政学の面での具体的な目標に対応するようになっています。たとえば、一帯一路構想の下での対外投資プロジェクトや重要なテクノロジーに関連する目標に対応しています。その結果、共同の対外投資と経済的競争の両方の文脈において、政府や企業がサイバースパイ活動の影響を受け、交渉において不利な立場に置かれたり、不公正な競争を強いられたりする可能性があります。中国の国家支援型サイバー活動の恒常的な標的となっている組織は、リスクの評価を見直す必要があります。サイバーリスクはデータ侵害に留まらないものであるということを認識し、交渉、競争力、戦略的位置付けへの潜在的な影響も考慮すべきです。

外部公開されているデバイス向けの斬新なエクスプロイトの開発が重視されているため、中国の国家が支援する活動の標的となり続けている可能性が高い組織では、ネットワークの防御に脆弱性中心のアプローチを用いていては不十分であり、多層防御による対策の改善が重要です。エクスプロイト後の永続化、探索、ラテラルムーブメントに関する活動の検知を重視します。標的となっている外部公開されたアプライアンスの大部分では、可視性、ログ機能、従来のセキュリティソリューションのサポートが限定的です。脅威を検知し対応する能力を強化するために、ネットワークアプライアンスを購入する際にこうした要因を考慮する必要があります。

主な調査結果

- 中国の国家支援型サイバー作戦では、中国の軍事、政治、経済、国内の治安に関する優先事項に沿った標的を重視しています。特に、中国の国家の支援を受けるグループは、適応力に優れていることを定期的に示しています。そうした適応力は、ロシアとウクライナの紛争や、アジア太平洋地域における一触即発の可能性をはらむ地域でのできごとなど、地政学的な動向によって影響を受けやすいものです。
- 中国がアジア太平洋地域、特に台湾と南シナ海で影響力を示し、目的を追求し続けるなかで、同地域の公共セクターおよび民間セクターのエンティティは、中国のサイバー脅威アクターによる従来のスパイ活動と、より破壊的なサイバー作戦および情報作戦がもたらすリスクの増加に直面する可能性が高いと考えられます。
- 中国の脅威アクティビティグループは、2021 年以降、外部公開されているアプライアンスを重点的に悪用しています。2021 年以降に中国の国家支援型グループによって悪用されたことがわかっている既知のゼロデイ脆弱性の 85%以上は、外部公開されているアプライアンスに関するものでした。これには、ファイアウォール、企業向け VPN 製品、ハイパーバイザー、ロードバランサー、メールセキュリティ製品などが含まれます。
- 外部公開されているアプライアンスのゼロデイ脆弱性の悪用を重視し、それらの製品の既知の脆弱性を迅速に武器化することは、世界中の多様な標的に対する初期アクセスを拡大するうえで効果的な戦術であることが示されています。組織がクラウドへの移行を進めるなか、外部公開されているアプライアンスを標的として重視する傾向はしばらく続くと考えられます。
- 中国の国家の支援を受けるアクター同士がマルウェアやエクスプロイトの能力を共有していることが確認されています。この共有を可能にしているのは、機能を開発している上流の開発者と、ソフトウェアの脆弱性の発見と武器化についての中国国内の幅広い政策の両方であると考えられます。

中国による世界のサイバー大国への進化

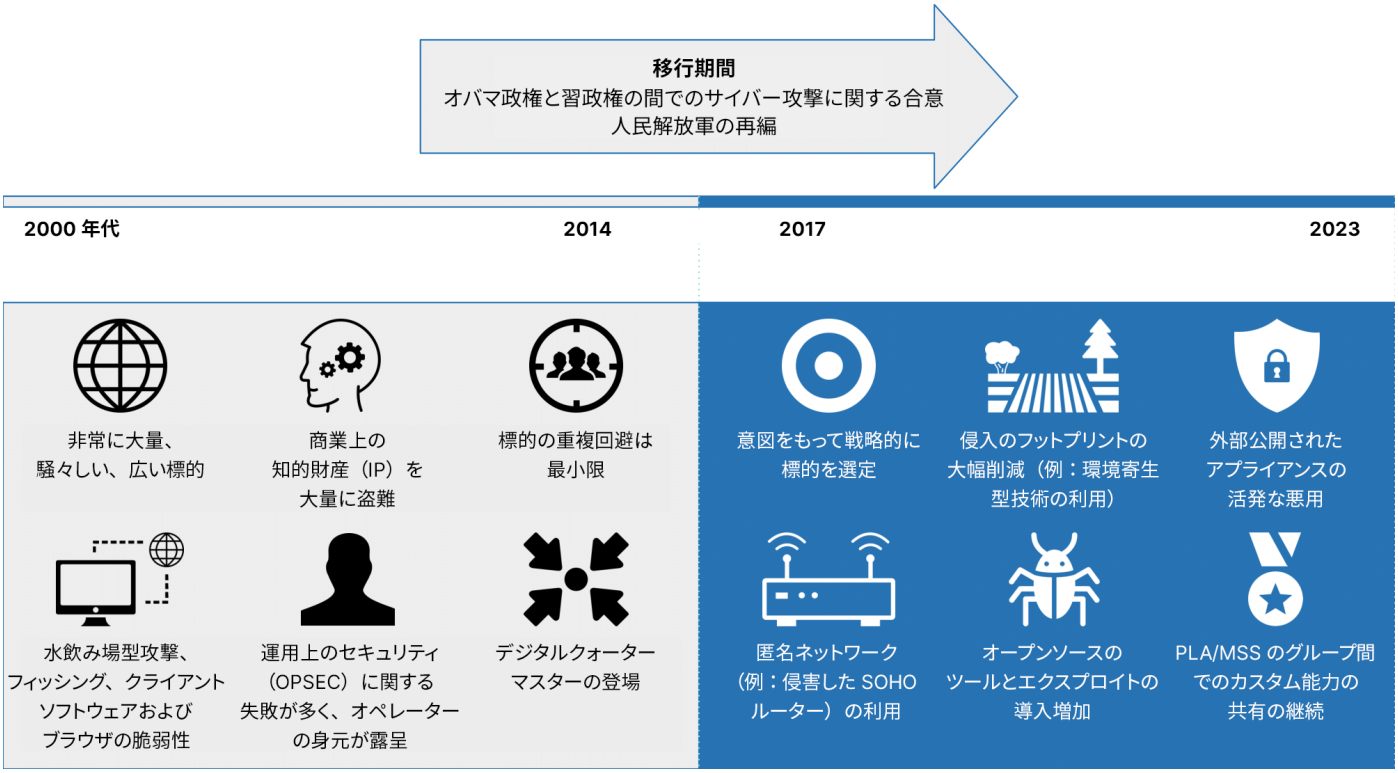


図 1：中国のサイバースパイ活動の進化（出典：Recorded Future）

2010 年代後半に、中国の国家が支援する活動に新しい傾向が見られるようになり、政府、セキュリティ企業、標的の組織による検知、アトリビューション、追跡の試みを妨げることがそれまでよりもかなり重視されるようになりました。この進化したアプローチがサイバー作戦で用いられるようになったのは、オバマ政権と習政権の間でのサイバー攻撃に関する合意の成立と、中国人民解放軍戦略支援部隊（SSF）の創設などが行われた中国での軍の再編のあと、一定の移行期間を経てからのことでした。この進化は、次に挙げるものを含む全体的な複数の要因によって特徴付けられます。

- 意図をもって戦略的に標的を選ぶようになり、2000 年代から 2010 年代半ばにかけてよりも標的の数が少なくなりました。それでも、アジア太平洋地域や中央アジア地域における、価値が高いインテリジェンスをもたらす標的では特に、同一ネットワーク内で中国の国家が支援する複数のグループの活動が発見されることが珍しくありません。
- 従来の初期アクセスベクターよりも、ファイアウォール、企業向け VPN 製品、メールサーバーソフトウェアなど、外部公開されているアプライアンスのゼロデイ脆弱性および既知の脆弱性を悪用するようになりました。こうしたデバイスは、可視性とログ機能が限られていて、その多くが従来のエンドポイントセキュリティソリューションをサポートしていません。
- 偵察、探索、コマンドアンドコントロール（C2）インフラストラクチャ向けに、大規模な匿名ネットワークの利用が進んでいます。匿名ネットワークの多くは、インターネットに公開されているモノのインターネット（IoT）デバイスや、SOHO ルーターなどのネットワークデバイス、仮想プライベートサーバー（VPS）インフラストラクチャを侵害して悪用しています。

- オープンソースのマルウェアファミリーやエクスプロイトの利用が進んでいます。これにより、公開されてまもない脆弱性の迅速な武器化、ハイエンドのカスタム機能の保護、アトリビューションの取り組みの阻害が可能になります。
- 人民解放軍（PLA）と中国国家安全部（MSS）の両方に関連する国家支援型グループにカスタムのマルウェアとエクスプロイトを供給する開発者は、能力を共有するサプライチェーンを継続的に利用しています。

これらの変化は、サイバーセキュリティの防御体制の全体的な改善や、攻撃者の戦術、技術、手順（TTP）について詳しく説明する脅威インテリジェンスレポートなど、複数の要因によって推進されていると考えられます。また、西側諸国の政府や Intrusion Truth などの第三者が、国家安全部から業務を請け負っている組織や個人の素性を明らかにするポリシーを採用するようになってきています。詳しく調査されるようなったことも、MSS から業務を請け負っている組織や個人による運用上のセキュリティの強化につながっていると考えられます。近年確認されている中国のサイバースパイ活動の変化には、国内の動向も関わっていると考えられます。中国では、前述のとおり情報機関が再編されたり、国内でのソフトウェアの脆弱性についての研究の成果を攻撃的な作戦で利用するようになったりました。人民解放軍が近年、海外のサイバー防衛について分析するオープンソースインテリジェンス（OSINT）サービス、サイバー攻撃およびサイバー防衛トレーニングシステム、海外製アンチウイルス製品を調達していることが Insikt Group によって確認されています。これは、中国人民解放軍戦略支援部隊（PLASSF）や人民解放軍による攻撃的サイバー作戦を強化するためと考えられます。

中国の国際情報機関

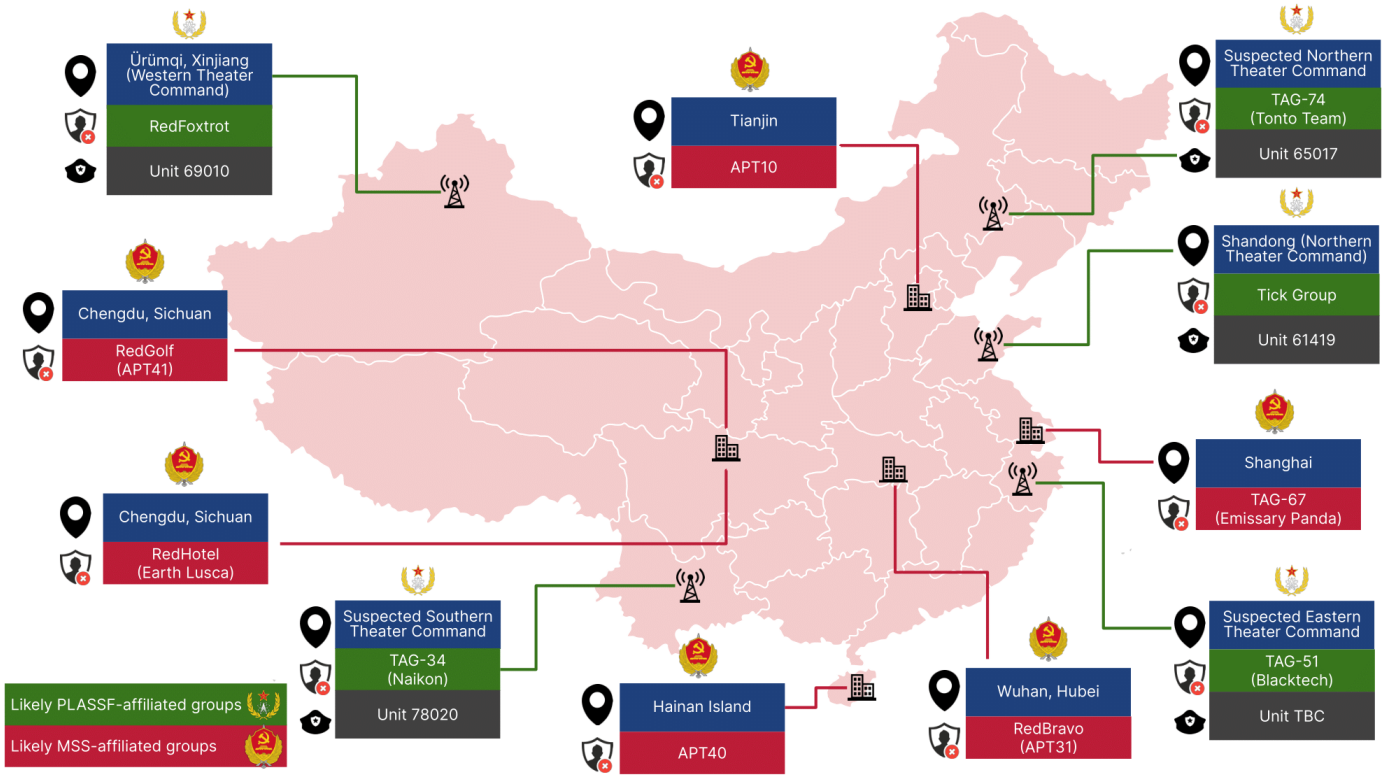


図 2：PLA または MSS にアトリビューションされる既知の脅威アクティビティグループの一部（出典：Recorded Future）

中国の国家支援型攻撃的サイバー活動を主に実行しているのは、中国の軍隊の関連部門、具体的には PLASSF と、軍隊には属さない国際情報機関である国家安全部（MSS）です。**図 2** には、人民解放軍または国家安全部との関係が疑われる、国家の支援を受けたグループの一部を、国内の活動拠点とともに挙げています。国家安全部は主に民間の契約業者を使っており、各地にある国家安全部の支局からインテリジェンスの収集を委託する形がよく取られています。米国政府による起訴状（1、2、3）で詳細を確認できます。国家安全部と関連があるグループは、人民解放軍と関連があるグループと比べると幅広い業種や地域を標的としており、防諜、海外の反体制派の監視、軍事関連以外の海外情報の収集、経済スパイ活動などに従事しています。

それとは対照的に、人民解放軍と関連があるグループの多くは、個々の戦区の地理的な標的を一貫して重視しています。たとえば、中国の国家支援型グループ RedFoxtrot は、以前 Recorded Future によって人民解放軍 69010 部隊とのつながりが指摘されました。この部隊は新疆ウイグル自治区ウルムチ市にあるので、人民解放軍の西部戦区に該当すると考えられます。西部戦区は人民解放軍の 5 大戦区の 1 つであり、確実にインド、パキスタン、中央アジアの監視を担っていると考えられます。この方向性は、観察された RedFoxtrot の活動と一致しています。同様に、防衛、軍事、通信、政府を対象にインテリジェンスを収集しているということは、人民解放軍の部隊に想定される活動範囲に一致するほか、人民解放軍と関係がある他のグループ（1、2、3）の標的とも一致します。

中国は経済および国家安全保障の面での関心に従い、全世界で大規模なサイバースパイ活動を展開

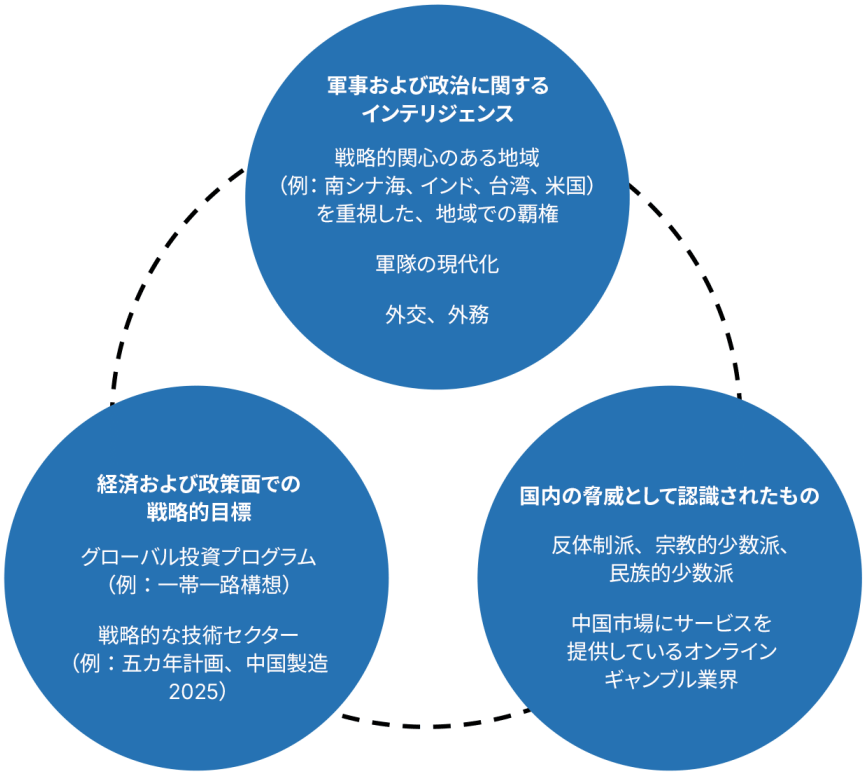


図 3：中国の国家支援型グループの活動で観察された主な標的のカテゴリー（出典：Recorded Future）

Recorded Future は、中国による世界中でのほぼ全業種に対する絶え間ないサイバースパイ活動を継続的に観察しています。中国の国家の支援を受けていることが疑われ、現在活動中の脅威アクティビティグループを合計で 50 以上追跡しています。ロシアやイランなど、他の国家の支援を受けていることが疑われるサイバー脅威アクターと比較すると、この規模は非常に大きなものです。中国の国家支援型グループは過去 5 年間では主に 3 つの領域を重視してきました。

- 軍事および政治に関するインテリジェンス
- 経済および政策面での戦略的目標への対応
- 民族的少数派や宗教的少数派などの国内の脅威への対応

軍事および政治に関するインテリジェンス

中国のサイバースパイプログラムは、従来の国際情報の収集と、軍隊の現代化と地域の覇権の獲得を目指す中国の継続的な取り組みに沿った活動となっています。国境を接する国と敵対関係にある国を特に重視して、航空宇宙、防衛、政府、メディア、軍事、通信などの業界や政治組織を標的にしています。

また、過去数年では、中国の国家支援型グループの間で、通信などの価値が高い上流の標的（サプライチェーンの侵害など）へのシフトが見られます。この傾向からも、中国のサイバー作戦の成熟度が高まったことがわかります。

地域の覇権の獲得と軍隊の現代化

アジア太平洋地域において中国の国家支援型グループが一貫して重視している地域は、中国が地域の覇権を握るうえで戦略的に重要な地域と、南シナ海、インド、台湾など、領土や主権を巡る争いがある地域です。インドと南シナ海を標的とした活動についてはすでにレポートを公開しています（1、2）。多くの場合、こうした活動のテンポと規模は、地政学的な緊張の度合いと、中国の国家の幅広い活動を反映したものになっています。**表 1** では、これらの地域における、中国の国家が支援した最近の活動の主な例を挙げています。アジア以外の地域では、中国の国家支援型グループは米国内の防衛産業基盤（DIB）を重視し続けています（1、2）。これには軍隊の現代化と従来の軍事インテリジェンス収集という 2 つの目的があるものと考えられます。

インド	Insikt Group は、中国の複数の国家支援型グループがインドで継続的に活動していることを確認しています。最も活発に活動しているのは、PLASSF と関係があるグループ、RedFoxtrot です。2022 年と 2023 年には、RedFoxtrot がインドの航空宇宙、防衛、通信業界の組織を標的にしていることが定期的に確認されています。 2022 年 5 月には、インドの宇宙計画に関連する複数の研究施設および稼働中の資産が一斉に標的となったことを Recorded Future が報じました。この活動が行われた時期は、BRICS（ブラジル、ロシア、インド、中国、南アフリカ）諸国による宇宙協力連合委員会の設立直前であり、また、インドが宇宙計画の一環として高い目標を掲げるようになりつつあるミッションを遂行している最中でした。
台湾	台湾は中国のサイバースパイ活動の重要な標的であり続けています。2023 年に台湾のエンティティを標的とする活動を Recorded Future が観察したところ、活動は中国の国家の支援を受けるアクターにアトリビューションされました。RedHotel（Aquatic Panda、Bronze University、Charcoal Typhoon）、TAG-67（Iron Tiger、Emissary Panda）、RedDelta（Vertigo Panda、Temp.Hex、Twill Typhoon）などのアクターが確認されました。 一例を挙げると、2023 年の 6 月から 8 月にかけて、RedHotel が ShadowPad バックドアを使って台湾の航空宇宙および防衛業界の企業を侵害しました。この企業は無人航空機（UAV）の製造を専門としています。

南シナ海	2023 年には、RedHotel、RedDelta、TAG-34（Naikon）、TAG-42（Earth Longzhi）などの中国のサイバースパイグループが、台湾に加えて南シナ海の国を標的としていることが継続的に確認されています。領有権を争う相手であるベトナム、マレーシア、フィリピンなどが標的に含まれていました。 2021 年の Recorded Future のレポートでは、中国の国家の支援を受けていることが疑われるグループ、TAG-16（BRONZE EDGEWOOD、Red Hariasa）が、南シナ海で領有権を争う、ベトナム、マレーシア、フィリピンの首相官邸、軍事関連エンティティ、政府機関を標的としていたことを明らかにしました。

表 1：インド、台湾、南シナ海周辺で中国の国家が支援した主なアクティビティ（出典：Recorded Future）

不測の事態に備えた重要なインフラストラクチャに対するアクセスの事前準備

中国の国家支援型アクターは、従来はイランやロシアの国家支援型グループよりも重要なインフラストラクチャを標的とするにあたってリスクを取らない傾向がありましたが、従来のインテリジェンス収集に留まらず、重要なインフラストラクチャのネットワークへのアクセスを戦略的に確保しようとする動きが徐々に見られるようになっています。近年の Recorded Future による調査では、2020 年から 2022 年にかけて、インドの送電網や他の重要なインフラストラクチャのセクターで稼働中の資産を標的とした、複数のキャンペーンが確認されています（1、2）。2020 年 5 月に、中国とインドの国境で衝突があり、それ以来、両国間では地政学的な緊張が高まった状態が続いています。この活動はその時期に行われています。中国の国家支援型グループによるこの一連のキャンペーンでは、インドの地域および州の給電指令所を重点的な標的としていました。給電指令所は、送電網をリアルタイムで運用し、送電を行う施設です。経済スパイの対象としては価値はほとんどありません。

2023 年 9 月に、Insikt Group は、米国の軍事、電力、通信関連組織を標的とした偵察活動を確認し、その活動を中国の国家の支援を受けていることが疑われるグループ、TAG-87（Volt Typhoon、BRONZE SILHOUETTE、Vanguard Panda）に結び付けました。この標的設定は、このグループについての過去の報告と整合性がありました。このグループは米国の重要なインフラストラクチャに対する関心を示し続けています。TAG-87 による以前のキャンペーンは、将来台湾海峡などで有事が発生した際に備え、米国とアジアを結ぶ重要な通信インフラストラクチャを麻痺させるための能力とアクセスを手に入れようとする中国の取り組みをサポートするものであると考えられていました。

中国は南シナ海と台湾での影響力の強化をもくろみ、同地域では米国と同盟国の活動が活発になっています。こうした要因は、関連する国家の重要なインフラストラクチャのネットワークを標的とする戦略的な偵察と事前準備に対して、今後大きな影響を与えると考えられます。ただし、重要なインフラストラクチャを標的とすることは、紛争が差し迫っていることを意味するわけではありません。こうした活動は、一般的には不測の事態への備えとして行われます。これは、複雑なネットワークに攻撃を行い麻痺させたり破壊したりするための能力を獲得するには、長い時間が必要となるためと考えられます。

経済および政策面での戦略的目標

これまで、中国は、経済に関する戦略的目標の達成を支援するために、インテリジェンスと技術移転の一環としてサイバースパイ活動を行っているということが確認されてきました。歴史的に、中国のサイバースパイ活動では、五カ年計画や中国製造 2025 などのその他の経済政策で優先される主要な技術分野を標的としてきました（1、2）。

一帯一路構想（BRI）や二国間での交渉などに基づく海外投資もサイバー空間でのインテリジェンス収集に影響を与えてきたと考えられます（1、2）。国家安全部は、一帯一路構想の下でのプロジェクトやその参加国を標的とする侵入活動を行ってきたことが確認されています。また、中国の対外政策に関する重要な構想の安全を確保するための支援を行っているということを明確に表明しています。2023 年 10 月 17 日に、中国は第 3 回となる一帯一路国際協力フォーラムを北京で開催しました。その前日、国家安全部の WeChat アカウントで、一帯一路構想に基づく中国の海外投資を保護するために、国家安全部がリスク管理や脅威の排除などさまざまな形で「積極的に」関与していることを表明する記事が公開されました。

中国は一帯一路構想を通じてその参加国を支援しています。陸上および海上輸送ネットワーク、通信システム、エネルギーインフラストラクチャなどを改善するために、金銭的な支援やその他の開発活動を行っています。注目すべきできごととしては、2023 年 9 月に、中国の国家の支援を受けていると疑われるグループ、TAG-68（BackdoorDiplomacy、CloudComputating、Playful Taurus）によってアンゴラの政府の支局が侵害されたと考えられることを Recorded Future が発見しました。アンゴラの政府を標的とすることには、このグループにアトリビューションされた過去の活動と整合性がありました。TAG-68 は、これまで一帯一路構想を通じた中国への負債についての情報収集に力を入れてきたと報じられています。ケニアなどのアフリカの他の国も標的となってきました。ケニアの場合と同様に、中国はアンゴラにとって最大の債権者となっており、アンゴラ政府の対外負債の約 40%は中国が貸し付けたものです（1、2）。Recorded Future は、他の国の政府を標的とする TAG-68 の活動についても以前に明らかにしました。アフリカとアジアにあり、中国と経済的および政治的な結び付きが強い国、具体的にはセネガル、南アフリカ、イランが標的となっていました。

Recorded Future は、第十四次五カ年計画で重視された主要な技術分野を中心とするインテリジェンス収集の特定にも引き続き取り組んでいます。この活動の一例として挙げられるのが、2023 年に Barracuda Email Security Gateway（ESG）アプライアンスのゼロデイ脆弱性を悪用して行われたキャンペーンです。このキャンペーンでは、半導体、公衆衛生、人工知能（AI）の業界など、第十四次五カ年計画で重視されていた主要なセクターのエンティティが繰り返し標的とされていました。また、2023 年 9 月には、台湾の半導体業界を標的としたと考えられる RedHotel キャンペーンについて Recorded Future が報じました。このキャンペーンでは、複数のステージからなる Cobalt Strike の感染チェーンが使われ、台湾の多国籍企業 Taiwan Semiconductor Manufacturing Company（TSMC）についての繁体字で書かれたおとりドキュメントが表示されました。

国内の脅威への対応

中国の国家支援型グループは、中国本土および海外で、中国共産党（CCP）にとっての国内の治安に対する脅威と見なされている個人およびコミュニティを定期的に標的としています。人権問題を重視する人道支援団体も標的に含まれます。

民族的少数派、宗教的少数派、反体制派への対応

過去 10 年にわたり、中国の国家の支援を受けるグループは、国内外の民族的少数派および反体制派を標的に、情報収集と監視のキャンペーンを定期的に行ってきました。この標的には、ウイグル、チベット、カトリック、民主化推進派、内モンゴル独立運動の参加者、法輪功の支持者などのグループが含まれますが、これらに限りません。2023 年 3 月に、Recorded Future は、RedDelta がモンゴルに関連する複数の非政府組織（NGO）および個人を標的としたことを報じました。この際の標的の大半は、モンゴルに拠点を置く仏教か、内モンゴル独立運動に関係していました。内モンゴルは中国北部にある自治区です。

国内での取り締まりと歩調を合わせたオンラインギャンブル業界への対応

Insikt Group は、中国市場にサービスを提供しているオンラインギャンブル業界を標的とした中国のサイバースパイ活動が近年増加していることを確認しています。オンラインギャンブルは中国本土では違法であり[1]、中国政府からは、政情不安と資本流出につながるものと見られていると考えられます。そのため、オンラインギャンブルの運営者と参加者に対する取り締まりが強化されています。2022 年の後半には、中国公安部（MPS）が 2,600 以上のオンラインギャンブルプラットフォームを閉鎖したと表明しました[2]。従来、オンラインギャンブルサービスを提供する組織の多くはフィリピンに本社を置き[3]、フィリピンオフショアギャンブリングオペレーター（POGO）と呼ばれ、継続的な取り締まりの対象となってきました。Recorded Future では、この業界を標的とするサイバースパイ活動が近年増加しているのは、中国公安部と中国のインターネット規制当局であるサイバースペース管理局が国内で行っている、オンラインギャンブルの取り締まり[4]をインテリジェンス面でサポートするためと考えています。

複数のキャンペーンで確認されている注目すべき戦術として、オンラインギャンブル企業が使用するチャットアプリケーションを標的として、サプライチェーンの侵害が行われています（1、2）。2023 年に、フィリピンのソフトウェア企業 Seektop が侵害を受けたことを Recorded Future が確認しました。攻撃を行ったのは、中国の国家の支援を受けていると疑われる 2 つのグループ、TAG-67（Emissary Panda、Iron Tiger、LuckyMouse）および TAG-78（Earth Berberoka）でした。活動は 2021 年から 2023 年にかけて行われていました。この活動、Seektop が開発した MiMi と呼ばれる暗号化メッセージングアプリケーションを標的としたソフトウェアのサプライチェーンの侵害については、以前に Trend Micro と Sekoia によるオープンソースのレポートで言及されています。Insikt Group がさらに分析を行った結果、Seektop は中国のオンラインギャンブル業界で使用されるソフトウェアを主に開発していること、MiMi アプリケーションは中国本土にいる顧客とギャンブル会社で働く海外のサポートスタッフがダイレクトメッセージをやり取りするために使われていた可能性が高いことがわかりました。

[1] https://www.scmp[.]com/news/china/politics/article/3157805/china-targets-online-casinos-war-illegal-gambling-authorities
[2] https://www.chinadaily[.]com[.]cn/a/202212/29/WS63ad9a75a31057c47eba6dd3.html
[3] https://www.scmp[.]com/week-asia/politics/article/3214584/will-philippines-ban-offshore-gambling-operators-amid-political -risks-chinese-customers
[4] http://english[.]www[.]gov[.]cn/statecouncil/ministries/202106/09/content_WS60c0bc08c6d0df57f98dafca.html

地政学的なイベントへの迅速な対応

中国の国家支援型グループは、外部からの地政学的な刺激に一貫して迅速に対応してきました。その迅速さは、多くの場合、特定のグループによるインテリジェンス収集と標的選定の確立されたパターンの変化を通じて直接観察できます。**図 4** に示したとおり、2020 年に、Insikt Group は、中国共産党とバチカン市国の役人が重要な対話を行う前に、RedDelta がバチカン市国やその他のカトリック関連エンティティを標的とするようになったことを確認しました。より最近では、ロシアによるウクライナ侵攻の前後の期間に、RedDelta がヨーロッパの政府および外交関連エンティティを標的とすることが増えたことを明らかにしました。インテリジェンス収集と破壊的な活動の増加に結び付いた外部のイベントの例としては、他にもインドと中国の間での緊張の高まり、2019 年の香港での抗議活動、新型コロナウイルスによるパンデミックなどが挙げられます。

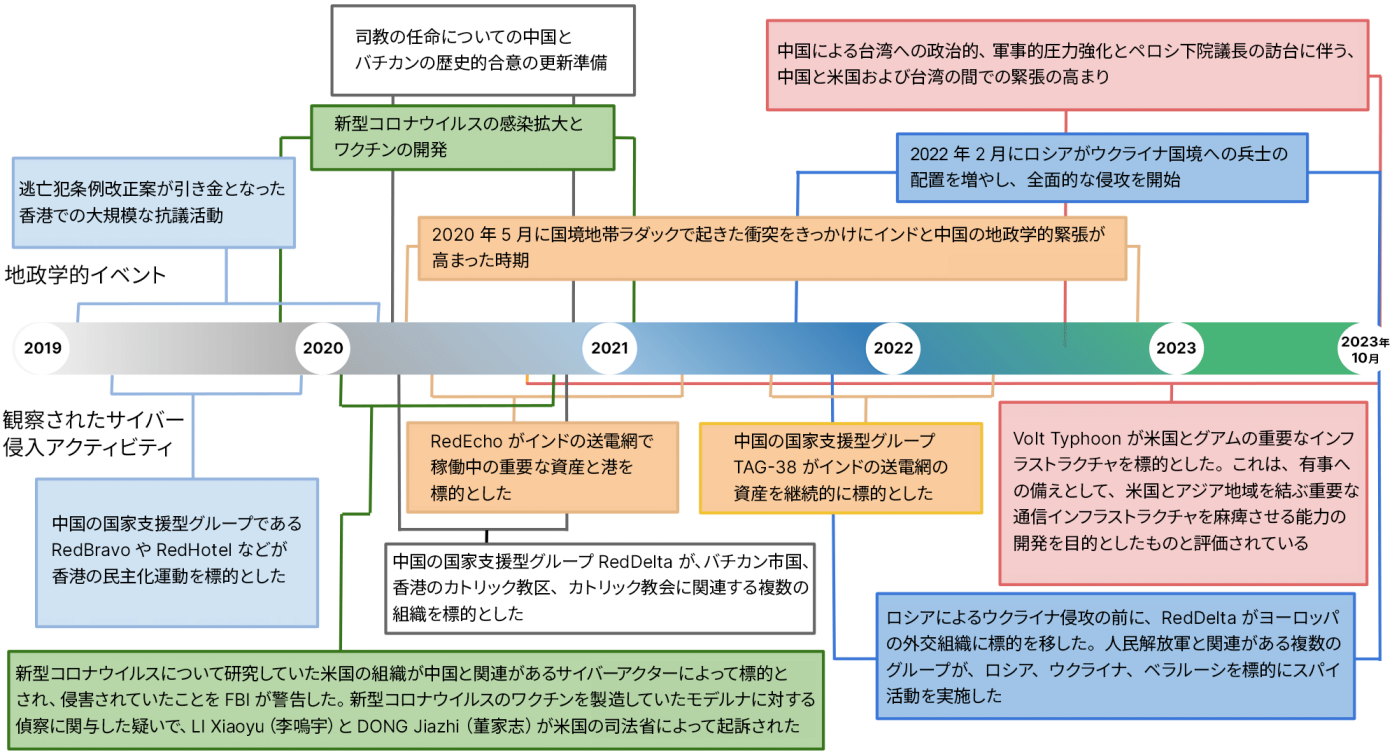


図 4：2019 年から 2023 年における地政学的イベントへの対応としての中国の国家支援型脅威アクティビティのタイムライン（出典：Recorded Future）

攻撃者のステルス性の向上と目的の明確化

中国の国家支援型グループ、特に北米とヨーロッパで活動しているグループは、運用上のセキュリティ（OPSEC）を徐々に高度化し、検知される可能性を最小限に抑えようとしています。この傾向は、インターネットに公開されているアプライアンスの悪用を重視していることからわかります。これらのアプライアンスの多くは、従来のエンドポイントセキュリティソリューションのサポート、ログ機能、モニタリング機能が十分ではありません。中国の国家支援型グループの多くは、アプライアンスを侵害してから、それらのアプライアンス専用に設計された Web シェルまたはカスタマイズしたマルウェアファミリーを使い、アクセスを永続化しています（1、2）。その後は環境寄生型技術と有効なクレデンシャルを組み合わせて、探索、収集、ラテラルムーブメントを行ったり、侵入活動のフォレンジック調査で使われる証拠を削除したりすることが増えています。被害者のネットワークとのやり取りにはプライベートな匿名ネットワークが用いられることが多く、アトリビューション、検知、追跡が困難になっています。

ゼロデイ脆弱性とインターネットに公開されたアプライアンスの悪用の迅速化

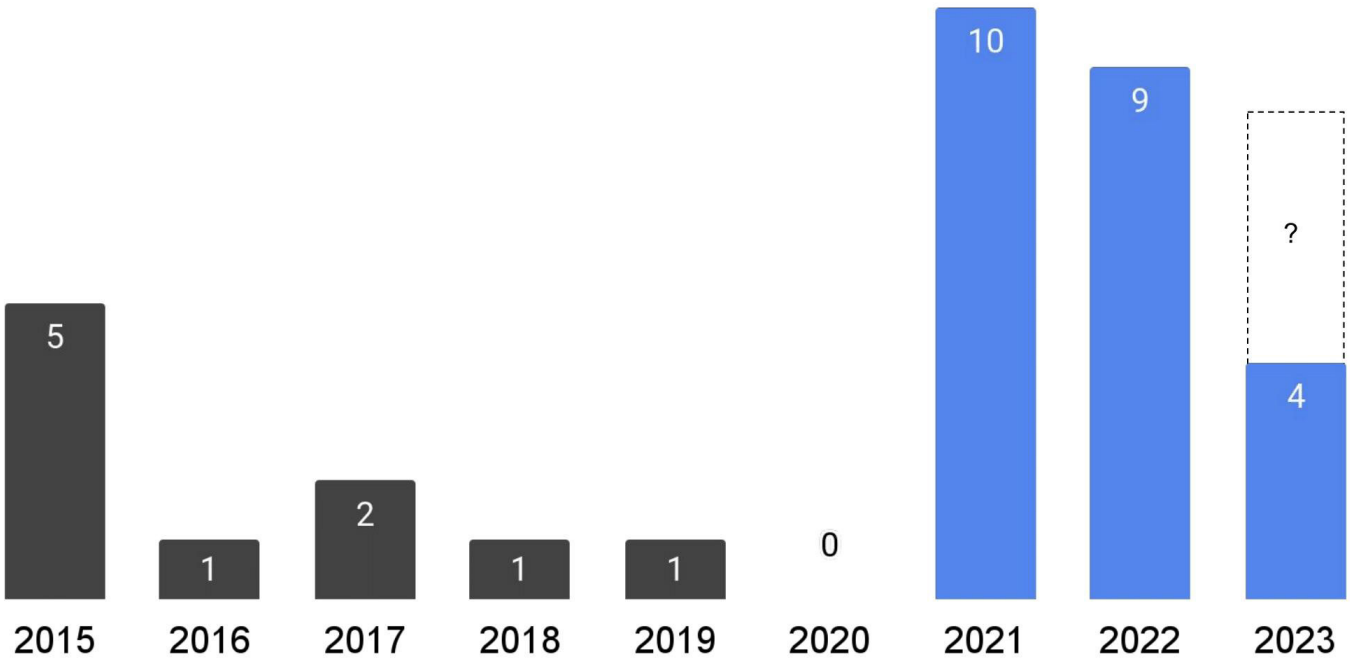


図 5：2015 年から 2023 年における中国の国家支援型グループによる既知のゼロデイ脆弱性の悪用（出典：Recorded Future）

2021 年の初めから、中国の国家支援型グループによるゼロデイ脆弱性の悪用が確認されることが大幅に増えています（完全なリストは付録 A を参照）。この期間に中国の国家支援型グループによって悪用された既知のゼロデイ脆弱性の 85%以上は、公開されているアプライアンスのものでした。メールのサーバーやアプライアンス（Zimbra、Microsoft Exchange、Barracuda ESG）、SSL VPN 製品（Pulse Secure や Fortinet FortiOS SSL-VPN など）、ファイアウォール（Sophos XG）、その他のインターネットに公開されるアプライアンス（Citrix ADC、Zoho ManageEngine、Atlassian Confluence など）の脆弱性が悪用されました。これがすべてのデバイス、すべての OS におよぶ中国によるゼロデイ脆弱性の悪用の全体というわけではありませんが、この

データからは、ゼロデイ脆弱性の悪用と、外部に公開されたネットワークアプライアンスの重視という、2021 年以降の明確な傾向がわかります。

複数の中国の国家支援型グループがゼロデイ脆弱性を同時に悪用している場合が複数確認されています。これは、共通の開発者がいるか、共通のエクスプロイトサプライチェーンがある可能性が高いことを示しています。広いエコシステムでこのような能力の共有が可能になっている要因としては、上流でエクスプロイトとマルウェアの開発者が共有されていることと、幅広い戦略的な政策を挙げることができます。中国は、Tianfu Cup などの競技会を開催したり、脆弱性の公開についての規制を課したりしています。また、Chinese National Vulnerability Database（CNNVD）を通じて価値の高い脆弱性を公開するにあたっては、中国の情報機関が直接影響力を行使できる可能性が高いと考えられます。

匿名ネットワークの大規模導入

中国の国家支援型グループが匿名ネットワークを利用することが増えています。匿名ネットワークの多くは、侵害した IoT デバイスや SOHO ルーター、あるいはアクターがプロビジョニングした VPS インフラストラクチャを運用インフラストラクチャとして利用しています。セキュリティ研究者にとっては、こうした匿名ネットワークはアクターがプロビジョニングする従来のインフラストラクチャよりも追跡が難しくなります。その理由としては、インフラストラクチャが蓄積されていき数量が増えていくことがまず挙げられます。また、侵害されたデバイスは所有者によって正規の目的で同時に使われるので、脅威アクターが通常のインターネットトラフィックに紛れ込むことができます。こうしたネットワークを使うことで、脅威アクターは、インフラストラクチャを迅速に循環させたり、標的のエンティティと同じ国にあるインターネットサービスプロバイダー（ISP）の IP アドレスを使ったりすることができます。

中国の国家支援型グループは匿名ネットワークも共有しています。PWC が公開した情報によると、複数のグループが匿名ネットワーク「RedRelay」などのシェアードサービスを利用していました。こうしたサービスの一部は、デジタルクォーターマスター（調達の担当者）を通じて提供されるような形式や、商用サービスとしての取り決めを通じた形で提供されている可能性が高いと考えられます。名ネットワークを使用した中国の国家支援型グループの例としては、インドの重要なインフラストラクチャを標的とする TAG-38、ヨーロッパの政府を標的とする RedBravo（APT31）、米国の重要なインフラストラクチャを標的とする TAG-87（Volt Typhoon）、台湾および日本のエンティティを標的とする TAG-51（BlackTech）などがあります。TAG-38 の場合、インターネットに公開されているサードパーティの DVR/IP カメラデバイスを侵害してネットワークを作り、ShadowPad のコマンドアンドコントロールインフラストラクチャとして、アクターが制御する上流のサーバーと通信させました。

緩和策

Recorded Future は、中国の国家の支援を受けたアクティビティに関連してよく確認される TTP を検知してその影響を緩和するために、以下の対策を講じることを推奨しています。

- 脆弱性へのパッチ適用にリスクベースのアプローチを取り入れ、リスクが高く、悪用されている脆弱性に優先的に対応するようにします。その判断のために Recorded Future®脆弱性インテリジェンスモジュールを利用してください。中国の国家支援型グループについては、特に環境内にあり外部に公開されているアプライアンスのリモートコード実行（RCE）に関する脆弱性に注意してください。
- 外部に公開されているサービスおよびデバイスのすべてでセキュリティのモニタリングと検知の機能を利用できるようにします。外部に公開されているサービスを悪用したあとに行われる可能性が高いアクティビティを監視します。Web シェル、バックドア、リバースシェルの展開や、内部ネットワークへのラテラルムーブメントなどがこれに該当します。
- インターネットに公開されるサービスをネットワークの非武装地帯（DMZ）内に隔離するなど、ネットワークのセグメンテーションを行います。
- すべての VPN 接続で多要素認証（MFA）の利用を強制します。また、VPN 接続向けのアノマリー検知の導入を検討します。
- 悪意のあるトラフィックの分析（MTA）を監視することで、Recorded Future のお客様は、既知の C2 の IP アドレスとの目立った通信に関与した可能性があるインフラストラクチャをプロアクティブに監視して、アラートを受け取ることができます。
- Recorded Future®サードパーティインテリジェンスモジュールを利用すると、リアルタイムの出力を監視して、物理環境、ネットワーク、ソフトウェアサプライチェーン内で、主要なベンダーやパートナーが関わる標的を絞った侵入活動の疑いを発見できます。
- 中国の国家支援型グループがよく利用している TTP の影響を緩和するための公開されているガイドを確認します（1、2、3、4）。

今後の展望

中国の国家支援型サイバー作戦の成熟度が向上し続けるなか、複数年におよぶ軍の再編と、国内での脆弱性の調査と武器化への重点的な取り組みも成果を上げるようになるでしょう。外部公開されているアプライアンスのゼロデイ脆弱性の悪用を重視し、それらの製品の既知の脆弱性を迅速に武器化することは、世界中の多様な標的に対する初期アクセスを拡大するうえで効果的な戦術であることが示されています。組織がクラウドへの移行を進めるなか、クラウド環境が標的にされる可能性が高いと考えられます。たとえば、STORM-0558 のアクティビティでは、認証トークンを偽造して、盗み出した Azure AD（現在の名称は Entra ID）エンタープライズ署名キーを使い、ユーザーのメールにアクセスしていました。

中国が南シナ海と台湾で力を示そうとし、米国がアジアでの同盟強化に努めるなかで、米国を含む関係国を標的とした中国によるインテリジェンス収集のテンポが速まると予想しています。また、これらの国で重要なインフラストラクチャのネットワークを標的とした戦略的な偵察と事前準備が行われる可能性が高いと考えられます。重要なインフラストラクチャを標的とすることは、紛争が差し迫っていることを意味するわけではありません。こうした活動は、一般的には不測の事態への備えとして行われます。これは、複雑なネットワークに攻撃を行い麻痺させたり破壊したりするための能力を獲得するには、長い時間が必要となるためです。多くの場合で、重要なインフラストラクチャを扱うセクターを標的とすることは、中国の経済的目標とも一致する可能性があります。動機や目標としてどのようなものが考えられるか推定するために、広い地政学的なコンテキストと、侵入について確認されたデータを分析することが重要です。

中国政府が攻撃的なサイバー作戦に多くの人員とリソースを割き、スパイ活動の技術と能力を過去 10 年で強化してきたことを考慮すると、中国はサイバースパイ活動と情報戦における世界の超大国としての立場を固めつつあると言えます。

付録 A：2021 年以降に中国の国家の支援を受けていると疑われるグループが悪用したゼロデイ脆弱性の一覧

CVE	製品
CVE-2023-22515	Atlassian Confluence Data Center および Server
CVE-2023-3519	Citrix NetScaler
CVE-2023-20867	VMware vCenter
CVE-2023-2868	Barracuda Email Security Gateway
CVE-2022-27518	Citrix ADC/Gateway
CVE-2022-41328	Fortinet FortiOS
CVE-2022-42475	Fortinet FortiOS
CVE-2022-41040	Microsoft Exchange Server
CVE-2022-41082	Microsoft Exchange Server
CVE-2022-3236	Sophos Firewall
CVE-2022-30190	Microsoft Windows
CVE-2022-26134	Atlassian Confluence Server および Data Center
CVE-2022-1040	Sophos Firewall
CVE-2022-24682	Synacor Zimbra Collaboration Suite
CVE-2021-40539	ManageEngine ADSelfService
CVE-2021-40449	Microsoft Windows
CVE-2021-30869	Apple macOS
CVE-2021-44077	Zoho ManageEngine
CVE-2021-35211	Solarwinds Serv-U
CVE-2021-26855	Microsoft Exchange Server
CVE-2021-26857	Microsoft Exchange Server
CVE-2021-26858	Microsoft Exchange Server
CVE-2021-27065	Microsoft Exchange Server

Insikt Group®について

Insikt Group は、Recorded Future の脅威調査部門です。政府、警察、軍、情報機関での豊富な経験を持つ、アナリストとセキュリティ研究者が在籍しています。Insikt Group のミッションは、インテリジェンスをもたらして、お客様のリスクを軽減し、具体的な成果を上げ、ビジネスの中断を防ぐことです。

Recorded Future®について

Recorded Future は世界最大級の脅威インテリジェンス企業です。Recorded Future のインテリジェンスクラウドは、攻撃者、インフラストラクチャ、標的にわたるエンドツーエンドのインテリジェンスを提供します。Recorded Future は、オープンウェブ、ダークウェブ、技術的なソースにわたってインターネットのインデックスを作成し、拡大するアタックサーフェスと脅威の状況をリアルタイムで可視化します。お客様が自信をもって迅速にリスクを削減し、ビジネスを安全に進めることができるようにします。ボストンに本社を置き、世界中にオフィスと従業員を展開しており、75 か国以上の 1,700 を超える企業と政府系機関で利用されています。偏見のない実用的なインテリジェンスをリアルタイムで提供します。

詳しくは、recordedfuture.com をご覧ください。また、Twitter で@RecordedFuture をフォローしてください。