Presented by Trellix ADVANCED RESEARCH CENTER

February 2026

TRELLIX® SECONDSIGHT

THREAT HUNTING REPORT 日本語版

Insights gleaned from Trellix SecondSight, expert threat hunters, and a global network of telemetry and intelligence

TABLE OF CONTENTS

TRELLIX SECONDSIGHT THREAT HUNTING REPORT

Trellix Advanced Research Centerが作成した本レポートは、(1) Trellix SecondSightを含む複数の重要なデータソースから得られた、2025年に観測された重大な上位 5つのキャンペーンに関する脅威ハンティングの洞察、インテリジェンス、ガイダンスを強調し、(2) これらの種類のキャンペーンから防御するためのベストプラクティスを知らせ、可能にするための専門的かつ徹底的なケーススタディを作成しています。本レポートは、主に2025年7月1日から2025年12月31日までに取得されたデータと洞察に焦点を当てています。

INTRODUCTION（はじめに）

Trellix SecondSightは、Trellix製品のテレメトリーと継続的なグローバルな人的監視を組み合わせた脅威ハンティングサービスであり、「敵は完璧なテレメトリーを待たない、我々も待つべきではない」というシンプルな信念に基づいて構築されています。このレポートは、従来の検出では見逃されがちなものを発見するために、Trellixのインテリジェンスと現実世界のテレメトリーを組み合わせて、顧客と並行して日常的に活動する当社のハンターの取り組みを反映しています。最初の不正使用されたドメイン、異常なDLLロード、通常とは異なるOAuthフローなど、初期の兆候が重要であるため、このレベルの詳細に踏み込みます。これらは、侵害が事後調査されるのではなく、まだ阻止できる瞬間だからです。

当社の手法は、意図的に実践的で、敵に焦点を当てています。製品からではなく、キャンペーンと攻撃手法から開始し、攻撃者の行動を顧客の環境にマッピングして、組織が検出できると信じていることと、実際にネットワークで何が起こっているのかとの間のギャップを明らかにします。このレポートの各調査は、Trellixがどのようにして弱い信号をアクティブな操作に接続し、複数のデータソースを通じて検証し、リスクを軽減するための具体的なアクションに変換するかを示しています。このアプローチは、既知のシグネチャが一致するのをただ待つのではなく、攻撃者の意図を理解することを優先するプロアクティブ・ハンティングの基本的な理念 によって推進されています。

セキュリティ製品がアラートの発火を待つのに対し、脅威ハンターは敵に圧力をかけ、コンテキストを提供し、顧客が損害を軽減するためにより迅速に行動できるよう支援し、連携してセキュリティ運用チームにプロアクティブな防御を強化します。このレポートのケーススタディは、標的型スパイ活動からOAuthの悪用、ゼロデイエクスプロイトに至るまで、このアプローチを実際に示し、なぜプロアクティブ・ハンティングが現代の脅威に対する最も効果的な防御策の一つであるかを裏付けています。過去 6か月間にSecondSightで観測された何千もの脅威の中から、潜在的な影響、使用された手法、および顧客にとっての重要性から、この5つをハイライトしました。

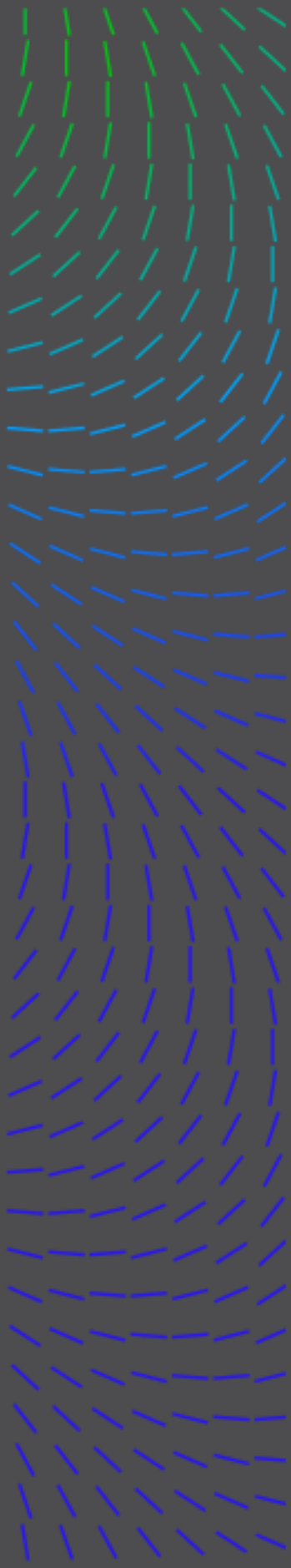
John Fokker
Vice President, Threat Intelligence Strategy, Trellix

HUNTING METHODOLOGY AND FRAMEWORK（調査手法）

SecondSightによるハンティングは、攻撃者が目的を達成する前に、意味のあるリスクを早期に特定するために設計された、構造化された優先順位付けフレームワークによって推進されています。当社のハンターは、アラートのみから開始するわけではありません。我々は、グローバルな状況全体で観測されたアクティブな脅威キャンペーン、敵の目的、および攻撃手法を継続的に評価し、そのインテリジェンスを顧客環境にマッピングして、どこに露出が最も存在する可能性が高いかを判断することから始めます。このアプローチにより、攻撃者の意図、能力、および機会が交差する場所に焦点を当てて努力を集中させることができます。

ハンティングの決定は、単一の指標ではなく、複数の信号によって知らされます。信頼度の低いアラート、異常な振る舞い、インフラストラクチャの再利用、および IDの悪用がまとめて評価され、関連性、信頼性、および潜在的な影響に基づいて重み付けされます。個々には、これらの信号は無害に見えるか、従来の検出閾値を下回る可能性があります。敵対的なコンテキストで組み合わせて配置されると、それらはしばしば初期段階の侵入活動、キャンペーンの準備、または信頼されたサービスの悪用を明らかにします。過去 6か月の例には、微妙なOAuthの悪用と既知のスパイ活動の手法との相関関係、またはデータアクセスが発生する前にラテラルムーブメントを露呈した、一見無関係なエンドポイントの振る舞いの連鎖が含まれます。

このフレームワークは、アナリストの判断を犠牲にすることなく一貫性を保証します。各ハンティングは、明確な決定ポイント（脅威インテリジェンスの関連性の検証、既知のテクニックとの行動の一致の確認、環境露出の評価、およびプロアクティブな顧客通知が正当であるかどうかの決定）を経て進行します。その結果、事後的な調査よりも早期の阻止を優先する、規律ある再現可能なアプローチが実現します。この手法は、効果的なセキュリティは生成されたアラートの数によって定義されるのではなく、意味のある影響を防ぐために意図、行動、およびコンテキストを時間内につなぎ合わせる能力によって定義されるという当社の信念を反映しています。



1 PERSISTENT WEB SERVER COMPROMISE: SHAREPOINT CVE-2025-53770 & COBALT STRIKE C2 INFRASTRUCTURE（SharePointのゼロデイ）

インシデントの概要

2025年7月、脅威アクターは、Microsoft SharePointの脆弱性（CVE-2025-53770）を悪用し、世界中の金融、医療、およびライフサイエンス組織を標的にして、永続的なウェブベースの侵害を確立しました。

2025年7月18日、脅威アクターはカナダの医療サービス組織を標的とし、w3wp.exeプロセスを通じてBase64エンコードされたPowerShellコマンドを実行しようと試みました。この特定の試みは永続的なウェブシェルを配備するには至りませんでしたが、SharePointのLAYOUTSディレクトリを標的とした活発なキャンペーンの兆候を示しました。

同時に、2025年7月18日から23日の間に、米国拠点の組織が多段階の侵入に成功しました。敵対者は、同じSharePointの脆弱性を利用して複数のウェブシェルをインストールしました。アクターはwhoamiとnetstatを使用して広範な偵察を実行し、機密性の高いシステムデータをZIPファイルにアーカイブして持ち出しのために準備し、sso-ishaansehgalという不正な管理者アカウントを作成することで長期的な永続性を確立しました。

2025年7月21日には、このキャンペーンはベトナムの金融機関に拡大し、攻撃者はOnline-TTDTホスト上の外部公開されたPHP-CGIアプリケーションを悪用しました。その結果、Cobalt Strikeビーコン（artifact_x64.exe）が配備され、IP 84[.]247[.]151[.]254への永続的なコマンド＆コントロール（C2）通信をポート1233経由で開始しました。これらの操作は、正規のウェブサーバープロセスを悪用し、高度なエクスプロイト後のエージェントを配備することを特徴としており、長期的なスパイ活動および潜在的なランサムウェアの配信を目的とした高リスク環境を浮き彫りにしています。

TTP Progression

Target	Status	Initial access (T1190)	Execution & persistence	Command & control
Canadian Health Services Organization	Exploitation attempt	**SharePoint exploit:** Adversary targeted host via CVE-2025-53770.	**PowerShell execution:** Used w3wp. exe to run $b64$- encoded commands	**Blocked phase:** Managed to execute code but failed to deploy persistent web shells.
U.S. Company	Successful compromise	**SharePoint exploit:** Adversary successfully exploited host.	**Persistence (T1505.003):** Installed web shells docssended. aspx and test. aspx.	**Data staging:** Archived sensitive files into F.zip and a.zip for exfiltration.
Vietnamese financial institution	Full compromise	**PHP-CGI exploit:** Exploited public-facing app on host.	**Admin Persitence** Created rogue local admin account and enumeration commands.	**C2 (T1071):** Deployed Cobalt Strike beacon with persistent check-ins to 84.247.151.254.

脅威ハンティングプロセス

容易に悪用可能なCVE-2025-53770の脆弱性がもたらす差し迫った高深刻度の脅威は、当社のチームに、堅牢な検出方法を確立するために、その悪用ベクトルをプロアクティブに調査するよう促しました。この分析により、複数の脅威アクター間で一貫したエクスプロイト後のパターンが明らかになりました。それは、Base64エンコードされたコマンドを実行するPowerShellインスタンスの生成です。この重要な洞察は、SharePointサーバーの実行を担うw3wp.exeプロセスから発せられる異常なPowerShell実行へと当社の脅威ハンティングを導きました。顧客のテレメトリーに対してこの特定の検出機会を活用することで、PowerShellコマンドを実行してウェブシェルやその他の悪意のあるツールを展開する、成功した悪用試行を迅速に特定しました。

ハンティング手法

- エクスプロイト後の振る舞いパターンを定義するためのプロアクティブな脆弱性研究。
- w3wp.exeから生成された異常な子プロセスを検出するためのプロセスツリーの異常ハンティング。
- エントロピーベースのスクリプト分析による難読化またはBase64エンコードされたコマンドの特定。

このキャンペーンから得られる主要な教訓は、脆弱性の悪用に関する調査が極めて重要であるということです。

修復手順

組織は直ちにCVE-2025-53770にパッチを適用し、潜在的なトークン窃盗を無効にするためにASP.NETマシンキーをローテーションする必要があります。セキュリティチームは、sso-ishaansehgal管理者アカウントと、docssended.aspxやtest.aspxなどのウェブシェルを捜索し、削除しなければなりません。アクティブなC2を阻止するには、84[.]247[.]151[.]254への通信をブロックし、w3wp.exeまたはphp-cgi.exeがコマンドシェルを生成していないか監視する必要があります。

脅威ハンティングのヒント

SharePointの永続的なウェブサーバー侵害は、脅威ハンティングチームにとっていくつかの重要な教訓を提供します。

- プロアクティブな調査：脆弱性研究を活用して、初期のアクターのベクターをより深く理解することで、防御側がアラートに反応するのではなく、エクスプロイト後の振る舞いを予測できるようにします。
- プロセスツリーの異常：w3wp.exeやその他の一般公開されているサービスプロセスから生成された異常なプロセスを検出するための仕組みの作成を優先します。
- 信頼できない実行：任意のシステムユーティリティを実行するために、ウェブサーバーのコンテキストで実行されているプロセスを信頼してはなりません。
- 高エントロピー文字列：特にコマンドライン内の高エントロピー文字列を捜索します。これは多くの場合、エンコードまたは難読化されたコマンドを示しています。

プロセスツリーの異常に検出の焦点を当てることで、脆弱性に関する知識を非常に効果的な挙動検出ルールに変え、この共通のエクスプロイト後パターンを共有する既知および将来のエクスプロイトの両方から保護することが可能です。

2 SIDEWINDER: TARGETED ESPIONAGE AND DLL SIDELOADING ANALYSIS（SIDEWINDERスピアフィッシング）

インシデントの概要

2025年9月23日、インド関連の脅威アクターであるSideWinderは、インドに拠点を置くヨーロッパの政府機関を標的とした標的型スピアフィッシングキャンペーンを開始しました。この作戦は、「中国バングラデシュ・シンクタンク・フォーラム」という外交的なおとりを利用して、正当性を装いました。侵入は、攻撃者がパキスタンの外交アカウント（asresearch@mofa[.]gov[.]bd[.]pk-mail[.]org）を偽装し、悪意のあるPDFを含むメールを送信したときに始まりました。この文書は、ソーシャルエンジニアリングを利用して、被害者に偽の「Adobe Reader」アプリケーションをダウンロードするよう説得しました。一度実行されると、インストーラーはClickOnceアプリケーションを利用して正規のMagTekソフトウェアをダウンロードし、それが悪意のあるコンポーネントであるDEVOBJ.dllをサイドロードするために使用されました。この多段階チェーンは最終的に、永続的なアクセスと機密データの持ち出しのために設計されたマルウェアであるStealerBotを展開しました。このような攻撃は、機密データ、知的財産、または機密の国家安全保障情報を盗むことを目的とした、巧妙で長期的な侵害の初期ベクトルとして機能します。このような侵害は、外交関係と国防に深刻な影響を与える可能性があります。このインシデントは、高価値の政府部門における従来の防御を回避するためのSideWinderのDLLサイドローディングの進化する使用を浮き彫りにしています。

TTP Progression

Phase	Technique (ID)	Observed Adversary Behavior
Initial access	Phishing: Spear phishing Attachment (**T1566.001**)	Sent an email with a weaponized PDF titled “China bangladesh Think Tak Forum-2025.pdf”.
Execution	User execution: Malicious file (**T1204.002**)	Victim prompted to click “Install” in the PDF to run a fake Adobe application.
Persistence	Boot or logon autostart execution: Registry run keys / startup folder (**T1547.001**)	Malware adds itself to Registry Run keys to maintain access after reboots.
Defense evasion	Hijack execution flow: DLL (**T1574.001**)	Employs **DLL sideloading** by using legitimate MagTek software to load malicious DEVOBJ.dll.
	System binary proxy execution (**T1218**)	Abuses legitimate binaries to mask the execution of StealerBot.
Discovery	Software discovery: Security software discovery (**T1518.001**)	Scans the system specifically for installed security products to aid in evasion.
Collection	Data from local system (**T1005**)	StealerBot automatically identifies and gathers sensitive data from the local machine.
Command & control	Application layer protocol: Web protocols (**T1071.001**)	Communicates with C2 servers using standard web protocols.
Exfiltration	Exfiltration over C2 channel (**T1041**)	Transfers stolen data out of the network via the established C2 channel.

脅威ハンティングプロセス

脅威ハンティングプロセスは、プロフェッショナルなメールのおとりを特定し、ジオフェンシングなどの高度なテクニックを活用したテレメトリーを分析することに焦点を当てました。SideWinderは通常、外交機関を標的としており、このキャンペーンも例外ではありませんでした。この特定のキャンペーンの具体的なTTP（戦術、技術、手順）が以前は知られていなかったため、初期の発見は困難でした。私たちの調査は、添付リンク付きのPDFを含むメールの特定に焦点を当てました。主な指標は、メールのおとりのプロフェッショナルなトーンと、東南アジアの政府機関のメールアカウントを模倣しようとする送信者の試みであり、これらはSideWinderが使用する一般的な戦術の両方です。

さらなる分析により、重要な発見が明らかになりました。最初の感染ペイロードであるClick-Onceアプリケーションは、特定の国（この場合はインド）からのみダウンロード可能であり、これは熟練度の低いサイバー犯罪者には一般的に採用されない高度なジオフェンシング戦術でした。

最初のメールを活用することで、追加のテレメトリーデータを取得することができました。いくつかの事例では、このテレメトリーには以前にSideWinderに関連付けられたドメインやメールアカウントが含まれていました。収集されたマルウェアサンプルの最終的な分析により、私たちの帰属特定への取り組みが確固たるものになりました。私たちのハンティング手法には以下が含まれていました：

- 政府機関を装ったプロフェッショナルなおとりを特定するためのメールメタデータ分析。
- 関連するドメインやアカウントを明らかにするための初期のメール識別子を使用したインフラストラクチャのピボット。
- 標的とされたジオフェンシング戦術を特定するための地理的テレメトリーの相関。

修復手順

同様のスピアフィッシングキャンペーンを修復するには、厳格なメールフィルタリングとソフトウェア制限ポリシーを実装して、不正なアプリケーションとClickOnceインストーラーの実行をブロックする必要があります。感染の兆候を示すシステムは直ちに隔離し、悪意のあるドメイン filenest[.]live および pk-mail[.]org への接続をブロックするようにファイアウォールを設定する必要があります。最後に、正規のソフトウェアアップデートを装ったスピアフィッシングの試みを認識するための、ターゲットを絞ったユーザー意識向上トレーニングを実施します。

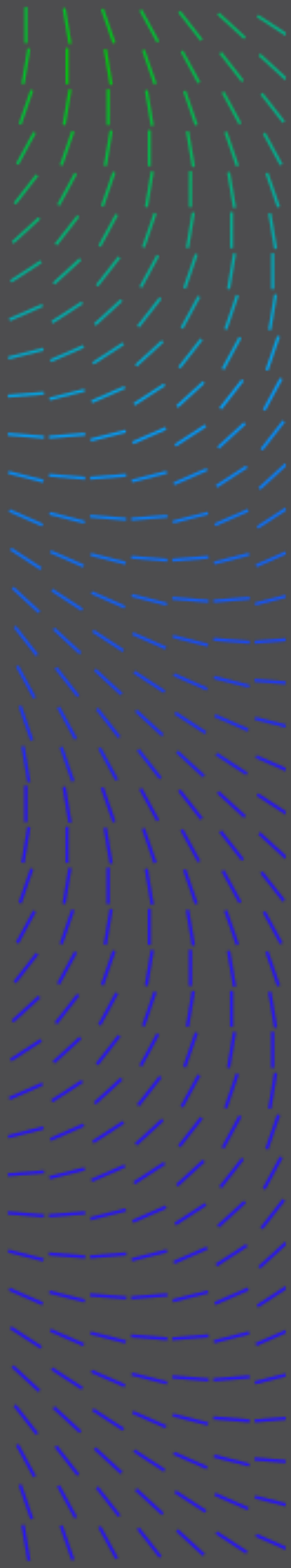
脅威ハンティングのヒント

SideWinderのインシデントは、脅威ハンティングチームにとっていくつかの重要な教訓を提供します。

- 地理的テレメトリー：最初のClickOnceペイロードを配信するために、高リスク地域でのジオフェンシング戦術の巧妙な使用に焦点を当てます。これは、敵対者がグローバルなセキュリティ監視を回避するために地理的ターゲティングを採用していることを示しています。
- 迅速なインフラストラクチャ分析：敵対者のC2インフラストラクチャのURLの寿命が短いことを考慮し、陳腐化した脅威フィードに焦点を当てるのではなく、新しいドメインの即時分析とプロアクティブなブロックを優先します。

- 非典型的なアクセスベクター：従来のメール添付ファイルフィルターを迂回することが多いClickOnceアプリケーションなど、一般的でない初期アクセスベクターをアクターが積極的に採用する傾向に注意を払う必要があります。
- DLLの異常：信頼されたバイナリによって開始された場合でも、DLLの実行を 明確に標的とし、疑わしい実行チェーンを継続的に監視する強化されたエンドポイント検出および対応（EDR）ルールを配備します。例として、正規のMagTekアプリケーションを悪用したDLLサイドローディング攻撃の成功が挙げられます。
- インストーラーの制限：ClickOnceなどのめったに使用されないインストーラータイプを制限するために、アプリケーションの許可リストを実装します。

主要な教訓は、従来のメール添付ファイルフィルターを迂回することが多いClickOnceのような、一般的でない初期アクセスベクターをアクターが積極的に採用している点です。



3 MUSTANG PANDA: EUROPEAN DIPLOMATIC ESPIONAGE CAMPAIGN(ムスタングパンダPlugX).

インシデントの概要

2025年9月26日、ヨーロッパの公的機関の職員が、偽の国境通過手続きを装ったスピアフィッシングメールを受信し、複雑な多段階の感染チェーンが開始されました。ユーザーが悪意のあるリンクをクリックすると、コマンドラインのパディング脆弱性を悪用して難読化されたPowerShellを実行する悪意のあるLNKファイルを含むZIPアーカイブがダウンロードされました。このスクリプトは、ネイティブのWindowsバイナリであるtar.exeを悪用して、DLLサイドローディングのための正規のCanonプリンターユーティリティを抽出し、最終的にEnumSystemGeoIDコールバックハイジャックという新しい手法を通じてPlugXバックドアを展開しました。

その直後の2025年9月29日と30日には、SideWinder攻撃からわずか1週間後に、別のヨーロッパの政府機関に対して同様の攻撃の波がありました。これらのインシデントは、NATOの統合分析・訓練・教育センター(JATEC)の防衛調達ワークショップやコペンハーゲンで開催された欧州政治共同体(EPC)サミットに関連するおとりを利用しました。これらのメールはセキュリティ制御をうまく回避し、受信者の受信トレイに到達しました。

これらの作戦は、PRCと関連するアクターであるMustang Pandaに高い確度で帰属され、長期的なスパイ活動とデータ持ち出しのために永続的なバックドアアクセスを確立しました。このキャンペーンは、ヨーロッパの外交官とNATOの防衛協力に対する戦略的な焦点を浮き彫りにしています。

TTP Progression

Phase	Technique (ID)	Observed Adversary Behavior
Initial access	Spear-phishing (T1566.002)	Emails targeting EU Government officials using EU/NATO themes.
Delivery	HTML smuggling (T1027.006)	Azure Blob Storage URLs used to smuggle and download malicious ZIP archives.
Exploitation	LNK padding	LNK files exploiting **ZDI-CAN-25373** to hide PowerShell commands beyond display limits.
Extraction	Binary proxy execution (T1218)	PowerShell carves a TAR archive and extracts it using native **tar.exe**.
Execution	DLL side-loading (T1574.002)	Signed Canon utility (**cnmpaui.exe**) used to load malicious **cnmpaui.dll**.
Payload injection	Callback hijacking (T1106)	**EnumSystemGeoID** API misused to execute PlugX shellcode and evade EDR.
Persistence	Registry run keys (T1547.001)	Establishes survival via the **"Canon Printer"** key and masquerading in Public folders.
C2 communication	Web protocols (T1071.001)	PlugX beacons to Cloudflare-proxied domains using HTTPS with randomized parameters.

脅威ハンティングプロセス

この調査は、2025年10月3日にStrikeReady Labsが発表したオープンソースインテリジェンス（OSINT）報告書から始まりました。この報告書では、セルビア政府機関に対するMustang Pandaの作戦が詳述されていました。OSINT報告書は、脅威アクターがHTMLスマグリングペイロードをホストするためにAzure Blob Storageを使用したことを明らかにしました。

私たちは直ちにメールテレメトリーにピボットし、SQLLIKEパターン：%download%web.core.windows. net%を使用して同様の配信インフラストラクチャを照会しました。これにより、初期のセキュリティ制御をうまく回避したヨーロッパの外交官に対する追加の標的化が明らかになりました。

このブレークスルーは、VirusTotalでHTMLペイロードを分析した際にもたらされました。偽のCloudflareTurnstileページには、特徴的なJavaScript変数 **SFAFAT_URL** が含まれており、XOR難読化（キー=23）と組み合わされていました。これは、関連するサンプルを確実にクラスタリングできる独自のアーティファクトです。このエンコードメカニズム（127 99 99 103...のような10進数値がURLに変換される）は、追加のキャンペーンインフラストラクチャをハンティングするための信頼できるシグネチャとなりました。

```
try {
  turnstile.render('#cf-turnstile', {
    sitekey: TURNSTILE_SITE_KEY,
    callback: function (token) {
      if (SFAFAT_URL) location.assign(SFAFAT_URL);
    },
    'error-callback': function () { console.warn('Turnstile error'); },
    'timeout-callback': function () {
      try { turnstile.reset('#cf-turnstile'); } catch(e) {}
    }
  });
} catch (e) {
  console.error('Failed to render Turnstile:', e);
}
```

Figure 1: The SFAFAT_URL variable is a distinctive artifact within a benign Cloudflare Turnstile CAPTCHA check.

私たちは、特徴的なTTP、すなわちZDI-CAN-25373を悪用するLNKファイル、CanonプリンターのDLLサイドローディング（cnmpaui.dll/cnmplog.dat）、および外交官を標的としたEU/NATOをテーマとするおとりをハンティングすることで、カバレッジを拡大しました。このマルチベクターアプローチにより、関連する攻撃が公に開示される前にプロアクティブに検出することができました。ZDI-CAN-25373は、UIの文字数制限を悪用して悪意のあるコードを隠すことで、リモートコード実行を可能にしていましたが、Microsoftによる最近の修正により、完全なコマンド文字列が公開されるようになり、これが阻止されています。私たちのハンティング手法には以下が含まれていました：

- Azure Blob Storageの配信パターンに関するStrikeReady Labsのレポートを使用したOSINTの相関。
- 特定のストレージURLに対してSQL LIKEパターンを使用したプロアクティブなメールテレメトリー検索。
- 一意のJavaScript変数 SFAFAT_URL とXOR難読化を使用したアーティファクト署名のクラスタリング。
- Trellix IVXとFAUDEを使用したマルチベクターピボットにより、追加の被害組織を特定。

修復手順

これに対応して、組織は非標準の場所にあるcnmpaui.exeが関与するDLLサイドローディングの即時ハンティングを実施し、racineupci[.]orgやcseconline[.]orgなどの特定されたC2インフラストラクチャをブロックする必要があります。復旧作業は、悪意のあるCanon Printerレジストリキーを削除することによる永続性の無効化、およびHTMLスマグリングと疑わしいAzure Blob Storage URLに対する検出ルールの実装に焦点を当てる必要があります。

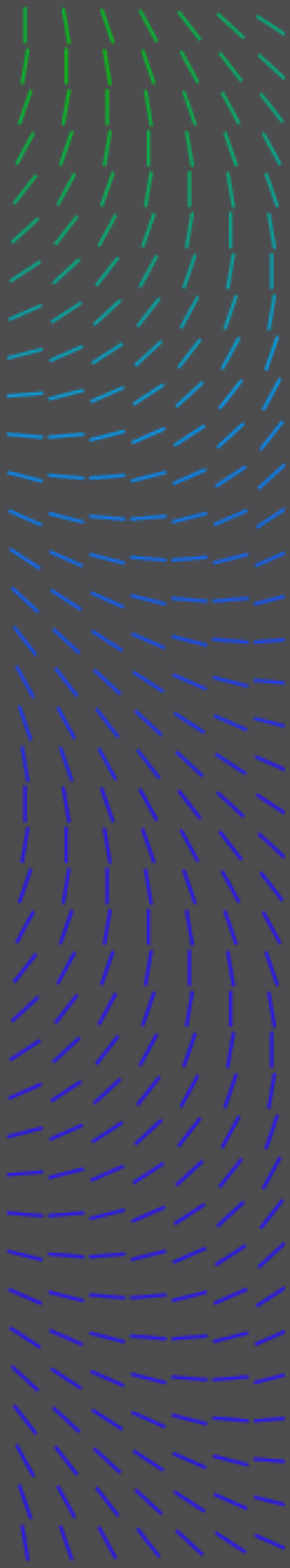
外部の脅威リサーチは、多くの場合、お客様の環境に適用可能なインフラストラクチャパターンを明らかにします。

脅威ハンティングのヒント

Mustang Pandaによるヨーロッパでのスパイ活動キャンペーンは、脅威ハンティングチームにとっていくつかの重要な教訓を提供します。

- **OSINTの統合**: OSINT（オープンソースインテリジェンス）をプロアクティブな脅威ハンティングに活用します。外部のリサーチは、しばしばお客様の環境に適用可能なインフラストラクチャのパターンを明らかにします。
- **マルチソースのテレメトリー**: ハンティングを単一のテレメトリーソースに限定しないでください。キャンペーンの全容を特定するために、メールログを超えて、Webソリューションやエンドポイントソリューションを含めたハンティングを拡大します。
- **地政学的コンテキスト**: 帰属と優先順位付けにおいて、コンテキストは重要です。主要な国際会議と一致するテーマのおとり（例：EUサミット、NATO会議）を監視し、既知のAPTの標的設定の傾向と照合して、脅威ハンティングと脅威の帰属特定を改善します。
- **固有のJavaScript変数**: 技術的なピボットのために、一般的なIOC、一時的なIP、またはドメイン名ではなく、**SFAFAT_URL** のような固有のアーティファクトに焦点を当てて、関連するキャンペーンをクラスタリングします。
- **クラウドインフラストラクチャ**: 特定のHTMLスマグリングのパターンとAzure Blob StorageのURL（例：%download%web.core.windows.net%）を照会します。この事例では、悪意のあるインフラストラクチャにアクセスした追加の被害顧客を明らかにしました。

アトリビューションと優先順位付けにおいて、コンテキストは重要です。テーマ的に関連するおとりを監視し、既知のAPTの標的設定の傾向と照合します。



4 THE “LONG GAME”: ANALYSIS OF KIMSUKY’S TRUST-BUILDING SPEAR-PHISHING CAMPAIGN（KIMSUKY LNK スピアフィッシングキャンペーン）

インシデントの概要

2025年後半、北朝鮮のAPTグループKimsukyは、韓国の組織の人事部門を標的とした、洗練された多段階のソーシャルエンジニアリングキャンペーンを実行しました。この作戦は、「信頼構築」の手法を通じて従来のメールフィルターを迂回するように設計された、高度な忍耐力と局所的な正確さを特徴としていました。

侵入は9月28日に始まり、攻撃者が「パク・ソンファン」という応募者になりすまし、信頼を築くために無害なPDFの成績証明書を人事担当者に送付しました。戦略的な10日間の遅延の後、脅威アクターは別の人事担当者にフォローアップメールを送信しました。これは、悪意のあるZIPアーカイブを含む内部の人事スレッドに見せかけるように偽装されていました。アーカイブの内部には、二重ファイル拡張子を介してDOCX文書になりすました、武器化されたLNKファイルがありました。

実行されると、LNKファイルは難読化されたPowerShellチェーンをトリガーしました。このスクリプトは、レジストリベースのジオフェンスチェックを実行し、**majority.docx**や**entiment.ps1**などのセカンダリペイロードを攻撃者が制御するGitHubリポジトリからダウンロードするように設計されていました。永続性を維持するために、マルウェアは30分ごとに実行されるようにスケジュールされたタスクを作成しようとしました。

Trellix Email Securityは、セカンドステージのペイロードを隔離することで緩和に成功し、永続的なバックドアの確立と潜在的なデータ持ち出しを防ぎました。このインシデントは、Kimsukyが韓国の商業的利益を標的とするために、長期的なソーシャルエンジニアリングと正規のクラウドサービスの悪用を引き続き頼っていることを浮き彫りにしています。

TTP Progression

Phase	Technique (ID)	Observed Adversary Behavior
Initial access	Spear-phishing attachment (T1566.001)	Stage 1: Attacker impersonated a job applicant to deliver a clean PDF Stage 2: Sent a follow-up email containing a malicious ZIP.
Execution	Human-triggered (T1204.002)	Required the recipient to open the ZIP and double-click the weaponized LNK file.
Execution	PowerShell (T1059.001)	LNK file executed cmd.exe to launch heavily obfuscated PowerShell commands.
Persistence	Scheduled task (T1053.005)	Attempted to create a task named “Majority Company” to run entiment.ps1 every 30 minutes.
Defense Evasion	Obfuscation (T1027) & masquerading (T1036.007)	Used Base64 encoding for scripts and double file extensions (.docx.lnk) to hide the true file type.
Command & control	Web service: GitHub (T1102)	Abused GitHub repositories to host and download secondary payloads using hardcoded API tokens.

脅威ハンティングプロセス

この発見は、「The Coordinated Embassy Hunt」に文書化された、北朝鮮と関連するGitHub C2スパイ活動キャンペーンに関する当社のチームの研究から明らかになりました。

外交的な標的設定パターンの分析中に、私たちは、パスワードで保護されたZIPアーカイブと二重ファイル拡張子のおとり（.docx.lnk、.pdf.lnk）を使用して、韓国の商業団体を標的とする同様のTTPをハンティングするためにピボットしました。

この発見は、Trellix Email Securityのテレメトリーで、韓国語のテーマと疑わしい添付ファイルチェーンの両方を含むメールをハンティングしたときに得られました。パスワードで保護されたアーカイブを処理するための当社の内部手法により、このAPTキャンペーンがフラグ付けされました。私たちは、一般的なKimsukyの指標である、GitHubホスト型のPowerShellペイロードとBase64エンコードされた実行チェーンを体系的に検索しました。当社のGitHub C2リサーチと相互参照された「miffiya1@naver[.]com」の送信者パターンは、ハードコードされたAPIトークン、難読化されたPowerShellドロッパー、XenoRAT配信など、複数の北朝鮮キャンペーンで一貫して観測されている重複するTTPを明らかにしました。

私たちのハンティング手法には以下が含まれていました：

- 韓国語のテーマとパスワードで保護されたZIPを検索するテーマ別のおとり分析。
- .docx.lnkのような二重拡張子を持つ.lnkファイルに焦点を当てたファイル検出。
- raw.githubusercontent[.]comへの不正な接続を監視するためのクラウドサービスの悪用監視。
- 既知のGitHub C2リサーチとの「miffiyal@naver[.]com」送信者パターンの相互参照。
- GitHubホスト型のPowerShellペイロード、ハードコードされたAPIトークン、難読化された実行チェーンの分析。

修復手順

送信者 miffiyal@naver[.]com をブロックし、ZIPアーカイブ内にネストされた .lnk ファイルのハンティングを実施します。セキュリティチームは、「Majority Company」スケジュールされたタスクを特定して削除し、**%TEMP%** および **%APPDATA%** ディレクトリから悪意のあるスクリプト（具体的には **entiment.ps1**、**addition.ps1**、および **system_first.ps1**）を削除する必要があります。アクティブなC2を阻止するには、raw.githubusercontent[.]com への不正な接続を監視し、.docx.lnk のような二重拡張子を持つ偽装されたドキュメントから発信されるPowerShellコマンドの実行をブロックします。

脅威ハンティングのヒント

環境内で同様の活動をプロアクティブに特定するために、アナリストは以下のハンティングパラメータに焦点を当てる必要があります。

- **ファイルの偽装:** パスワードで保護されていることやユーザー操作が必要なために自動サンドボックスを常に回避する、パスワードで保護されたZIP内の .lnk ファイル、特に二重拡張子(.docx.lnk、.pdf.lnk)を持つものを優先的にハンティングします。
- **GitHub C2の検出:** 予期しないプロセス、特にBase64エンコードされたコマンドを実行するPowerShellからの raw.githubusercontent.com への接続を監視します。異常なリポジトリアクセスパターンに対する検出を実装します。
- **挙動によるハンティング:** 韓国の会社名を持つスケジュールされたタスク、%TEMP%/%APPDATA% からのPowerShell実行を検索します。

パスワードで保護されていることやユーザー操作が必要なために自動サンドボックスを常に回避する、パスワードで保護されたZIP内の .lnk ファイル、特に二重拡張子を持つものを優先的にハンティングします。

5 UTA0355: WESTERN POLICY AND DIPLOMATIC SPEAR-PHISHING CAMPAIGN（UTA0355 スピアフィッシングキャンペーン）

インシデントの概要

2025年11月14日、ロシアの脅威アクターUTA0355は、米国の組織に対して高度なスピアフィッシングキャンペーンを開始しました。この作戦は、ベオグラード安全保障会議のおとりを利用して、詐欺的な登録ドメイン bsc2025[.]org で政策専門家を標的にしました。

侵入は、攻撃者がGmailアカウントを介して研究者になりすまし、受信者をOAuthデバイスコード認証ワークフローにだますように設計されたメールを送信したときに始まりました。初期の試みはブロックされましたが、11月18日のフォローアップメールは防御を迂回し、受信者に届きました。攻撃チェーンはOAuthトークンの収集に依存しており、これによりアクターは多要素認証（MFA）をバイパスし、Microsoft 365アカウントへの永続的なアクセスを獲得しました。

アクセスが確立されると、攻撃者はMicrosoft Entra IDに不正なデバイスを登録し、データ持ち出しを隠蔽し、ステルス性を維持しました。このインシデントは、UTA0355が西洋のシンクタンクに焦点を当てていること、および従来の境界セキュリティを回避するためにOAuth悪用へと移行していることを浮き彫りにしています。このような侵害は、機密性の高い国家安全保障ネットワーク内での情報収集とラテラルムーブメントの深刻なリスクをもたらします。

TTP Progression

Phase	Technique	Observed adversary behavior
Initial access	Phishing: spearphishing link (T1566.002)	Targeted emails were sent to policy professionals containing a link to a fake conference registration portal.
Persistence	Account manipulation: additional cloud credentials (T1098.001)	After obtaining access, attackers registered new devices in Microsoft Entra ID to maintain persistent access to the tenant.
Defense evasion	Impersonation (T1656)	The campaign posed as a legitimate researcher from the Belgrade Centre for Security Policy.
Credential access	Steal application access token (T1528)	The attack used OAuth Device Code workflows to trick users into granting permissions to their Microsoft 365 accounts.
Credential access	Input capture: web portal capture (T1056.003)	A fraudulent landing page was used to harvest corporate credentials and email addresses.
Discovery	Account discovery: cloud account (T1087.004)	The threat actor identified and targeted specific high-value cloud accounts within the organization.
Collection	Email collection: remote email collection (T1114.002)	Attackers gained unauthorized access to collect sensitive data from email, OneDrive, and Teams.
Command and control	Proxy: external proxy (T1090.002)	Residential proxy networks, such as Comcast IP addresses, were used to mask the attacker's true geographic origin.

脅威ハンティングプロセス

この調査は、OAuthフィッシングのためにヨーロッパのセキュリティイベントを装うUTA0355のキャンペーンに関するVolexityの「Dangerous Invitations」という脅威インテリジェンス報告書から始まりました。このOSINT（オープンソースインテリジェンス）は、ベオグラード安全保障会議やブリュッセル・インド太平洋対話のような会議になりすますロシアの脅威アクターに関する重要なコンテキストを提供しました。
その後、私たちは、bsc2025[.]org ドメインと関連するインフラストラクチャパターンについて、プロアクティブにメールテレメトリーをハンティングしました。この発見は、悪意のあるドメインから“Ivana Ranković <ivanaarankovic@gmail[.]com>”という送信者ペルソナを特定するためにピボットしたときにもたらされました。

弊社のハンティング手法には以下が含まれていました。

- Volexityのキャンペーンインテリジェンスを用いたOSINT（オープンソースインテリジェンス）の相関。
- 会議なりすましパターンを対象としたプロアクティブなドメイン検索。
- 送信者ペルソナと配信パターンを特定するためのメールメタデータ分析。
- 回避戦術を検出するためのスパムスコアの相関：Trellix Email Securityは、初期メールに対して8.608のスパムスコアで既存の検出機能を提供。

修復手順

同様のスピアフィッシングキャンペーンを修復するには、侵害されたアカウントのすべてのOAuthトークンとアクティブなセッションを直ちに失効させる必要があります。承認されていないOAuthアプリケーションのアクセス許可と、Microsoft Entra IDに登録されている不正なデバイスを監査し、削除してください。組織は、条件付きアクセス**ポリシー**を介してデバイスコード認証フローをブロックし、未検証のアプリに対するユーザーの同意を制限すべきです。最後に、将来の悪用を防ぐために、信頼構築型のソーシャルエンジニアリングとOAuthフィッシングの戦術に焦点を当てた標的型トレーニングを実施します。

脅威ハンティングのヒント

ロシアのスピアフィッシングキャンペーンは、脅威ハンティングチームにとっていくつかの重要な教訓を提供します。

- **プロアクティブな脅威インテリジェンスを活用：** Volexityのレポートなどの質の高いリサーチを購読する。
- **脅威インテリジェンスの相互参照：** 公的な脅威インテリジェンスレポートを、キャンペーンパターン、インフラストラクチャのIOC（侵害の痕跡）、およびターゲティングプロファイルを使用して、自社のテレメトリーと比較する。
- **会議なりすましパターンを特定：** セキュリティ/政策イベントのキーワードを含む新規登録ドメイン（90日未満）を、特に会議シーズン中に監視する。UTA0355のbsc2025[.]orgは、攻撃の29日前に登録されていました。

パブリックな脅威インテリジェンスを、キャンペーンパターン、インフラストラクチャのIOC（侵害の痕跡）、およびターゲティングプロファイルを使用して、自社のテレメトリーと相互参照する。

THE TRELLIX SECONDSIGHT ADVANTAGE(SecondSightの優位性)

Trellixは、敵対者が活動している間に完璧なテレメトリーを待つことはできないという原則に基づいてSecondSightを構築しました。セキュリティ製品はデータの表面化に優れていますが、巧妙な攻撃者はしばしば正規の管理活動のノイズの中に身を隠します。SecondSightは、お客様の環境に「第二の目」を提供する優秀な人間のハンターをSOCに追加することで、このギャップを埋めます。

CONCLUSION(結論)

敵対者は単一のプレイブックに頼っていません。俊敏で忍耐強く、正当な環境への融合に長けています。

SideWinderグループのジオフェンスされたClickOnceインストーラーの使用からUTA0355のOAuthワークフローの悪用まで、脅威の状況は従来の防御を迂回する「弱い信号」によって定義されています。

主な教訓

- 敵対者は信頼とコンテキストを優先：Kimsukyのような現代のキャンペーンは、「長期戦」のソーシャルエンジニアリングを利用してペイロードを配信する前に信頼を築き、自動フィルターによる初期検出を著しく困難にしています。
- 正当なツールが主要なベクターに：脅威アクターは、ネイティブのWindowsバイナリや正当なソフトウェア（例：MagTekやCanonユーティリティ）を一貫して悪用し、マルウェアをサイドロードして実行を隠蔽し、信頼されたアプリケーションを侵害の手段に変えています。
- プロアクティブな可視性は不可欠：古い脅威フィードに頼るだけではもはや不十分です。効果的な防御には、新しいインフラストラクチャの即時分析と、w3wp.exeのようなウェブサーバーから生成された異常な子プロセスなどのプロセスツリーの異常ハンティングが必要です。

現代の敵対者とその進化する戦術に遅れをとらないように、組織はプロアクティブな脅威インテリジェンスセキュリティ戦略を優先すべきです。Trellixはお客様と並行して活動し、グローバルなインテリジェンスと現実世界のテレメトリーを組み合わせて、認識されているネットワークセキュリティと実際のネットワークセキュリティとの間のギャップを露呈します。Trellix SecondSightでは、生の製品データに人間の直感を適用して信号の背後にある「意図」を理解し、脅威を組織のリスクを軽減するための具体的で実行可能なステップに変えます。絶えず進化する脅威の状況の中で、Trellixは、お客様、パートナー、コミュニティに対し、回復力を強化するための実行可能な脅威インテリジェンスを提供することに揺るぎないコミットメントを持ち続けています。

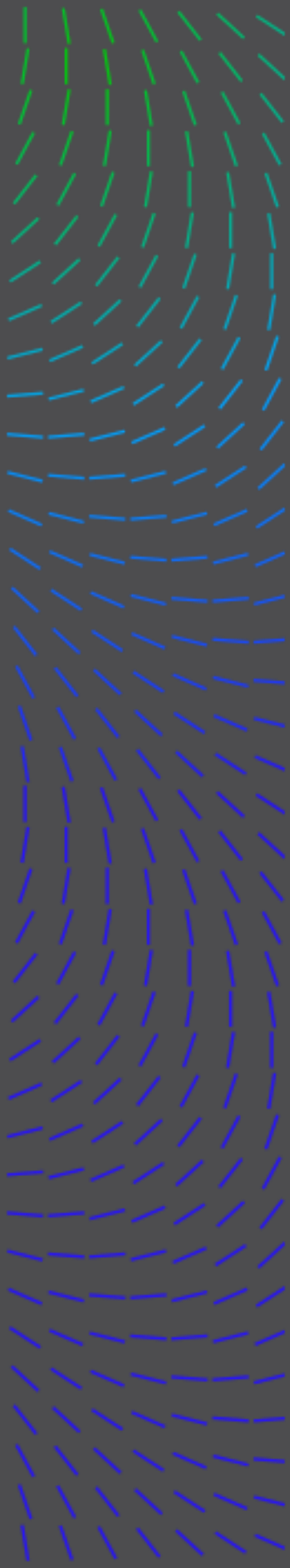
Nanhi Singh

President and Chief Customer Officer, Trellix

Learn more about how Trellix SecondSight turns your telemetry into decisive defensive action at Trellix.com/SecondSight

Contributors

Ale Houspanossian
Duy-Phuc Pham
Ernesto Fernández Provecho
Heather Mackey
Ilya Kolmanovich
Jenn Jackson
John Fokker
John Wells
Megan Haley
Nanhi Singh
Ryan Delany
Alex Lanstein



Trellix