Digital Security
Progress. Protected.

APT 活動レポート

ワイパー型マルウェア、フィッシング、パッチが適用されていない脆弱性

2024 年 10 月～ 2025 年 3 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、2024 年 10 月から 2025 年 3 月末までに 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、この期間に ESET が調査した多様な脅威の中で代表的なものであり、重要なトレンドおよび動向を示しています。本 APT 活動レポートは、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たものです。

この期間中には、中国とつながりのあるサイバー攻撃者が、欧州の組織を主な標的としてスパイ活動を執拗に継続していたことが確認されています。Mustang Panda は依然として最も活発に活動しており、Korplug ローダーや悪意のある USB ドライブを使用して政府機関や海運企業を標的に攻撃を繰り返していました。DigitalRecyclers は、KMA VPN の匿名ネットワークを使用し、RClient、HydroRShell、GiftBox バックドアを展開し、EU の政府機関を標的とした攻撃を継続していました（注：KMA VPN は、中継システムである ORB ネットワークを使用してトラフィックを匿名化する技術）。PerplexedGoblin は、ESET が NanoSlate と命名したスパイ活動のための新しいバックドアを使用して、中央ヨーロッパの政府機関を攻撃しています。一方で、Webworm は SoftEther VPN を使用してセルビアの政府機関を攻撃しており、中国とつながりのあるサイバー攻撃グループ間でこのツールが引き続き広く利用されていることを示しています。また、ShadowPad クラスタは、金銭的な利益を得るためにランサムウェアを散発的に展開していましたが、その主な目的はスパイ活動だと考えられます。ESET はまた、Worok が HDMan、PhantomNet、Sonifake などのスパイ活動のためのツールセットを頻繁に共有および使用している状況を明らかにし、これらのツールを使用したキャンペーンを Worok 以外のグループが実施しているという矛盾点のある第三者の見解を正しました。

イランとつながりのあるサイバー攻撃者も活発に活動し続けています。その代表的なグループが MuddyWater です。MuddyWater は、スピアフィッシング攻撃においてリモート監視および管理（RMM）ソフトウェアを頻繁に悪用していました。注意が必要なのは、MuddyWater が OilRig 傘下のグループである Lyceum と緊密に協力し合い、イスラエルの製造会社を標的にしていることです。BladedFeline は、過去に一度攻撃したことがあるウズベキスタンの通信会社を再度攻撃していますが、これはイランがウズベキスタンとの外交戦略を進めていた同時期に発生しています。CyberToufan は、イスラエルの複数の組織に対してワイパー型攻撃を展開し、破壊的な活動を行っています。北朝鮮とつながりのあるサイバー攻撃者は、金銭の獲得を目的としたキャンペーンを積極的に実行していました。DeceptiveDevelopment は、主に暗号通貨、ブロックチェーン、金融分野の偽の求人情報を利用しながら、標的を大幅に拡大しています。このグループは、ClickFix 攻撃や GitHub への偽の問題を投稿するなど、新しいソーシャルエンジニアリングの手法を駆使しながら、マルチプラットフォームに対応するマルウェア「WeaselStore」を配信しました。Bybit の暗号通貨が窃取されたインシデントは、FBI によって TraderTraitor の犯行と特定されましたが、このケースでは、Safe{Wallet} のサプライチェーンが侵害され、約 15 億米ドルの損失が発生しました。一方、北朝鮮とつながりのあるサイバー攻撃グループの活動には変化が見られています。2025 年初頭、Kimsuky と Konni の活動は 2024 年末に大幅に減少した後で、通常のレベルに戻り、英語圏のシンクタンク、NGO、北朝鮮の専門家から、主に韓国の団体と外交関係者に標的を限定するようになりました。Andariel は、1 年間活動を休止していましたが、再び舞い戻り、韓国の産業用途のソフトウェア企業に対して高度な攻撃を実行しています。

Sednit や Gamaredon に代表されるロシアとつながりのあるサイバー攻撃グループは、主にウクライナと EU 諸国を標的としたキャンペーンを積極的に継続しています。Sednit は、Web メールサービスにおけるクロスサイトスクリプティング（XSS）の脆弱性のエクスプロイトを改良し、RoundPress 作戦では攻撃対象の Web メールサービスを Roundcube だけではなく、Horde、MDaemon、Zimbra にまで拡大しています。ESET は、同グループがウクライナの企業に対して、MDaemon メールサーバー（CVE-2024-11182）のゼロデイ脆弱性への攻撃に成功していることを発見しました。一方、RomCom は Mozilla Firefox（CVE-2024-9680） と Microsoft Windows（CVE-2024-49039）に対するゼロデイエクスプロイトを展開し、高度な能力を有していることを示しています。ESET の研究者は、これらのすべての脆弱性を各ベンダーに報告しています。Gamaredon は、今でもウクライナを標的として最も多くの攻撃を実行しているグループです。Gamaredon は、マルウェアの難読化の手法を強化し、Dropbox を利用するファイル窃取ツールである PteroBox も採用しています。一方で悪名高い Sandworm グループは、ウクライナのエネルギー企業に対する破壊活動を強化し、Active Directory のグループポリシー経由で ZEROLOT という新しいワイパー型マルウェアを展開し、侵害の初期段階では RMM ツールを活用しています。

最後に、知名度がそれほど高くないサイバー攻撃グループによる注意すべき活動もお伝えします。APT-C-60 は、北朝鮮とつながっている可能性のある日本人を重要な標的としています。また、正体不明のサイバー攻撃グループが、世界経済フォーラムや選挙の Web サイトになりすまし、ウクライナの高官や外交官から機密情報を入手するために高度な標的型フィッシングキャンペーンを行っています。さらに、StealthFalcon は、トルコとパキスタンでスパイ活動に重点を置いた作戦を実施しています。

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詳細な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 活動レポート」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。

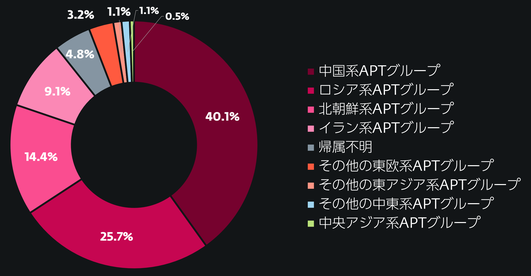
高品質で実用的な戦略立案に役立つサイバーセキュリティ脅威インテリジェンスを提供する「ESET APT 活動レポート」の詳細は、**ESET 脅威インテリジェンスのページ**を参照してください。

攻撃者と標的

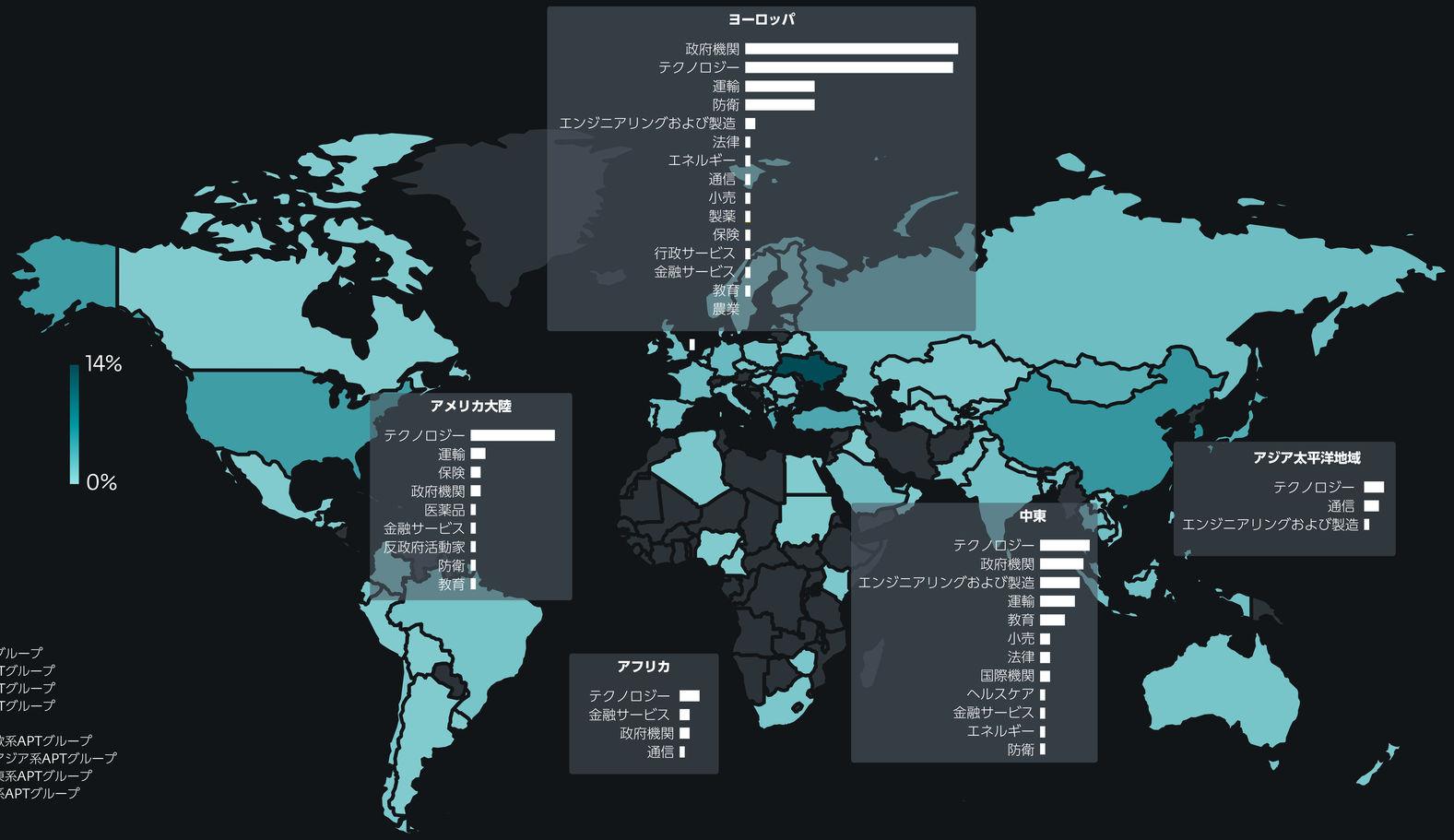
中国とつながりのある APT グループは、ヨーロッパ全土にわたる政府機関をスパイ活動の重要な対象にし続けています。ウクライナは最も激しいサイバー攻撃を受けていますが、これは主にロシアとつながりのあるサイバー攻撃グループによる国の重要インフラや政府機関を狙った継続的なキャンペーンによるものでした。

アジアでは、中国とつながりのある APT グループが政府機関や学術機関を対象とした攻撃を続けています。一方で、北朝鮮とつながりのあるサイバー攻撃グループは、特に個人、民間企業、大使館、外交官を標的にした攻撃を大幅に増加させており、特に韓国への攻撃を強化しています。

イランとつながりのある APT グループは主に中東地域の標的を攻撃しており、特にイスラエルの政府機関や製造・工業分野の組織を標的にした攻撃を続けています。技術系企業へのサイバー攻撃は世界的に顕著に増加していますが、これは主に北朝鮮とつながりのあるサイバー攻撃グループが実行している Deceptive Development 活動が活発になっていることに起因しています。



攻撃グループ



対象となった国と業界

中国

UnsolicitedBooker Worok Webworm PerplexedGoblin DigitalRecyclers Mustang Panda

中国とつながりのある APT グループによる活動の概要

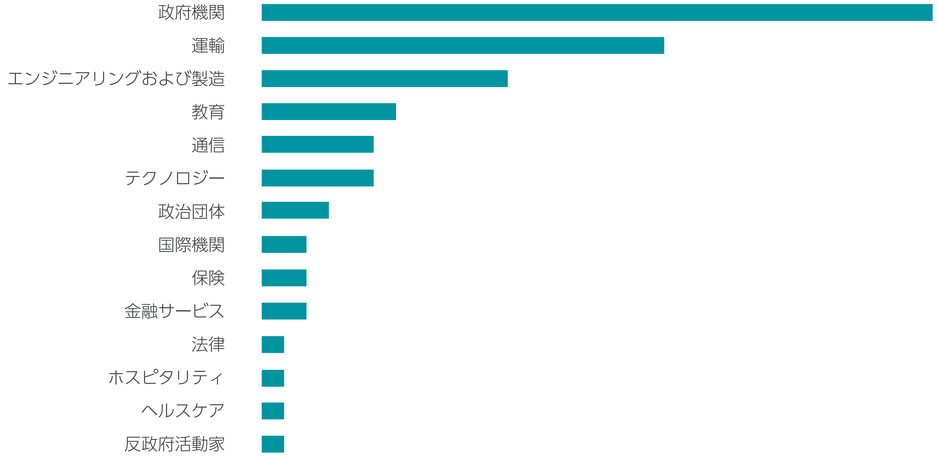
ESET の研究者は、中国とつながりのある APT グループが欧州の組織を標的に実施した複数のキャンペーンを観測しており、これらのグループによる一貫性と継続性のある攻撃を明らかにしました。

中国とつながりのあるサイバー攻撃グループである UnsolicitedBooker は、2023 年に発見され、政府機関を標的にする際に航空券に関連するメールを偽装したスピアフィッシングメールを頻繁に使用しています。このグループは、サウジアラビアの国際機関を標的にして、新たなスピアフィッシングキャンペーンを展開しました。その手口では、偽のサウディア航空のメールが使用されており、このフィッシングメールによって MarsSnake バックドアが展開されます。

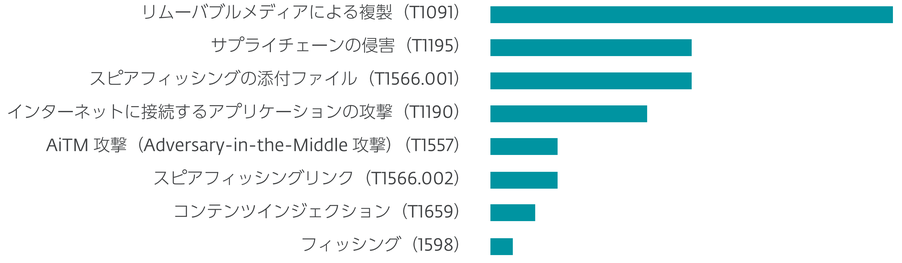
ESET の研究者は、中国とつながりのあるサイバースパイグループである Worok の活動を継続的に追跡しています。このグループは、2021 年初頭に Microsoft Exchange Server の脆弱性である ProxyShell を悪用していたときに最初に確認されました。同グループは最近、英国の学術機関やカンボジアの政府機関を標的にしています。他のセキュリティ研究者は複数のキャンペーンの攻撃グループについて一貫性のない主張を行っていましたが、ESET は詳細な解析結果を提供し、これらのキャンペーンが Worok によるものであることを示しました。

中国系グループによる欧州の組織に対する脅威の動向

2024 年 10 月から 2025 年 3 月にかけて、中国とつながりのある APT グループがヨーロッパの組織を標的にした攻撃を継続しており、複数のサイバー攻撃グループによるキャンペーンが ESET のテレメトリ（監視データ）で特定されました。2024 年 10 月、セルビアの政府機関が使用しているマシンで、攻撃が疑われる SoftEther VPN の悪用が検出されました。このサイバー攻撃グループは、SoftEther サーバーに接続するように設定された SoftEther Bridge の実行ファイルを展開しました。このサーバーは、Webworm（Flax Typhoon や GALLIUM など、SoftEther を使用している中国とつながりのある APT グループの 1 つ）が利用していると、ESET は確信しています。これについては、**2024 年第 2 四半期～第 3 四半期の APT 活動レポート**でも説明しています。



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

2024 年 12 月、ESET は PerplexedGoblin の活動を中央ヨーロッパの政府機関のネットワークで観測しました。PerplexedGoblin の TTP は、APT31 と重複しています。このグループは新しいスパイ活動のためのさまざまな機能を実装しているバックドアを展開しました。ESET はこのバックドアを NanoSlate と命名しました。NanoSlate と以前から知られている TurboSlate（ESET は、PerplexedGoblin のみが TurboSlate を使用していると考えています）を比較したところ、これらのバックドアの動作とコーディングの方法は酷似しており、PerplexedGoblin が NanoSlate を利用しているという ESET の主張を裏付けています。また、被害者の業種が当該グループの標的の傾向と一致している点も、この主張を補強しています。

DigitalRecyclers（**ESET の APT 活動レポート 2023 年第 2 四半期〜第 3 四半期**で解説）も、欧州の組織を標的として攻撃を続けています。DigitalRecyclers は、中国とつながりのある APT グループであり、RClient、HydroRShell、GiftBox バックドアを使用し、**オペレーショナルリレーボックス**（ORB）ネットワークである KMA VPN を使用してネットワークトラフィックを匿名化しています。これは中国とつながりのあるサイバー攻撃グループで共通する傾向であり、同様の匿名化ネットワークが複数存在します。今年の 3 月に、ESET はこのサイバー攻撃グループが EU 加盟国の政府機関を攻撃していることを観測しました。これらの機関は、2024 年にも同グループの標的となっていました。

2 月に **Trend Micro** と **Orange Cyberdefense** の研究者がブログを公開し、ShadowPad クラスタがランサムウェアを展開するいくつかの事例について解説しました。これまで、ShadowPad はスパイ活動にのみ使用されており、中国とつながりのある攻撃グループのみが使用していました。ESET もこのクラスタを調査しており、ESET のテレメトリから、イタリア、ルーマニア、フランスにまたがる複数の政府機関や民間企業が、このサイバー攻撃グループの標的になっていることを特定しています。しかし、ランサムウェアの展開は観測されていません。おそらく、ESET 製品が初期段階で攻撃をブロックし、ランサムウェアが展開される段階にまで攻撃が到達するのを防止していることが理由だと考えられます。この攻撃クラスタを実行しているグループは、主にスパイ活動に従事していると考えられますが、副業的として時折、金銭的な利益を得るためにランサムウェアを展開している可能性もあります。ShadowPad は中国とつながりのあるサイバー攻撃グループにのみ販売されているため、ESET はこの活動を、まだ正体が明らかになっていませんが、中国とつながりのある攻撃グループによるものであると確信しています。

最後になりましたが、重要な情報として、Mustang Panda はヨーロッパの組織を標的としており、ヨーロッパで活動している中国系グループの中で最も活発に活動していることが挙げられます。同グループは引き続き海運業界と政府機関を中心に攻撃を行っています。Mustang Panda は、悪意のある USB ドライブを利用し続けており、さまざまなファイル形式やプログラミング言語を試行しながら、引き続き Korplug ローダーを使用しています。ESET は、ノルウェー、オランダ、イギリス、ブルガリア、ギリシャ、デンマーク、ポーランド、ハンガリーで、MSC ダウンローダーと同様に、Delphi、Go、Nim ベースの Korplug ローダーを観測しました。

航空券をおとりとするサイバースパイ活動：UnsolicitedBooker によるフィッシングキャンペーン

ESET は、2023 年 3 月に中国とつながりのあるサイバー攻撃グループによるサウジアラビアの国際機関への侵入を初めて発見し、このグループを UnsolicitedBooker と命名しました。2024 年 3 月にも再びこのグループによる侵入を確認しています。同グループは、Chinoxy、DeedRAT、Poison Ivy、BeRAT など複数のバックドアを展開しています。これらのバックドアは、複数の中国系グループ間で共有されています。このグループはまた、独自のファイル窃取ツールを展開していることから、このサイバー攻撃グループの動機はスパイ行為とデータ窃盗であると考えられます。UnsolicitedBooker は通常、アジア、アフリカ、中東の政府機関を標的とし、航空券をおとりとしてスピアフィッシングメールを送信しています。ESET の調査によると、UnsolicitedBooker は、**Space Pirates** および **Zardoor** バックドアを使用する不明のサイバー攻撃グループの両方と活動が重複しています。

最近では、2025 年 1 月に UnsolicitedBooker からのスピアフィッシングキャンペーンを検出しました。このサイバー攻撃グループは、2023 年および 2024 年にも標的となったサウジアラビアの同じ組織に対し、`saudia.etickets@outlook[.]com` というアドレスからフィッシングメールを送信しました。このメールの件名は、`「サウディア航空の航空券をダウンロードできます」` となっています。図 1 に、サウディア航空を装ったフィッシングメールの本文の日本語訳を示します。

> *XXX 様、*
>
> *サウディア航空の航空券が発行されたことをお知らせいたします。*
>
> *ご旅行に必要な航空券を添付いたしましたので、ご確認ください。*
>
> *サウジアラビア航空をお選びいただき、誠にありがとうございます。*
>
> *お客様をお迎えし、快適で楽しい旅行体験をご提供できることを楽しみにしています。*
>
> *ご質問やご不明点がございましたら、どうぞご遠慮なくご連絡ください。*
>
> *心よりお待ち申し上げております。*
>
> *サウディア航空カスタマーサービスチーム*

図 1. フィッシングメールの本文

Microsoft Word の文書がメールに添付されており、おとりのコンテンツは改変された航空券ですが、学術研究を共有するプラットフォームであり PDF ファイルのアップロードが可能な Academia の Web サイトで公開されていた PDF を元にしています（図 2 を参照）。

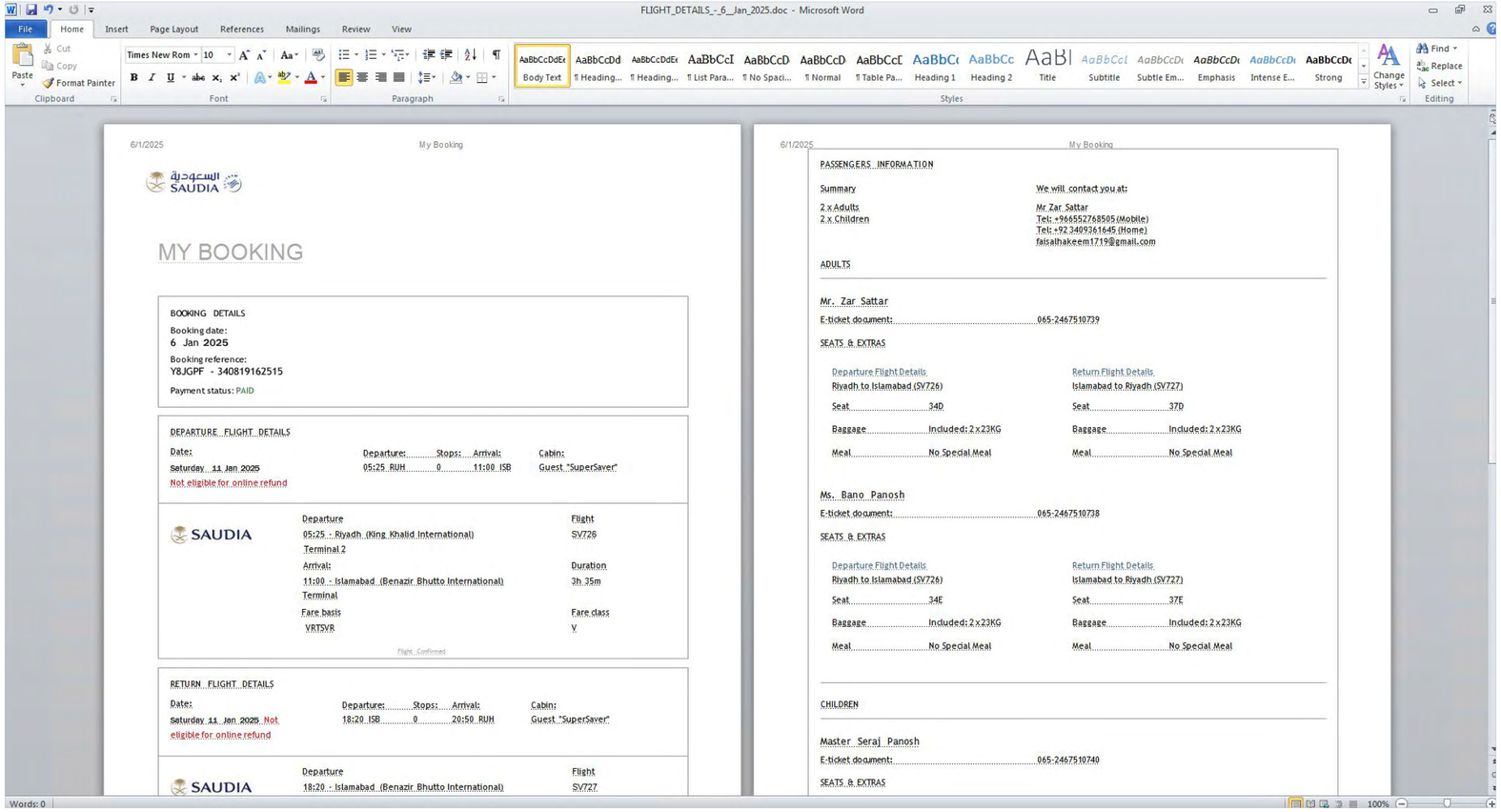


図 2. UnsolicitedBooker が使用したおとり文書

注目すべきなのは、2024 年に同グループが使用していたおとりの文書の 1 つは、同じ元の航空券をベースにしていたことです。

この文書には、VBA マクロが含まれており、ペイロードを復号して `C:\ProgramData\smssdrvhost.exe` に書き込みます。このペイロードは、バックドアのローダーであり、開発者は MarsSnake と呼んでいます。この根拠は、ローダーの PDB パス「`D:\yu_project\MarsSnake\bin_shellcode\load_http_64.pdb`」とバックドアの PDB パス「`D:\yu_project\MarsSnake\x64\http\MarsSnake.pdb`」に「MarsSnake」が含まれていることです。C&C のドメインは、`contact.decenttoy[.]top` です。

同じ組織では、さらに 2 つのフィッシング攻撃が検出されています。最初のフィッシングメールは侵害されている可能性があるアドレスから送信されており、その件名（日本語訳）は「サウジアラビアの新しい経済都市が製造業をさらにサステナブルにする」となっています。もう 1 件のフィッシングメールの件名（日本語訳）は「ファイルチェックのお願い」でした。

2023 年、2024 年、そして 2025 年に同組織の侵害を何度も試行していることから、UnsolicitedBooker がこの組織を重要な標的にしていることは明らかです。

Worok の最新情報

2022 年に ESET は、Worok についてのブログを **WeLiveSecurity** で公開しました。Worok は、中国とつながりのあるサイバースパイグループであり、2021 年の初めに ProxyShell の脆弱性（**CVE-2021-34523**）が公開されたときに、その脆弱性を攻撃していた同グループの活動を初めて観測しました。Worok は、おそらく別のデジタルフォーターマスターから入手した、同じスパイ機能を持つツールセットを使用しています。HDMan（別名 EAGERBEE）と PhantomNet は、中国とつながりのある APT グループの間で共有されているよく知られたツールセットであり、Worok の多くの作戦で同時に展開されています。Worok は、ESET が Sonifake と命名したツールセットも使用しています。Sonifake は、**BackdoorDiplomacy** などの複数の中国系 APT グループによって使用されています。高度に難読化されているバックドア **Impersoni-fake-ator** と **RUDEBIRD** もこのツールセットに含まれています。

最初のブログを公開して以来、ESET は引き続きこのサイバー攻撃グループを追跡しており（詳細は「**APT 活動レポート 2023 年第 2 四半期～第 3 四半期**」を参照）、Worok がモンゴル、キルギス、トルコ、台湾、タイのさまざまな業種の組織を標的にしていることを確認しています。これらの標的には、民間企業だけでなく、政府機関や公共部門の組織も含まれます。

昨年 11 月に、Worok はこれまでに特定および文書化されていないバックドアによって英国の学術機関を標的にしました。ESET はこのバックドアを XMLDoor と命名しました。Worok は XMLDoor を 2021 年から使用し続けています。最近では、Worok がカンボジアの政府機関に対して、GoFighting バックドアの更新版を展開しているのを確認しました。GoFighting は、同グループが以前使用していた PowHeartBeat バックドアを再実装したものであり、ESET は WeLiveSecurity のブログで解説しています。この新たな亜種では、Dropbox を利用するネットワーク通信手法が導入されています。なお、Worok が Dropbox を利用したマルウェアを展開するのはこれが初めてではなく、2022 年 11 月に **Avast** が報告した DropboxControl という C# で記述されたバックドアでも同様の手法が確認されています。

これまでの ESET の調査結果や公開されている他のレポートを精査した結果、中程度の確度で、他の研究者が別のグループが実行主体だと述べていた複数のキャンペーンは、Worok によって実行されたと判断しています。

- 2023 年 2 月に日本のコンサルティング会社を標的とした攻撃。日本のセキュリティ企業「LAC」によって**報告**されており、当初は中国とつながりのあるサイバー攻撃グループ（LuckyMouse および TA428）に関連付けられていました。
- 2023 年 11 月に Elastic によって**報告**された、東南アジアの政府機関に対する攻撃。コードネーム REF5961 が付けられています。Elastic は、これらの活動を LuckyMouse と TA428 と関連付けています。
- 2023 年 3 月から 2023 年 10 月にかけて南アジアの政府機関を対象に実施された Crimson Palace 作戦と呼ばれる攻撃。これは Sophos によって**報告**されています。これらの活動はクラスタアルファとして追跡されており、BackdoorDiplomacy、Worok、TA428、REF5961（ すべて中国系の攻撃グループ）に関連付けられています。

これらのレポートを ESET が検証したところ、これらの攻撃は実際に Worok の活動と密接に一致していることが判明しました。攻撃者に関する主張が異なっている主な理由は、Worok が PhantomNet や HDMan のようなツールを頻繁に使用していることですが、これらのツールは複数のグループ間で共有されています。一方で、Crimson Palace 作戦を Worok および BackdoorDiplomacy の両方に関連付ける見解について、ESET は同意しています。このことから、Worok と BackdoorDiplomacy の両グループが連携している可能性があります。ESET のテレメトリでは、両グループが標的を共有していたことを示す活動は確認されていませんが、公開された情報によれば、両者は Crimson Palace 作戦の実行期間中、同一のネットワーク内で活動していたことが示されており、ESET の調査でもそれが裏付けられています。

イラン

OilRig BladedFeline Lyceum GalaxyGato MuddyWater CyberToufan

イランとつながりのある APT グループによる活動の概要

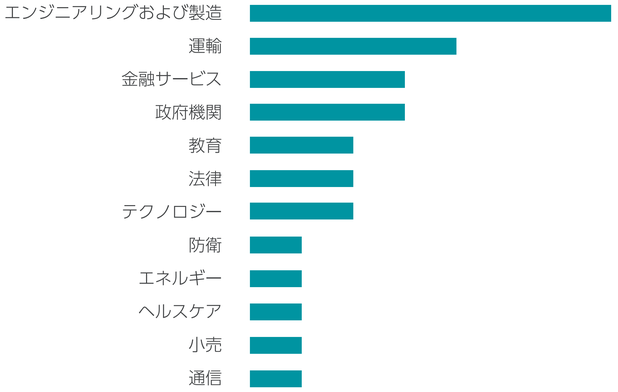
2024 年第 4 四半期から 2025 年第 1 四半期にかけて ESET の研究者は、イランとつながりのあるサイバー攻撃グループである OilRig（およびその傘下の BladedFeline と Lyceum）、GalaxyGato、MuddyWater、および CyberToufan によるキャンペーンを追跡してきました。

繊細さに欠ける攻撃

MuddyWater は、ESET の研究者が追跡しているイラン系の APT グループの中で、最も活発に活動を続けています。また、攻撃の痕跡や不審な挙動を非常に多く残しており、通常、ESETのセキュリティソフトウェアによって簡単に検出されています。特定のキャンペーンでこのグループは、デフォルトで Atera、Level、PDQ、SimpleHelp、Syncro、および Tactical RMM といった正規のリモート監視・管理（RMM）ソフトウェアを使用しています。これらのツールは通常、スピアフィッシングメールを通じて配信され、メールにはファイルホスティングサービス（特に OneHub や Mega）へのリンクが含まれており、そのリンクは多くの場合 PDF ファイルに記載されています。

ESET は、ネットワークインフラが少なくとも毎月更新されているのを確認しており、4 つの異なるキャンペーンを検出して報告しています。2 つのキャンペーンは典型的な MuddyWaterの攻撃パターンに従っており、1つは他のイラン系グループと共同で実行したキャンペーンです。もう 1 つは新しい注意が必要なキャンペーンであり、MuddyWater はインジェクターを使用してバックドアをメモリに動的に読み込み、ディスクに保存しない手法で、セキュリティソフトウェアを回避しようとしていました。このキャンペーンは、2024 年の 9 月から 10 月まで 2 か月間続き、イスラエルのエンジニアリング企業と政府機関を標的にして被害をもたらしました。

2025 年 2 月に実行された典型的な 2 つの MuddyWater のキャンペーンでは、新しい手法や注意が必要なマルウェアは使用されていませんでしたが、標的がこれまでとは異なっています。カンボジアとケニアの組織が被害を受けており、これらの国に対してイラン政府が外交的働きかけを行った直後に攻撃が発生しています。イランとつながりのあるサイバー攻撃グループは、その能力をあくまでサイバースパイ活動に限定して使用しており、これまではいかなる物理的な作戦の支援には使用していないと考えられてきました。ESET の APT 活動レポート 2024 年第 2 四半期～第 3 四半期では、物理的な作戦の準備に使用されていた可能性がある運輸業界を標的としたいくつかの攻撃について解説しましたが、実際には物理的な作戦のための攻撃ではなかったことが分かりました。



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

第 4 のキャンペーンは 2025 年 1 月と 2 月に実行されました。このキャンペーンが注目されたのは、MuddyWater による侵害の後に、Lyceum（OilRig 傘下のグループ）がイスラエルの製造業企業のシステムへのアクセス権を獲得しており、グループ間の協力とインフラやツールの共有を伺わせる動向があったためです。MuddyWater は、RMM インストーラ（Syncro）へのリンクが記載されたスピアフィッシングメールを介して最初の侵害を行いました。その後、MuddyWater は別の RMM（PDQ、MuddyWater が最近利用し始めた RMM）をインストールしました。MuddyWater のオペレーターは、Windows のシェルコマンドのセッションを手動で実行して、膨大な痕跡を残し、作戦上の目的はほとんど達成できませんでした。最後に、MuddyWater はカスタムローダーとインジェクターを使って Mimikatz を展開しました。同日に、Lyceum は組織内部で自由に攻撃を実行できる状態になりましたが、おそらく Mimikatz を使って入手した認証情報を使用したと考えられます。ESET は以前に MuddyWater がイラン系のグループのアクセスブローカーとして活動している可能性について説明しています。

リバーストンネルの利用の広がり

MuddyWater は、長年にわたり GitHub 上の Go 言語で作られたリバーストンネル（内部ネットワークから外部へトンネルを確立し、ファイアウォールを迂回してリモート操作を可能にする手法）を使用してきたグループですが、その傾向は Lyceum にも広がっていると考えられます。しかし、Lyceum はわざわざ C#/.NET で独自のリバーストンネルを作成しています。Lyceum は、このリバーストンネルを使用して 2025 年 1 月にイスラエルの組織（詳細は不明）を侵害し、続いて 2 月には、複数の攻撃者グループに侵害されていた別のイスラエルの組織への攻撃を開始しました。このリバーストンネルは、別の設定ファイルを使用するローダーから展開されています（設定ファイルには悪意のあるコンテンツが含まれておらず、検出を回避できるため）。これは、OilRig とその傘下のグループ（BladedFeline を含む）が頻繁に用いている戦術です。

両方のキャンペーンでは、通信中のデータに対して簡易なカスタム暗号化アルゴリズムが使用されており、ローカルのポート 3389（RDP）および 445（SMB）を開いて、ハードコードされたリモートポート 1500 または 10443（3389 とペア）、および 15475（445 とペア）へと接続するリバースシェルが使われていました。2 つ目のキャンペーン（MuddyWater と共同して行われた攻撃）では、リバーストンネルがアップデートされました。Lyceum はリバーストンネルの機能を 1 つのモジュールから 2 つに分割し、設定ファイルの形式を変更しています。いずれのアップデートも、ESET のセキュリティ製品が元のバージョンを検出したことへの対応であると考えられます。

復活した古いバックドア

2024 年 11 月 ESET は、2019 年に Talos によって初めて報告された OilRig の古いバックドア「Karkoff」の新しいバージョンをレバノンの VirusTotal ユーザーから発見しました。この新バージョンには以下の機能が追加されています。

- 難読化されたクラス
- スクリーンキャプチャ
- 特定のファイル拡張子があるファイルの列挙（`.pdf`、`.txt`、`.png`、および `.jpg`）

Karkoff の以前のバージョンは、OilRig によってレバノンの被害者を標的に使用されていました。この攻撃は今も続いています。

通信企業への攻撃

BladedFeline は、以前（2022 年 4 月）にウズベキスタンの通信企業を侵害しています。2025 年 3 月、ESET は、BladedFeline の TTP（戦術 / 技術 / 手順）と一致する活動を検出しました。この活動は、同じ企業を標的にし、PowerShell コマンドを駆使した VBScripts を使用して、被害者のシステムを列挙してバックドアのような機能を提供するものでした。MuddyWater は、長きにわたってバックドアのような機能を持つ PowerShell スクリプトを使用していることから、BladedFeline が MuddyWater からこの戦術を習得した可能性があります。あるいは、この侵害は MuddyWater が BladedFeline のためにアクセス権限を再度取得した結果である可能性もあります（ただし、この仮説を裏付ける具体的な根拠はありません）。

以前の被害者を再び侵害したことに加えて、BladedFeline はウズベキスタンの別の通信会社を標的にして侵害した可能性があります。これらの侵害を予兆するかのように、イランとウズベキスタンは 2025 年 2 月に外交関係を深め、イランとウズベキスタン間を移動する輸送車両に対する **400 米ドルの通行料を免除**しました。外交交渉がイラン系 APT グループによるサイバースパイ活動の前兆となる可能性は今後もあるでしょう。

注意が必要な C&C との通信方法

GalaxyGato は 2024 年 9 月に C&C との通信のために新しいドメイン `virgomarketingsolutions[.]com` を立ち上げました。約 1 週間後の 2024 年 10 月に ESET は、イスラエルから VirusTotal にアップロードされた GalaxyGato ZIP アーカイブを検出しました。そのアーカイブには 3 つのファイルが含まれていました。1 つは正規の目的で使用される実行可能ファイルで、他のファイルの 1 つ（ローダー）をサイドロードするために使用され、そのローダーが 3 つ目のファイル（バックドア）をロードします。このバックドアは MINICHOPPER と呼ばれ、Mandiant によって最初に報告された MINIBIKE と共通点があります。

注意すべきなのは、バックドアよりも C&C との通信方法です。MINICHOPPER は URL（`https://virgomarketingsolutions[.]com/news/photos/<victim_id>`）と POST リクエストを C&C との通信に使用します。どちらも特に新しい手法ではありませんが、両方を組み合わせ、さらに MuddyWater などの他のイラン系グループによる類似の活動と合わせて見ると、興味深いパターンが浮かび上がってきます。イラン系グループは、正規のトラフィックを装って紛れ込み、検知を回避していると考えられます。新たに登録されたドメインはセキュリティオペレーションセンター（SOC）で検知されやすい一方で、C&C を Web サーバーのディレクトリ内に深くネストさせることで、正規の活動のように見せかけることができ、防御側の担当者が詳細に調査するのを思いとどまらせる可能性があります。

CyberToufan

CyberToufan は 2025 年 1 月、イスラエルの 50 の組織に対してワイパー型マルウェアを使用した攻撃を行いました。このワイパー型マルウェアは、図 3 に示すように「Flood」という用語が使われていることや、ワイパー型マルウェアが突如出現したことに基づいて、ESET は「FlashFlood」と命名しました。このワイパー型マルウェアは、2023 年 10 月にハマスがイスラエルを攻撃した際のプロパガンダを利用していました（図 3 を参照）。

興味深いことに、CyberToufan は暗号化された文字列や API 関数名を復号するための鍵として、「`Saturday, October 07, 2023, 6:29:00 AM`」というフレーズを使用していました（これは、ハマスによるイスラエルへの攻撃が開始された時刻です）。

図 3. CyberToufan のワイパー型マルウェアによって設定されたデスクトップの背景

北朝鮮

DeceptiveDevelopment TraderTraitor Operation DreamJob Kimsuky Konni ScarCruft Andariel

北朝鮮とつながりのある APT グループの活動の概要

北朝鮮関連のグループによる最も注意が必要であり目立った活動は、DeceptiveDevelopment と Bybit によるハッキングです。Kimsuky と Lazarus の活動はこれまでと比較すると少なくなっています。

DeceptiveDevelopment の活動の広がり

DeceptiveDevelopment は北朝鮮とつながりのあるサイバー攻撃グループであり、金銭を獲得する活動を重視しています。DeceptiveDevelopment のオペレーターは主に金銭的な動機で、暗号通貨を窃取するために Windows、Linux、macOS のソフトウェア開発者を標的にしていますが、サイバースパイを二次的な目的としている可能性もあります。

この半年間、ESET は、このサイバー攻撃グループがさらに広範な個人を標的にしていることを観察してきました。ESET の調査では、暗号通貨、ブロックチェーン、金融関連（Coinbase、Binance、Etoro、Okcoin、Kraken、RobinHood など）を中心に、著名な業界リーダー企業から比較的小規模なスタートアップ企業まで、数十社にわたる企業の偽の求人情報が確認されました。また、Barrow Wise、Bitwise、Pantera といった投資会社や、Halliday のような革新的なテクノロジーを提供するスタートアップ企業も含まれていました。また、この攻撃グループは暗号通貨企業の経営者を標的にし、事業協力に関心のある投資家を装って接触していたことも確認されました。これは、2025 年 3 月に X への投稿で報告しています。

この攻撃グループは、特定の選択基準もなく、地理的な場所にも拘らず、広く標的を選んでいると考えられます。

ESET は前回の APT 活動レポートで説明したソフトウェアのコードベースにトロイの木馬を組み込む攻撃手法の他にさらに 2 つの攻撃手法を検出しました。その 1 つは、近年広く悪用されるようになってきた ClickFix 型のソーシャルエンジニアリング手法であり、もう 1 つはオープンソースプロジェクトで悪意のあるコードをプロジェクトに組み込ませるために、意図的にバグや機能追加要求などの虚偽の問題（イシュー）を報告する手法です。

ClickFix 攻撃では、攻撃者は被害者を有名なビデオ会議サイトや採用プラットフォームを装ったサイトに誘導し、マイクが動作していないことを標的のユーザーに信じ込ませ、その問題を「修正する」ように指示します。そして、被害者に一連のコマンドをコピーしてターミナルに貼り付けるように促します。

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

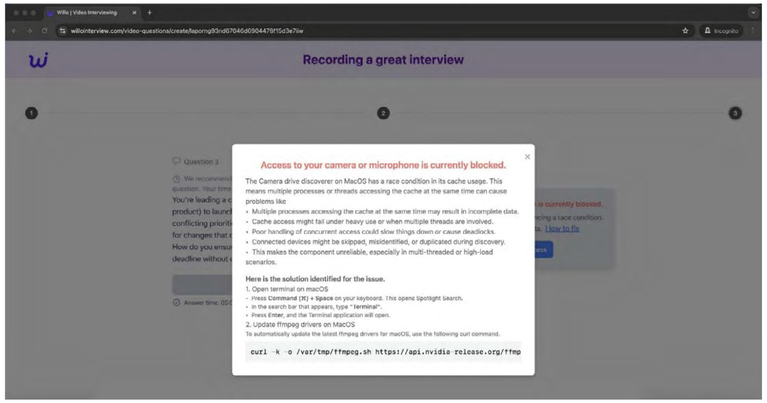


図 4. 偽の Willo ウェブサイトに求人情報を表示し、候補者にビデオで回答を録画するよう求め、さらに ClickFix メッセージを表示して、被害者にシェルコマンドを実行させて WeaselStore マルウェアをダウンロードして実行させようとする（出典：@tayvano_ の[ツイート]）。

公開リポジトリを利用して標的を誘引する手法では、攻撃者は有名なプロジェクトで公開されている GitHub リポジトリにイシューを立てて、一般的な偽の問題を説明して、同様の ClickFix 指示を含む解決策を提供します。

これら 2 つの手法はいずれも、Go で記述された新しいマルチプラットフォーム対応のバックドアと情報窃取の両方の機能を実装したマルウェア「WeaselStore」を配信するために使われていました。WeaselStore マルウェアは、過去の DeceptiveDevelopment キャンペーンで使用された **BeaverTail や InvisibleFerret** などの情報窃取型マルウェアと類似した機能を備えています。具体的には、Chrome ブラウザに保存されたデータ、MetaMask ウォレット拡張機能のデータ、ローカルのキーチェーンのデータを外部に送信して窃取する機能があります。別のマルウェアは、ブラウザやカメラに関連するアプリを偽装しており、macOS でユーザーに偽のパスワード入力プロンプトを表示します。これによりアカウントのパスワードが窃取され、その後 macOS のキーチェーンに保存されたログイン情報の復号に使用されます。

図 5. 有名なリポジトリの GitHub のイシューに攻撃者が投稿した ClickFix 型の悪意ある作業指示

Bybit のハッキング

2025 年 2 月 21 日、世界第 2 位の規模の暗号通貨取引所である Bybit から、40 万 ETH 以上およびその他の暗号通貨（当時の時価で約 15 億ドル相当）が**盗まれました**。FBI は、このインシデントを実行したのは TraderTraitor グループであることを特定しました。

このサイバー攻撃グループは、Bybit のコールドウォレットからホットウォレットへの ETH のマルチ署名のトランザクションを傍受して改ざんしました。この攻撃者は、影響を受けたコールドウォレットを制御し、そのウォレットの保有資産を攻撃者が管理するウォレットに転送することに成功しました。注意すべきなのは、これらの攻撃者が利用した手法です。

攻撃者は Bybit を直接攻撃するのではなく、暗号通貨業界の大手企業の一部で使用されている人気のマルチ署名ウォレット「Safe{Wallet}」の開発者を標的にしています。**Safe の声明**によると、攻撃者は Safe{Wallet} の開発者の 1 人が使用しているマシンを侵害しています。侵害したマシンを起点として、この攻撃者はブロックチェーンでのトランザクションへの署名に使用される `app.safe.global` フロントエンドの一部である JavaScript ファイルを変更しました。この悪意あるインプラントは、特定の条件下でのみ実行されるように特別に細工されています。その後、攻撃者はこの悪意のあるインプラントを使用し、ソーシャルエンジニアリングと組み合わせることで、Bybit の従業員にスマートコントラクトのアップグレードを承認させました。このアップグレードには悪意のあるコードが含まれており、ETH や ERC20 トークンが攻撃者の管理するウォレットに送金されるようになっていました。

サプライチェーン攻撃は、依然として検知と対処が非常に難しいサイバー脅威の 1 つであり、Bybit のハッキングはこれまでで最も影響の大きいインシデントの 1 つと言えます。

高待遇の求人を今でも悪用

過去 6 か月間にわたり、「DreamJob 作戦」の活動が継続して観測されています。この作戦は主に EU 諸国の防衛・航空宇宙関連企業の従業員を標的にしています。攻撃手法や TTP（戦術 / 技術 / 手順）はほとんど変わっておらず、攻撃者は LinkedIn やその他の求人プラットフォームを通じて、高待遇の求人情報を提示し、標的ユーザーに接触します。これらの標的ユーザーの信頼を得ると、攻撃者はマルウェアを仕込んだアーカイブファイルを送信します。このファイルには通常、トロイの木馬化された PDF ビューアと、おとりの PDF 文書が含まれています。

韓国でのスピアフィッシング

2024 年の終わりから 2025 年の初めにかけて、Kimsuky と Konni の両方の活動が減少しましたが、2025 年 2 月と 3 月には通常のレベルに戻りました。しかし、両グループのキャンペーンの標的が大きく変化しており、初期アクセスの手法も変化しています。

前回の APT 活動レポートでは、Kimsuky が英語圏のシンクタンク、NGO、北朝鮮の専門家へのインタビュー依頼を装って、積極的に標的を絞っていたことを指摘しました。このようなキャンペーンは減少傾向にあります。過去 6 か月間、Kimsuky と Konni が実行したとされるキャンペーンの大半は、韓国の個人や企業、韓国にある大使館や外交関係者を標的にしていました。

Konni は、税金、警察、その他の行政関連をテーマにした一般的なスピアフィッシングメールを多く使用していますが、Kimsuky のフィッシングメールは、時事問題をテーマにしたり、本物の文書をおとりとして使用したりするなど、標的に合わせてさらにパーソナライズされています。おとりとして使用されている文書は、以前に侵害されたマシンから流出した可能性が高いです。スピアフィッシングメールは、Windows ショートカット（LNK）ファイルを配信するために使用され、侵害を次の段階に進めます（PowerShell、JavaScript、VBScript を組み合わせた攻撃）。

Kimsuky は C&C サーバーにクラウドサービスを引き続き使用しており、Dropbox と Google Drive が最も多く悪用されています。また、ESET は攻撃者が GitHub の非公開リポジトリを悪意のあるスクリプトの配信や窃取したデータの流出に利用したケースについても報告しています。一方、Konni は、C&C として使用する目的で侵害したサードパーティの Web サーバーを使い続けており、独自の Web サーバーを導入したケースも確認されています。

ScarCruft は引き続き、ペイロードを埋め込んだ HWP 文書を使用し、攻撃にはソーシャルエンジニアリングを利用していました。2024 年 11 月、ESET は韓国語を話す団体が中国で侵害された事例を報告しました。このときには RokRAT が使用され、より複雑なバックドアである BirdCall がインストールされた可能性が高いです。このバックドアは、複数の侵害された韓国の Web サイトを C&C サーバーとして使用するように設定されていました。

2025 年 2 月、ESET は 1 年ぶりに Andariel グループによるサイバー攻撃を観測しました。韓国で産業用ソフトウェアを開発している企業が、未知の初期アクセス手法による攻撃を受けました。攻撃者は、NirSoft の WebBrowserPassView、キーロガー、Windows イベントログを操作するツール、そして Andariel の TigerRAT を思い起こさせる TCP バックドアを展開しました。以前の亜種と比較すると、バックドアのコードは大幅に変更されており、この期間中に同グループが開発に集中的に取り組んでいたことを示唆しています。

ロシア

Sednit RomCom Gamaredon Sandworm

ロシアとつながりのある APT グループによる活動の概要

過去 6 か月間、ESET はロシアとつながりのあるサイバー攻撃グループによる多くの活動を分析してきました。これらのグループは、主にウクライナと EU 諸国を標的にしており、初期アクセスを取得するためにスピアフィッシングメールを使用しています。さらに、XSS エクスプロイトを使用して Web メールサーバーを攻撃し、新たに特定されたケースではゼロデイの脆弱性も利用していました。これらの攻撃の通常の目的はスパイ活動ですが、Sandworm はデータの破壊を重要な目的としています。

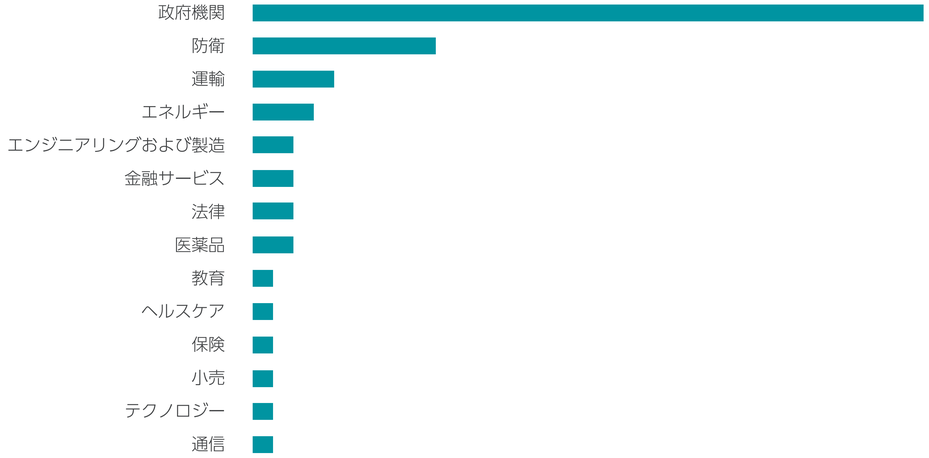
XSS を悪用する手法を巧みに使いこなす Sednit

ロシアとつながりのあるサイバースパイグループは、セルフホスト型 Web メールサーバーを標的にし続けています。例えば、Sednit が実行した RoundPress 作戦では、Roundcube だけではなく、Horde、MDaemon、および Zimbra などの他のいくつもの Web メールサービスにまで攻撃対象を広げています。RoundPress 作戦を背後で操っているこの攻撃者は、XSS エクスプロイトを仕込んだスピアフィッシングメールを送信しており、通常はパッチが適用されている脆弱性を攻撃しています。

このエクスプロイトにより、ブラウザウィンドウで実行されている Web メールクライアントの Web ページで悪意のある JavaScript コードが実行されます。ESET は、SpyPress.HORDE、SpyPress.MDAEMON、SpyPress.ROUNDCUBE、および SpyPress.Zimbra などのいくつかの JavaScript ペイロードを特定しました。これらの SpyPress ペイロードの大半は、脆弱な Web メールクライアントが悪意のあるメールを受信または表示するときに、被害者の受信箱からメールメッセージと連絡先情報を収集します。これらのデータは、C&C サーバーに送信されます。

ESET は、ブルガリアとウクライナにある防衛関連企業に対する Sednit のキャンペーンをいくつか検出しました。

例えば 2024 年 11 月に ESET は、ブルガリアの企業を標的としたスピアフィッシングメールを検出しました。このフィッシングメールは、侵害されたメールアドレスから送信されており、件名は「Путин се стреми Тръмп да приеме руските условия вдвустранните отношения（日本語



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

訳：プーチン、二国間関係におけるロシアの条件を受け入れるようトランプに働きかけ)」となっていました。メッセージ本文（図 6 を参照）には、ブルガリアの信頼できる新聞である News.bg の記事の引用 (ブルガリア語) とリンクが含まれています。

図 6. バックグラウンドで XSS の脆弱性をトリガーする Sednit のおとりメールの内容

2024 年 11 月 1 日に ESET は、ウクライナの企業を標的としたスピアフィッシングメールを検出しました。これらのメールは、**MDaemon メールサーバー**に存在するゼロデイの XSS 脆弱性を悪用しています。この脆弱性は、メールメッセージに含まれる信頼されない HTML コードのレンダリング処理に存在します。

ESET は、この脆弱性を 2024 年 11 月 1 日に開発元に報告し、その後**バージョン 25.4.1** が 2024 年 11 月 14 日にリリースされ、この脆弱性が修正されました。ESET が報告したこの脆弱性には、**CVE-2024-11182** が割り当てられました。

RomCom が 2 つのゼロデイを展開

Storm-0978、Tropical Scorpius、UNC2596 などとも呼ばれている RomCom は、サイバー犯罪とスパイ活動の両方に重点を置いており、サイバースパイを専門とするグループとは一線を画しています。このロシア系グループは、さまざまな業界に対して、場当たり的なキャンペーンと、標的型のスパイ作戦キャンペーンの両方を実行しています。RomCom は少なくとも 2022 年から活動しており、**Cuba ランサムウェア**の展開に関与していると指摘されており、**ウクライナ政府**、**ウクライナの防衛産業**、NATO 加盟国、そして欧州の政府機関を標的にしてきました。このグループは、フィッシングキャンペーンやトロイの木馬化されたソフトウェアなど、さまざまな手口でマルウェアを展開しており、**SnipBot** のような新たな亜種を用いたり、人気の高いソフトウェアの脆弱性を悪用したりするなど、手法を絶えず進化させています。例えば、2023 年 6 月に、**RomCom** は、Microsoft Word に存在するゼロデイの脆弱性（**CVE-2023-36884**）を攻撃しています。

2024 年 10 月に ESET は、Mozilla 製品（**CVE-2024-9680**）と Microsoft Windows（**CVE-2024-49039**）に存在していたこれまで未知であった脆弱性が RomCom グループによって悪用されていたことを特定しました。これらのゼロデイ脆弱性は、エクスプロイトが仕込まれた Web ページにユーザーがアクセスしただけで、何も操作しなくても RomCom という同名のバックドアを展開するために使用されました。ESET は、これらの脆弱性の攻撃チェーンについて**詳細な分析結果**を公開しました。特に、Firefox のアニメーションタイムラインにおける Use-After-Free の脆弱性と、Windows タスクスケジューラにおける特権昇格の脆弱性について詳しく説明しています。ESET のテレメトリデータによると、これらのエクスプロイトは、最大 250 社の潜在的な被害者を標的にした、広範囲にわたるキャンペーンで使用されたと考えられます。この高度な開発能力は、ステルス機能を獲得または開発しようとする意志と能力をこのサイバー攻撃者が有していることを示しています。

Gamaredon の最新情報

Gamaredon は、ウクライナを標的とする攻撃を最も活発に行っている APT グループです。Gamaredon のツールは継続的に改良されており、難読化、ネットワークベースの検出回避手法、主要な機能に関連する数多くの変更が加えられています。

初期アクセスを取得するために、Gamaredon はアーカイブファイル（RAR、ZIP、7z）や、これらのアーカイブのダウンロードプロセスを模倣するために HTML スマグリングの手法を使用する XHTML ファイルを添付したメールを送信します。これらのアーカイブには、`mshta.exe` を起動して別の HTA ファイルをダウンロードする HTA ファイルまたは LNK ファイルが含まれており、その HTA ファイルには追加のペイロードを取得するための VBScript ダウンローダー「PteroSand」が含まれています。2024 年 10 月 Gamaredon は、スピアフィッシングキャンペーンで HTA ファイルを大幅に難読化し始め、空白行、未使用の文字列変数、および偽の C&C サーバーを追加しています。

ESET のテレメトリと VirusTotal の統計によると、Gamaredon は 2024 年の下半期に大幅に大規模化したキャンペーンを実施しています。特に、2024 年 10 月に Gamaredon は最も活発に活動しており、スピアフィッシングキャンペーンに使用された新しいユニーク検体数が最も多くなりました。

2024 年 11 月、ESET は Gamaredon によって展開された新たな悪意のあるツールを発見し、PteroBox と命名しました。これは PowerShell で記述されたファイル窃取マルウェアであり、Dropbox の API を使用して Dropbox にデータを流出させ、必要に応じてアクセストークンを更新します。USB ドライブや、「デスクトップ」や「ドキュメント」などの一般的なフォルダを監視し、特定の種類のファイルを探します。攻撃者の主に狙っているのは、Microsoft Office 文書、画像、PDF、アーカイブ、データベース、証明書、鍵などです。このマルウェアは、特定のファイルを避けており、その独自の方法ですでに窃取したファイルを追跡・管理しており、同じファイルを何度も窃取しないようにします。

Sandworm が使用する RMM ツールとデータワイプ型マルウェア

2024 年 10 月、ESET はウクライナの複数のエネルギー会社で Sandworm の活動を検知しました。少なくとも 1 つのケースにおいて、Sandworm が侵害の初期段階で、リモート監視および管理（RMM）ツール、具体的には **Atera Agent** を使用しているのを確認しました。Sandworm は、過去 6 か月間にわたってデータワイプ型マルウェアを使用する作戦を強化してきました。

2024 年 12 月、そして 2025 年 2 月と 3 月に再び、Sandworm はウクライナのさまざまな組織に ZEROLOT[1] という名前の新しいワイパー型マルウェアを展開しました。いずれの場合も、この攻撃者は Active Directory のグループポリシーを使用して、標的となった組織のコンピュータにこのワイパーを展開しています。一度実行されると、ZEROLOT は `C:\Users\` の以下にあるディレクトリと、`C:` ドライブを除くすべての論理ドライブのルートからすべてのファイルを消去します。ただし、拡張子が `.dll`、`.exe`、および `.sys` のファイルは除外します。ZEROLOT は、`fsutil.exe` を使用してファイルデータを上書きした後に、ファイルを削除します。さらに、Windows API の `DeviceIoControl` を使用して物理ドライブのレイアウトを削除します。

[1] SHA-1:4D4635D5DAB0E79AAEFAB0AD054627B9C154E051

その他の APT グループの活動

APT-C-60 Stealth Falcon

他の注意が必要な 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、日本を標的とした最近の APT-C-60 キャンペーンと、世界経済フォーラムをテーマとしたスピアフィッシングキャンペーンについて説明します。

イランとつながりのあるサイバー攻撃グループに加え、トルコやパキスタンにおける Stealth Falcon グループの活動など、中東系のサイバー攻撃グループの活動も観察されています。

日本を狙う APT-C-60

2025 年 2 月 28 日、悪意のあるショートカットと暗号化されたダウンローダーを含む VHDX ファイルが日本から VirusTotal[2] にアップロードされました。ESET はこのダウンローダーを RadialAgent と命名しています。RadialAgent は、韓国とつながりのあるサイバースパイグループである **APT-C-60** のみが使用していると考えられるマルウェア系統です。

このルートフォルダには、「メールリスト .rtf」や「会社系 .rtf」のような日本人が興味を引きそうなファイルも含まれています。1 つ目のファイルには、ハッカー集団 Anonymous が過去にリークした情報である在日本朝鮮人総聯合会（**朝鮮総連**）の**構成員 3,667 名のリスト**が含まれます。この団体は、北朝鮮との密接な関係があるとされています。

これは、APT-C-60 が北朝鮮と関係のある日本国内の人々を標的にして活動していることを示しています。

ダボス会議をテーマにしたフィッシングキャンペーン

2025 年 1 月、報道ジャーナリストの Christo Grozev 氏は、特定の標的に送られたフィッシングメッセージについて**ツイート**しました。そのメッセージは、ダボスで開催される世界経済フォーラムへの参加を確認するよう求める内容で、Signal を通じて送信されていました（図 7 を参照）。

標的となった人物がこのリンクをクリックすると、図 8 に示すフィッシングページが表示され、いくつかの個人情報を確認するように求められます。

標的のユーザーが「続行」をクリックすると、図 9 に示すように、標的となりうる人物の身元を確認するために電話番号を入力するように要求されます。

この Web サイトには、標的外の電話番号を除外し、攻撃対象となりうる人物をふるい分けるための許可リストが存在していました。このリストには、主にウクライナの政府関係者や外交官を含む 25 名の標的となりうる人物の氏名、職名、生年月日、電話番号が記載されており、フィッシングページのデザインの意図を説明する内容にもなっています。

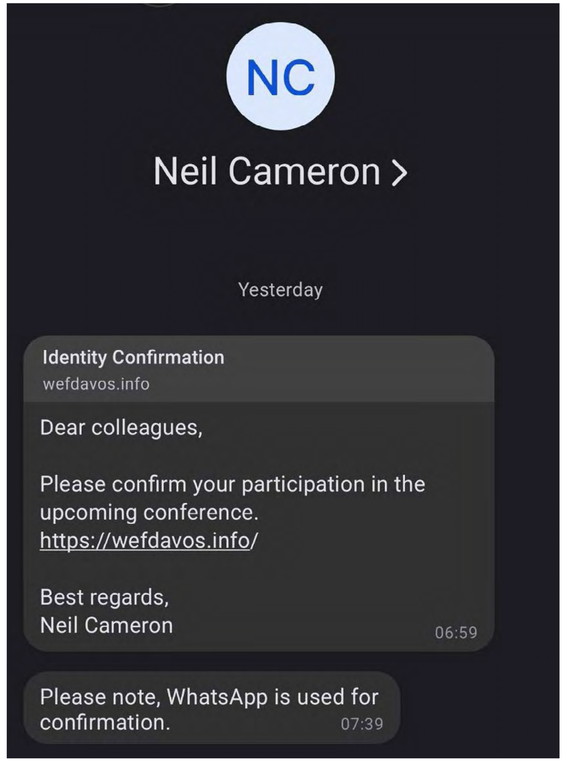


図 7. Signal で受信したフィッシングメッセージ
（出典：Christo Grozev 氏の**ツイート**）

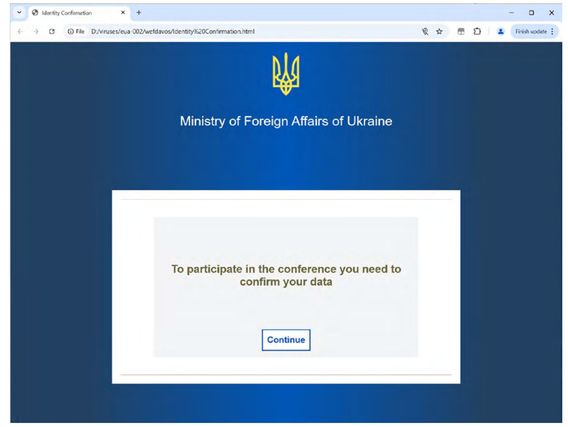


図 8. 個人情報確認のリクエスト

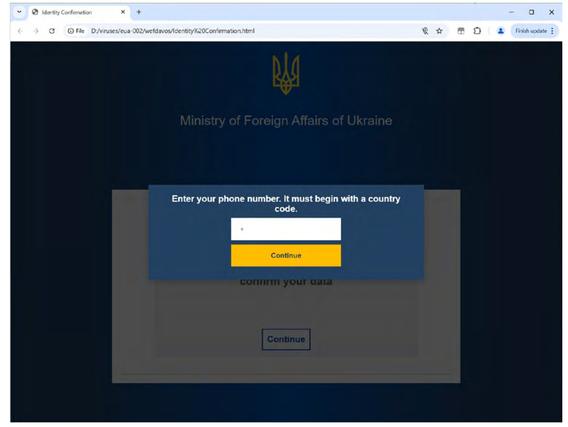


図 9. 電話番号の確認

[2] SHA-1:F32F07F2A4F019976B83088ED1D17B9D19A520CA

この Web サイトは、ユーザーデータも収集しており、アクセスしたユーザーの IP と地理情報をこのサイバー攻撃グループが管理する C&C サーバーに送信します。

1 月の翌日、もう 1 つの類似したフィッシングサイトが発見されました（図 10 を参照）。このサイトは gov-abh[.]org（南コーカサスに位置し、国際的にはジョージアの一部とされながらも一部で独立が認められているアブハジアの公式 Web サイト）を装い、gov-abh[.]site というドメインを使用していました。

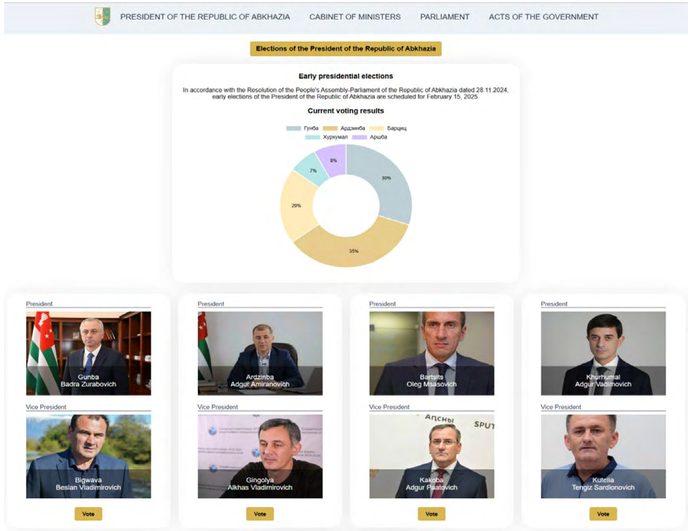


図 10. アブハジア共和国の選挙 Web サイト

どちらのフィッシングサイトも Cloudflare でホストされていましたが、今回は電話番号の許可リストは存在していませんでした。この Web サイトで大統領と副大統領の組み合わせの下にある「投票」ボタンをクリックすると、電話番号で身元を確認するように求められます（図 11 を参照）。国番号が +7 の番号は、ロシアとカザフスタンの電話番号ですが、有効であればどのような電話番号でも入力できます。

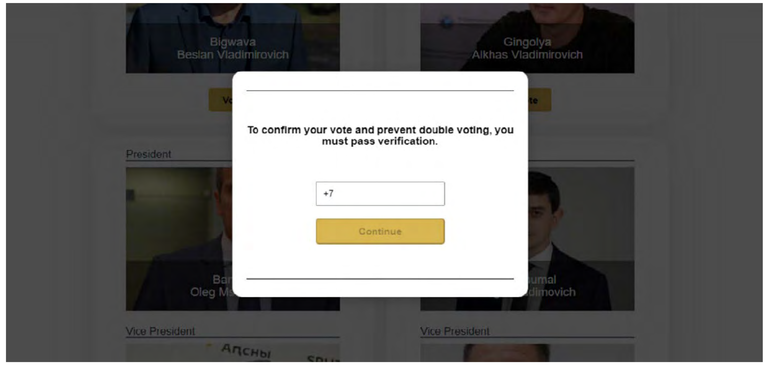


図 11. 電話番号のリクエスト

世界経済フォーラムの Web サイトと同じように、入力コードが記載されたメッセージが標的のユーザーに送信されます。

これらのキャンペーンは、標的を厳格に絞ったフィッシングであり、特に最初の機能では、あらかじめ定義されたリストと照らし合わせて標的を確認しており、標的となりうる人物から機密情報を盗むことを目的としている可能性が高いと考えられます。

Stealth Falcon

2024 年 10 月、Stealth Falcon は、トルコの被害者にインジェクターを展開しました。この被害者が VirusTotal にそのインジェクターをアップロードしました。このインジェクターは、ブラウザデータを窃取するツールを展開することを最終的な目的とする多段階のエクスプロイトチェーンの一部であり、特に中東を拠点とするサイバー攻撃グループが広く利用しています。この情報窃取ツールは、C#/.NET で作成されており、Chrome や Edge のような Chromium ベースのブラウザを攻撃します。収集されたデータは、AES-256-CBC で暗号化され、base64 でエンコードされたうえで、ネットワーク上のストレージに書き込まれ、別の手段で外部に送信されるための準備が行われます（エクスプロイトチェーンの中には、バックドアのような機能は含まれていません）。

別途、2025 年 1 月に ESET は、パキスタンでインジェクターとキーロガーを検出しました。これらは、おそらく 2020 年から 2023 年の間に作成されたものと考えられます。このキーロガーは、キーボードレイアウト情報を解析し、仮想キーコードを文字に適切に変換します。リガチャやデッドキーなども考慮しており、おそらくアラビア語のようなラテン文字以外の言語を対象にできるようにする意図があると考えられます。ここでも、Stealth Falcon はツールを分割していますが、検出を回避することを目的としていると考えられ、別の手段で情報を外部に送信します。

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** で最新の情報をご確認ください。

ESET 脅威インテリジェンス

ESET 脅威レポートと APT アクティビティレポート

ESET GitHub

@ESETresearch

WeLiveSecurity.com

Digital Security
Progress. Protected.

(eset):research