Press Release
2021 年 6 月 17 日（木）
レコーデッド・フューチャー・ジャパン株式会社

Recorded Future、脅威活動グループ RedFoxtrot が 中国の軍隊と関係していることを示唆

調査から人民解放軍（PLA）のサイバー作戦の一端が明らかに

航空宇宙／防衛、通信、鉱業の各業界、並びに政府機関、研究組織を 標的としたネットワークへの侵入を検知

2021 年 6 月 17 日（木）– エンタープライズセキュリティインテリジェンスのグローバルリーダー、Recorded Future Inc.の日本法人、レコーデッド・フューチャー・ジャパン株式会社（本社：東京都中央区、執行役 社長：牛込 秀樹、以下 Recorded Future）は本日、中国の国家支援型の脅威活動グループによるものと疑われるサイバースパイ活動を明らかにする、最新レポートを公開しました。このグループは、Recorded Future のスレットリサーチ（脅威調査）部門、Insikt Group によって「RedFoxtrot」と名付けられました。Insikt Group は、RedFoxtrot の活動と、中国人民解放軍戦略支援部隊（SSF）に属する情報組織、人民解放軍（PLA）69010 部隊との具体的なつながりを特定しました。これは人民解放軍が 2015 年に再編されて以来、中国人民解放軍戦略支援部隊（SSF）の活動を垣間見ることができる貴重な資料になります。

Recorded Future によるネットワークトラフィックの大規模な自動分析と専門家による分析から、中国と国境を接するアジア諸国の複数の業種を標的とする侵入が検知されました。レポートの要点は次のとおりです。

- 2014 年から活動している RedFoxtrot は、アフガニスタン、インド、カザフスタン、キルギスタン、パキスタン、タジキスタン、ウズベキスタンの航空宇宙／防衛、通信、鉱業の各業界、および政府機関、研究組織を主な標的としています。これは、人民解放軍 69010 部隊の管轄と一致します。
- RedFoxtrot は、大規模な運用インフラを管理しており、独自のマルウェアファミリーと一般に公開されているマルウェアファミリーの両方を使用している可能性が高いと考えられ、これらのマルウェアファミリーは、中国のサイバースパイグループが共通で利用しているものです。
- RedFoxtrot の活動内容は、他のセキュリティベンダーが追跡している脅威グループ、Temp.Trident や Nomad Panda などと重なるところがあります。
- 人民解放軍の特定の部隊とのつながりが確認されたことと、中国のサイバースパイグループに特有のものと考えられる共通のカスタム機能を使用していることから、高い確度をもって、RedFoxtrot は中国の国家支援型の脅威活動グループであると考えられます。

「人民解放軍の最近の活動は、その大部分がインテリジェンスコミュニティにとってブラックボックスとなっています。今回のように、人民解放軍の活動、中国の軍事戦術、中国の目的を垣間見ることができるのは珍しい機会であり、グローバルでの脅威の状況について貴重な情報をもたらすことができます。攻撃者を阻止し、組織または政府機関のセキュリティ体制に情報を提供するには、

インテリジェンスを持続的かつ広範に監視し、収集することが極めて重要です」（ Recorded Future、CEO 兼共同創業者、Dr. Christopher Ahlberg）。

レポートの全文はこちらからご覧下さい： 中国の人民解放軍 69010 部隊と関係する脅威活動グループ RedFoxtrot が、中国と国境を接するアジア諸国を標的に侵入

中国の脅威活動グループについてのその他のリソースは、Recorded Future の Web サイトをご覧下さい：https://www.recordedfuture.com/resources/

Insikt Group について

Insikt Group は、Recorded Future のスレットリサーチ（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、顧客のリスクを軽減し、具体的な成果を挙げ、ビジネスの中断を防ぐためのインテリジェンスを生み出すことです。

Recorded Future について

Recorded Future は、エンタープライズセキュリティインテリジェンスを提供する世界最大のプロバイダです。継続的かつ広範な自動化されたデータ収集／分析と、人による分析を組み合わせることにより、タイムリーかつ正確で実用的なインテリジェンスを提供します。混沌と不確実性が増している時代において、Recorded Future は組織が脅威をより迅速に特定／検知する上で必要な可視性を提供するとともに、攻撃を阻止するためにプロアクティブなアクションを取り、人、システム、アセットを保護することで安心してビジネスを展開できるように支援しています。Recorded Future は、世界中で 1,000 以上の企業や政府系機関で利用されています。詳細は https://www.recordedfuture.com/jp/をご覧下さい。

*本プレスリリースは米国本社が作成したプレスリリースの翻訳版になります。

【本プレスリリースに関するお問合せ】
レコーデッド・フューチャー・ジャパン株式会社
〒104 0031
東京都中央区京橋 2-2-1
京橋エドグラン 26 階
Tel：03-6838-9830
Email：Japan-Info2@recordedfuture.com
URL：https://www.recordedfuture.com/jp