NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI20250401

月刊ハッキンググループの動向レポート

Monthly Threat Actor Group Intelligence Report

- twitter.com/nshcthreatrecon
- service@nshc.net

April 2025

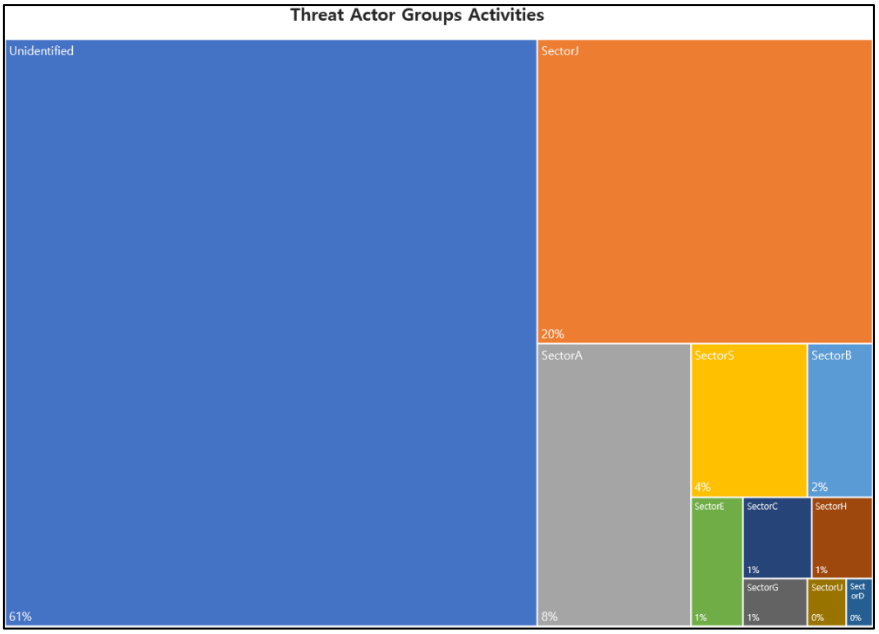
NSHC PTE. LTD.

このレポートは 2025 年 3 月 21 日から 2025 年 4 月 20 日まで見つけた政府支援のハッキンググループ活動と関係あるイッシューを説明し、それに伴う侵害事故の情報と ThreatRecon Platform 内のイベント情報を含む。

Table of Contents

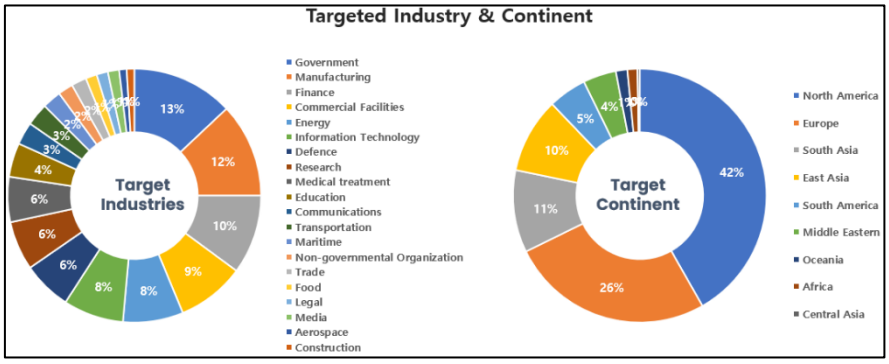
エグゼクティブサマリー

2025 年 3 月 21 日から 2025 年 4 月 20 日までの間に NSHC 脅威分析研究所（Threat Research Lab）が収集したデータと情報に基づいて分析したハッキンググループ（Threat Actor Group）の活動を要約した内容です。
今月 4 月には合計 77 のハッキンググループの活動が確認されており、確認されていない未識別（Unidentified）グループが 61%で最も多く、SectorJ、SectorA グループの活動がそれに続きました。



[Figure 1: 2025 年 4 月に確認されたハッキンググループ別活動統計]

今年 4 月に発見されたハッキンググループの活動は、政府機関や製造業分野に従事する関係者またはシステムを対象に最も多くの攻撃を行い、地域別では北アメリカとヨーロッパに位置する国々を対象としたハッキング活動が最も多いことが確認されています。



[Figure 2: 2025 年 4 月に攻撃対象となった産業分野と国の統計]

2025 年 4 月の 1 か月間に、多数の APT およびサイバー犯罪組織が活発に活動しており、その中でも SectorA および SectorJ グループの脅威行為が顕著に観察されました。全体として、約 10 以上の主要な組織群が政府、金融、暗号通貨、防衛産業、NGO、教育などの多様な産業をターゲットに、多様なメディアを通じたフィッシング、サプライチェーン攻撃、脆弱性の悪用、情報窃取およびランサムウェアの配布などの複合的な戦術を駆使しました。

特に APT（Advanced Persistent Threat）グループの場合、巧妙なソーシャルエンジニアリング技術と共に、オープンソースツール、合法的な署名を偽装する技術、難読化されたスクリプトおよび高度な暗号化チャネルを通じて検出を回避する戦略が支配的に現れました。サプライチェーンを利用した侵入試み、採用詐称を通じた初期アクセス、暗号通貨産業内でのスピアフィッシングおよびバックドア配布などは、その欺瞞性と技術的洗練さを示す代表的な事例です。

一方、サイバー犯罪グループは RaaS（Ransomware-as-a-Service）や MaaS（Malware-as-a-Service）を基盤とした営利目的の活動に集中しており、フィッシングリンクの拡散、ランサムノートの公開脅迫、暗号通貨ウォレットの窃取、複数国を対象とした活動の拡大など、収益化戦略が体系化されています。

共通して、多くのグループが C2 サーバーの隠蔽、クラウドインフラの悪用、動的ドメインの回転、ソーシャルメディアの連携など、検出回避と長期的な侵入維持に重点を置いており、これは伝統的な防御システムを回避し、長期間の偵察および攻撃を可能にするという点で深刻な脅威として作用します。

SectorA グループは 4 月の間、最も活発で高度な脅威活動を行いました。主に採用プロセスの偽装、技術テストの詐称、偽の GitHub プロジェクトの利用など、ソーシャルエンジニアリングの手法を通じて初期侵入に成功し、Golang ベースのバックドア、YAML 逆シリアル化ベースのマルウェアローダー、npm パッケージを利用したサプライチェーン攻撃など、様々な手段を活用しました。特に暗号通貨産業、防衛技術、工学分野をターゲットに、広範な C2 インフラとカスタマイズされたマルウェアを展開し、内部侵入後の情報収集、資格情報の窃取、破壊的行為まで行う精巧な攻撃フローが確認されました。

SectorB グループは、企業インフラへの侵入に焦点を当てた偵察中心のサイバー作戦を展開しました。Fortinet ファイアウォールおよび VPN を狙ったスクリプトの配布、DLL サイドローディングや PowerShell ベースのバックドアの導入、DNS over HTTPS（DoH）を利用した通信の偽装など、伝統的なセキュリティ検出システムを回避する高度な技術が目立ちます。また、Ivanti 機器の脆弱性を分析した後、再利用（ポストパッチエクスプロイト）を試みるなど、戦略的で先制的な脅威の試みが顕著でした。対象産業は政府、金融、エネルギー、通信などで、長期的なスパイ活動が主な目的です。

SectorC グループは主にウクライナおよび西側諸国を対象としたサイバー諜報活動を主導しました。DNS Fast Flux、Dead Drop

Resolvers、暗号化されたレジストリベースの持続性技法など、隠蔽性の高いインフラ設計が特徴であり、主要な Malware は GammaSteel、PteroLNK、Remcos などの情報窃取型系列であることが確認されました。LNK ファイル、PowerShell および VBScript ベースのペイロードが主に活用され、高度に難読化されたコマンドおよびコントロール（Command and Control、C2）チャネルの運用が確認されました。主要な産業分野は防衛、文化、政府機関および軍事機関です。

SectorH グループは、鉄道、エネルギー、防衛産業を中心に新しい戦略を試みながら活動を展開しました。HTA の代わりに MSI ベースのペイロードを使用する変形された侵入戦略が観察され、Spark RAT、CurlBack のようなオープンソースベースの RAT を活用して、全方位的な侵入および情報収集を行いました。政府機関および主要な基幹インフラを狙った彼らは、多段階のコマンド実行および認証情報の窃取戦術を使用して、高度な脅威レベルを示しました。

SectorJ グループは、ランサムウェアおよび情報窃取を中心とした収益化戦略に集中しました。代表的なものとして、RALord、Qilin、Interlock などのさまざまなランサムウェアがフィッシング、スピアフィッシング、脆弱性の悪用といった初期侵入を通じて配布され、その後、ファイルの暗号化、バックアップの削除、データ流出サイトを利用した脅迫戦略が体系的に構築されました。特に、Amethyst Stealer、NetSupport Manager、DarkWisp などの情報窃取ツールが併用され、Telegram を通じた MaaS/RaaS サービスやスミッシングキットの配布など、新しい拡散経路も確認されました。また、ソーシャルメディアのなりすまし、ポッドキャストの偽装、リモートコントロール機能の悪用など、社会工学的手法がますます高度化しており、これらの攻撃範囲はアジア、ヨーロッパ、南米などに拡大しています。

詳細情報

APT（高度な持続的脅威）ハッキンググループの活動

1) SectorA01は、求人メールに偽装したBeaverTailマルウェアを使用しました（2025-04-02）

https://cti.nshc.net/events/view/13943

SectorA01 グループは 2024 年 11 月、開発者コミュニティプラットフォームで偽の採用メールを通じてマルウェアを拡散しました。該当グループはマルウェアを挿入した BitBucket リンクを提供し、これは「BeaverTail」と「car.dll」として識別されました。「car.dll」ダウンローダーは、組み込まれた Windows コマンドを使用して命令を実行し、これは過去の類似した脅威活動で観察された方法と類似しています。このマルウェアは、資格情報の窃取および追加のマルウェアペイロードのダウンロード機能を実行することが分析されています。「tailwind.config.js」は「car.dll」を実行するス

クリプトで、様々なフィッシングキャンペーンで使用された履歴があると知られています。バックドアは実行時にコマンド＆コントロールサーバー（Command & Control, C2）に接続を試み、サーバーアドレスを復号してシステム情報を収集します。また、RSA キーを使用して暗号化されたキーとセッション情報を C&C に送信する高度な暗号化技術を示しています。その後の通信は、ネットワーク診断、ファイル操作などの命令実行を許可し、これはかなりのセキュリティリスクを引き起こします。

攻撃の流れ

1. [初期アクセス] フィッシング: スピアフィッシング添付ファイル (T1566.001)
   a. 偽の採用メール送信
   b. ビットバケット(BitBucket)リンク提供
2. [実行] コマンドとスクリプトインタープリタ: JavaScript (T1059.007)
   a. "tailwind.config.js" 実行
   b. "car.dll" 実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 難読化された JavaScript ルーチン
   b. RSA キー暗号化
4. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. ウェブブラウザ資格情報の窃取
   b. 暗号通貨ウォレットデータの窃取
5. [コマンドと制御] 暗号化されたチャネル (T1573)
   a. C&C サーバーとの暗号化通信
   b. RSA 公開鍵で暗号化されたキー送信
6. [収集] スクリーンキャプチャ (T1113)
   a. スクリーンショットキャプチャ
   b. ファイル情報収集
7. [流出] C2 チャネル経由の流出 (T1041)
   a. システム情報を C&C に送信
   b. コマンド実行結果送信
8. [影響] データ破壊 (T1485)
   a. ファイル削除 (NULL データで上書き)
   b. ファイル削除 (ランダムな値で上書き)

2) SectorA01は、技術的課題に偽装したBeaverTailマルウェアを使用しました（2025-04-12）

https://cti.nshc.net/events/view/14241

攻撃対象産業群: 防衛、技術

SectorA01 グループは、リモート採用プロセスとオープンソースソフトウェアのエコシステムを対象にした高度なサイバーキャンペーンを主導しています。このグループは、「LinkedIn」や「GitHub」などのプラットフォームで偽のプロフィールを作成し、ソーシャルエンジニアリング技術を利用して攻撃対象を欺き、合法的な企業の採用プロセスに侵入し、面接過程で偽の技術テストを通じて Malware を配布します。このキャンペーンの主な攻撃対象産業は、技術、暗号通貨、防衛産業であり、その目的は諜報活動、金融窃盗、デジタル破壊を含みます。このグループは、「BeaverTail」や「InvisibleFerret」といったカスタム Malware を使用して資格情報や暗号通貨資産を盗み、現代のセキュリティソリューションを回避するための高度な回避技術を活用しています。2024 年には内部脅威に重点を置いて活動が増加し、偽の身分を持つエージェントが世界中の企業に侵入しました。採用された後、企業の機器は「Laptop
farm」にルート変更され、知的財産や機密データを盗むためにリモートでアクセスされました。このソーシャルエンジニアリングと Malware 攻撃のハイブリッドモデルは、サプライチェーンと企業内部アクセスを狙った持続的な脅威を示しており、ますます複雑化しています。

攻撃の流れ

1. [戦術] 初期アクセス (T1190)
   a. 偽のプロフィール作成
   b. 採用プロセスへの侵入
2. [戦術] 実行 (T1059)
   a. 技術テストでの Malware 実行
   b. Node.js ベースのトロイの木馬実行
3. [戦術] 永続性 (T1505)
   a. 「ノートブック農場」での機器経路変更
   b. リモートアクセスのための RMM ツールインストール
4. [戦術] 資格情報アクセス (T1555)
   a. ブラウザ保存資格情報の収集
   b. 暗号通貨ウォレット情報の収集
5. [戦術] 収集 (T1119)
   a. 知的財産の収集
   b. 機密データの収集
6. [戦術] 流出 (T1041)
   a. 収集されたデータをリモートサーバーに送信
   b. 「InvisibleFerret」を通じた C2 サーバー接続
7. [戦術] 防御回避 (T1562)

a. 高度な回避技術の使用
b. 変数およびデータの Base64 エンコード使用

3) SectorA01は、就職面接プロセスに偽装したGolangGhostマルウェアを使用しました（2025-03-31）

https://cti.nshc.net/events/view/13879

攻撃対象産業群: 金融

SectorA01 グループは、2025 年 3 月に UAE を拠点とする暗号通貨取引所プラットフォームを対象に大規模なサイバー攻撃を行い、史上最大規模の 15 億ドルを奪取しました。この攻撃は、暗号通貨産業を主に狙う国家支援グループによって実行され、国際制裁を回避し、ミサイルプログラムの資金調達に使用されました。この攻撃は巧妙なキャンペーンを含んでおり、特に中央金融（CeFi）機関内の暗号通貨分野の求職者を誘引するために偽の求職インタビューウェブサイトを活用しました。この偽のウェブサイトは「クリックフェイクインタビュー（ClickFake Interview）」という戦術を使用し、ユーザーが Windows と macOS システムにマルウェアのバックドアをダウンロードするよう誘導しました。Windows では、VBS スクリプトが NodeJS ベースのダウンロードプログラムを実行して「GolangGhost」バックドアをインストールし、macOS ユーザーは Bash スクリプトを通じて「フロスティフェレット（FrostyFerret）」スティーラーを実行した後、GolangGhost をインストールしました。このマルウェアはリモートコントロールとデータの窃取を可能にし、プロセスインジェクション、ユーザーエージェント（User-Agent）不一致の悪用、偽の UI 要素を活用したシステム資格情報のキャプチャといった高度な回避技術を強調しました。

攻撃の流れ

1. [初期アクセス] フィッシング (T1566.001)
   a. フィッシングサイトで求職者を誘導
   b. 求職インタビューウェブサイト内の偽インタビュープロセス
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. Windows VBS スクリプトの実行
   b. macOS Bash スクリプトの実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. Windows レジストリキーの作成
   b. macOS plist ファイルの作成
4. [防御回避] 偽装 (T1036)
   a. 偽の UI 要素の使用
   b. ユーザーエージェントの違いを悪用

5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. FrostyFerret でシステムパスワードを盗む
   b. Dropbox で情報を送信
6. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. GolangGhost を通じたデータ送信
   b. 暗号化された POST リクエストで C2 通信
7. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
   a. HTTP POST で C2 サーバーと通信
   b. RC4 暗号化の使用

4) SectorA01はコーディングチャレンジに偽装したマルウェアを使用しました（2025-04-14）
https://cti.nshc.net/events/view/14386

SectorA01 グループは、暗号通貨業界を対象としたサイバー攻撃を実行しました。彼らは LinkedIn で採用担当者に偽装し、開発者に「コーディングチャレンジ」という名目で Malware を含むプロジェクトを提示しました。初めは無害な PDF ファイルを通じて職務説明を提供し、その後 GitHub プロジェクトを通じて悪性ペイロードを注入しました。このグループは YAML 逆シリアル化技術を使用してペイロードを実行し、直接的な Malware 挿入を避けて検出を回避します。検証済みの攻撃対象にのみ、制御されたコマンド＆コントロール（Command and Control, C2）サーバーを通じてペイロードを送信します。「RN Loader」という Malware はメモリ上で動作し、基本的なシステム情報を送信し、サーバーの指示に従って追加のコマンドを実行します。また、「RN Stealer」というツールを使用して機密データを収集し、これは macOS をターゲットにしたカスタムペイロードを使用します。この悪意のあるキャンペーンは数十億ドルの利益を上げ、人気のあるプログラミング言語で GitHub リポジトリを戦略的に作成して検出を避け、攻撃対象を誤導する高度な運用戦術を示しました。

攻撃の流れ

1. [初期アクセス] フィッシング (T1566)
   a. LinkedInで採用担当者を装う
   b. PDFファイルで職務説明を提供
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. YAML逆シリアル化を使用
   b. Pythonのyaml.load()関数でコードを実行
3. [持続性] システムプロセスの作成または変更 (T1543)
   a. メモリ内で「RN Loader」を実行

b. __init__.pyファイルを作成
4. [防御回避] 偽装 (T1036)
a. GitHubプロジェクトを装う
b. 正当なソースに似たC2サーバードメインを使用
5. [コマンドとコントロール] ウェブサービス (T1102)
a. HTTPSを通じたC2サーバー通信
b. Base64エンコードされたトークンを使用
6. [収集] 入力キャプチャ (T1056)
a. macOSにカスタマイズされた情報収集
b. ログインキーチェーンおよびSSHキーを収集
7. [データ流出] C2チャネルを介したデータ流出 (T1041)
a. 収集されたデータをC2サーバーに送信
b. XORキーでデータを暗号化して送信
8. [影響] データ操作 (T1565)
a. 攻撃対象のデータを操作して持続的なアクセスを試みる
b. 必要に応じてペイロードの配信および実行を停止

5) SectorA01は、暗号プラットフォーム上でUI修正に偽装したマルウェアを使用しました（2025-04-11）

https://cti.nshc.net/events/view/14433

攻撃対象産業群: 工学

SectorA01 グループは 4 月にフィンテックおよび暗号通貨業界の専門家を対象としたサイバー脅威キャンペーンを実施しました。彼らは「Wilton Santos」という開発者を装い、分散アプリケーション（DApp）「Gamba v2」の UI 問題を解決するよう依頼し、500 USDT を提案しました。BitBucket リポジトリで共有されたコードは一見正常なコードのように見えましたが、Try/Catch ブロック内に罠がありました。これはフィンランドに位置するサーバーに外部 API リクエストを実行し、エラーコードを悪性ペイロードとして実行する方法でした。この方法は「OtterCookie」という Malware を導入し、この Malware はブラウザのパスワードや暗号通貨ウォレットのデータを盗むように設計されていました。このグループはエンジニアに感染したコーディングチャレンジを含む偽の採用提案を行い、経営陣には偽の Zoom 通話で接触し、システムを損傷させるアップデートを共有しました。彼らの攻撃は、インフラの詳細情報、開いているポート、管理者権限などに基づいて欺瞞と技術的搾取に焦点を当てた洗練された戦略を明らかにしました。

攻撃フロー

1. [初期アクセス] サービスを介したスピアフィッシング (T1193)
   a. 'Wilton Santos'になりすまして DApp UI 修正依頼
   b. BitBucket リポジトリを通じてクリーンに見えるコードを共有
2. [実行] クライアント実行のためのエクスプロイト (T1203)
   a. Try/Catch ブロック内で外部 API リクエストを実行
   b. エラーコードをマルウェアペイロードとして実行
3. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. "OtterCookie"マルウェアを通じてブラウザパスワードを盗む
   b. 暗号通貨ウォレットデータの窃取
4. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. 外部 API との通信を通じてマルウェアを制御
   b. Node.js Express で実行される API との接続
5. [探索] ネットワークサービススキャン (T1046)
   a. フィンランドサーバーの開いているポートを確認
   b. リモートデスクトッププロトコル(RDP)の使用を確認
6. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. JavaScript コードの難読化
   b. オンラインツールを利用したコードの隠蔽

6) SectorA01はnpmパッケージをユーティリティとして偽装し、マルウェアの展開に使用しました (2025-04-04)

https://cti.nshc.net/events/view/14076

SectorA01 は「Contagious Interview」キャンペーンを通じてソフトウェアサプライチェーンを主要な標的とし、悪性の「npm」パッケージを配布することで「BeaverTail」マルウェアと新しいリモートアクセス型トロイの木馬（RAT）ローダー機能を拡散させました。このパッケージは 16 進数文字列エンコーディングを利用して自動検出を回避します。このグループの主な目的は、開発者のシステムに侵入して資格情報や金融資産を盗み、侵害された環境へのアクセスを維持することです。このキャンペーンは「npm」、「GitHub」、「Bitbucket」などのプラットフォームを利用してユーティリティツールに偽装したマルウェアを配布し、活動を続けています。識別されたパッケージは共通のインフラリンクを共有し、難読化されたコード、ペイロード配信および搾取戦略などの共通の構造的特性を示します。持続的な脅威アクターは、共有 C2 エンドポイントと高度な難読化戦術を使用して検出を回避します。彼らは「BeaverTail」と「InvisibleFerret」を含む複数のマルウェア亜種を配布し、複数のパッケージがアカウント活動と関連付けられています。この脅威アクターは 5,600 回以上のダウンロードに影響を与える悪性の「npm」パッケージを継続的に生成および配布しています。

攻撃の流れ

1. [初期アクセス] サプライチェーンの妥協 (T1195.002)
   a. マルウェアの「npm」パッケージ配布
   b. 「GitHub」および「Bitbucket」を通じたコードホスティング
2. [実行] ユーザー実行 (T1204.002)
   a. マルウェアファイルの実行
   b. RAT ローダー機能の活性化
3. [防御回避] 難読化されたファイルまたは情報 (T1027.013)
   a. 16 進数文字列エンコーディングの使用
   b. 難読化されたコードの使用
4. [持続性] イベントトリガー実行 (T1546.016)
   a. インストールパッケージにイベントトリガーを挿入
   b. 持続的な C2 サーバー接続の維持
5. [資格情報アクセス] ウェブブラウザからの資格情報 (T1555.003)
   a. ウェブブラウザからの資格情報抽出
   b. 「Solana」の「id.json」ファイルからの秘密鍵抽出
6. [発見] システム情報の発見 (T1082)
   a. システム情報の収集
   b. ブラウザプロファイルの探索
7. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. HTTP POST リクエストを通じたデータ流出
   b. C2 サーバーへの情報送信
8. [コマンドと制御] ツール転送の受信 (T1105)
   a. C2 サーバーからのマルウェアダウンロード
   b. リモートコマンドの実行

7) SectorA02は、防衛研究論文に偽装したLNKマルウェアを使用しました (2025-03-27)

https://cti.nshc.net/events/view/13757

SectorA02 グループは、防衛分野で学術論文に偽装した「RokRAT」マルウェアを配布しました。この作戦は、悪意のある Windows ショートカット（LNK）ファイルを利用して「PowerShell」スクリプトを含んでいます。Windows ショートカットファイルが実行されると、複数のコンポーネントが%TEMP%フォルダに抽出され、ダミーの PDF ファイルとエンコードされたマルウェアファイルが含まれます。ユーザーはダミーの PDF ファイルによって正常な文書が開かれたと錯覚します。「toy03.bat」ファイルが実行されると、「toy01.dat」に保存されたエンコードされた「RokRAT」マ

ルウェアを「XOR」演算で復号化します。復号化されたシェルコードはメモリに直接ロードされ、ファイルなしで実行され、「RokRAT」は感染したシステムの情報とユーザー情報を収集し、該当グループの命令に従って様々な悪意のある行為を行うことができます。この過程で、「pCloud」、「ヤンデックス（Yandex）」、「ドロップボックス（Dropbox）」などの合法的なクラウドサービスがC2（コマンド＆コントロール）サーバーとして利用されます。これらの攻撃は、高度な回避および持続性技術を示しています。

[図3: SectorA02グループが利用した学術誌に偽装したおとりPDF文書]

攻撃フロー

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. 防衛産業分野に学術論文に偽装したファイルを配布
   b. 悪性の「LNK」ファイルを添付してユーザーを誘導
2. [実行] コマンドおよびスクリプトインタープリター: PowerShell (T1059.001)
   a. 「LNK」ファイル実行時に「PowerShell」スクリプトを実行
   b. ファイルを抽出し、%TEMP%フォルダーに保存
3. [防御回避] 偽装 (T1036)
   a. デコイ「PDF」ファイルを実行してユーザーを欺く
   b. 悪性活動を隠すためにファイルを自己削除
4. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. 「toy03.bat」ファイルを実行して持続性を確保
   b. システム再起動時にマルウェアを維持
5. [権限昇格] プロセスインジェクション (T1055)
   a. 復号化されたシェルコードをメモリに直接ロード

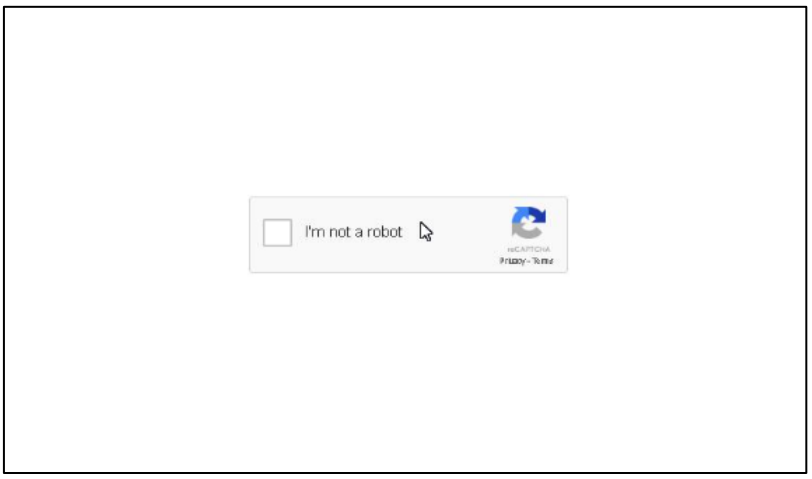
b. ファイルを生成せずにメモリ内で実行

6. [資格情報アクセス] パスワードストアからの資格情報 (T1555)
   a. システム情報およびユーザー情報を収集
   b. ユーザー資格情報の窃取を試みる
7. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. 「pCloud」、「Yandex」、「Dropbox」などのクラウドサービスを活用
   b. C2サーバーとの通信およびコマンド受信
8. [収集] ローカルシステムからのデータ (T1005)
   a. 感染したシステムの情報を収集
   b. ユーザー活動情報を抽出
9. [流出] 代替プロトコルを介した流出 (T1048)
   a. 収集されたデータを外部に送信
   b. クラウドサービスを通じたデータ流出
10. [影響] データ破壊 (T1485)
   a. 特定ファイルおよびデータの損傷の可能性
   b. システム障害を引き起こす可能性

8) SectorA05はClickFix Verificationを使用してマルウェアを実行しました (2025-03-29)

https://cti.nshc.net/events/view/13799

クリックフィックス（ClickFix）は、2025 年 3 月 24 日に識別された CAPTCHA 認証を悪用した欺瞞的な攻撃手法です。この攻撃は、ユーザーが人間であることを確認するために一般的に使用されるクリックベースの確認プロセスを悪用します。この手法を通じて、ユーザーは「Windows + R」を押し、「Ctrl + V」と「Enter」を行う指示を受け、これは悪意のある PowerShell スクリプトの実行につながります。このスクリプトは外部の Malware をダウンロードし、隠された PowerShell コマンドで実行してユーザーのシステムを損傷し、個人情報を盗みます。HTML インターフェースは正式な検証プロセスのように見えるように偽装され、心理的に安心させるメッセージでユーザーを誘導します。JavaScript 形式のマルウェアスクリプトは主にデスクトップ環境のユーザーを対象に動作し、モバイル環境では警告メッセージを通じてアクセスを遮断する方法でフィルタリング機能を果たします。これらのスクリプトはユーザーとの直接的な相互作用を誘導したり、回避して実行されたりし、外見上は正常なウェブコンテンツに偽装してユーザーが気付かないうちに悪意のある行為を行います。結果として、マルウェアはユーザーの介入なしにシステム内に密かにインストールされ、長時間常駐することができるため、セキュリティの脅威となります。



[Figure 4: SectorA05グループが利用したフィッシングサイト]

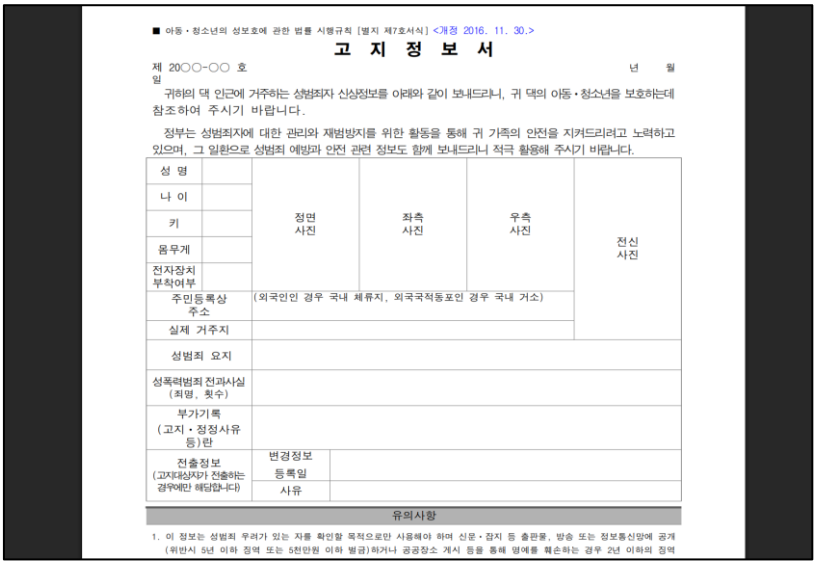
攻撃フロー

1. [初期アクセス] ユーザー実行 (T1204)
   a. CAPTCHA認証の模倣
   b. ユーザーが指示に従うよう誘導
2. [実行] コマンドとスクリプトインタープリター (T1059)
   a. PowerShellコマンドの実行
   b. 隠されたPowerShellウィンドウの実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 隠されたPowerShellコマンドの使用
   b. ユーザーに気付かれずにコマンドを実行
4. [コマンドと制御] インバウンドツール転送 (T1105)
   a. 外部スクリプト「32[.]ps1」のダウンロード
   b. PowerShellを通じて即時実行
5. [収集] 情報リポジトリからのデータ (T1213)
   a. 個人情報の窃取
   b. ユーザーシステムからのデータ収集
6. [データ流出] C2チャネルを介したデータ流出 (T1041)
   a. 窃取されたデータの送信
   b. C2チャネルを通じたデータ流出

9) SectorA05は、性犯罪者通知に偽装したLNKマルウェアを使用しました (2025-03-28)

https://cti.nshc.net/events/view/13798

SectorA05グループは、「성범죄자 신상정보 고지.pdf.lnk」というファイルを利用したマルウェアキャンペーンを実施しました。このファイルは1MBのサイズで、PDFに偽装した悪意のあるリンクファイルを通じて特定のグループを対象に攻撃を行いました。ファイルが実行されると、リモートサーバーからcurlを使用して悪意のあるHTMLアプリケーション（HTA）ファイルをダウンロードし、Windowsコンポーネントであるmshta.exeを使用して実行します。「sfmw.hta」という名前のこのHTAファイルはVBScriptベースで作成されており、コード難読化技術を使用して分析を妨げます。スクリプトは「chr()」関数を活用してコマンドを組み合わせ、「CreateObject('WScript.Shell')」を通じてCOMオブジェクトを生成し、「oShell.Run」を通じてコマンドを実行します。難読化は文字列操作を混合し、「chr()」関数内で意図的にエラーを挿入して分析を困難にします。この攻撃は、性犯罪者関連情報を配布するふりをして、法律または児童保護関連分野の個人や組織を対象にする可能性が高いと分析されています。



■ 아동·청소년의 성보호에 관한 법률 시행규칙 [별지 제7호서식] <개정 2016. 11. 30.>

고 지 정 보 서

제 20○○-○○ 호　　년 월 일

귀하의 댁 인근에 거주하는 성범죄자 신상정보를 아래와 같이 보내드리니, 귀 댁의 아동·청소년을 보호하는데 참조하여 주시기 바랍니다.

정부는 성범죄자에 대한 관리와 재범방지를 위한 활동을 통해 귀 가족의 안전을 지켜드리려고 노력하고 있으며, 그 일환으로 성범죄 예방과 안전 관련 정보도 함께 보내드리니 적극 활용해 주시기 바랍니다.

성 명		정면 사진	좌측 사진	우측 사진	전신 사진
나 이					
키					
몸무게					
전자장치 부착여부					
주민등록상 주소	(외국인인 경우 국내 체류지, 외국국적동포인 경우 국내 거소)				
실제 거주지					
성범죄 요지					
성폭력범죄 전과사실 (죄명, 횟수)					
부가기록 (고지·정정사유 등)란					
전출정보 (고지대상자가 전출하는 경우에만 해당합니다)	변경정보 등록일				
	사유				

유의사항

1. 이 정보는 성범죄 우려가 있는 자를 확인할 목적으로만 사용해야 하며 신문·잡지 등 출판물, 방송 또는 정보통신망에 공개 (위반시 5년 이하 징역 또는 5천만원 이하 벌금)하거나 공공장소 게시 등을 통해 명예를 훼손하는 경우 2년 이하의 징역

[図5: SectorA05グループが利用した性犯罪者の身元情報通知書に偽装したマルウェア]

攻撃の流れ

1. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. cmd.exeを通じたコマンド実行
   b. mshta.exeを利用したHTAファイル実行
2. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. chr()関数を利用した文字列の組み合わせ
   b. 難読化されたVBScriptコードの使用
3. [持続性] システムプロセスの作成または変更 (T1543)
   a. WScript.Shell COMオブジェクトの生成
   b. 外部コマンドの実行
4. [防御回避] 偽装 (T1036)

a. マイクロソフトエッジ(Edge)アイコンの使用
b. PDFファイルに偽装
5. [コマンドと制御] アプリケーション層プロトコル (T1071)
a. curlを通じたリモートサーバーとの通信
b. HTTPリクエストでのマルウェアファイルのダウンロード

10) SectorA05は、性犯罪者通知に偽装したLNKマルウェアを使用しました（2025-04-05）
https://cti.nshc.net/events/view/14016

SectorA05グループは韓国の政府機関を対象に2つのキャンペーンを実施しました。彼らは政府関連の文書を餌として使用し、フィッシングメールを通じて「Windowsショートカット（LNK）」ファイルの添付を送信しました。このWindowsショートカットファイルは難読化された「VBScript」をドロップし、追加のファイルをダウンロードしました。ダウンロードされた「ZIP」ファイルには4つの悪意のあるファイルが含まれており、その中のスクリプトは追加のファイルをC2サーバーから取得する機能を持っています。彼らは最初のキャンペーンでは税務文書を悪用し、2番目のキャンペーンでは性犯罪者通知関連の規制文書を使用しました。Windowsショートカットファイルは「Base64」でエンコードされた難読化されたスクリプトをダウンロードするように誘導しました。これらのスクリプトはデータの窃取、暗号通貨ウォレット情報の盗難、ブラウザーデータの抽出などのマルウェアを配布しました。「PowerShell」スクリプトはBIOSシリアル番号を取得し、攻撃特定ディレクトリを生成し、仮想マシンの実行を確認して検出されると攻撃ファイルを削除しました。また、攻撃チェーンは「PowerShell」コマンドを呼び出してキーロギング活動を行い、セキュリティ対策を回避し、検出を避けるための隠密な技術が強調されました。

[Figure 6: SectorA05グループが悪用した税金関連文書]

攻撃の流れ

1. [初期アクセス] フィッシング: スピアフィッシング添付ファイル (T1566.001)
    a. "LNK" ファイルが添付されたフィッシングメールの送信
    b. 政府関連文書の利用
2. [実行] コマンドおよびスクリプトインタープリタ: PowerShell (T1059.001)
    a. "PowerShell" スクリプトの実行
    b. BIOSシリアル番号の確認およびディレクトリの作成
3. [実行] コマンドおよびスクリプトインタープリタ: Visual Basic (T1059.005)
    a. "VBScript" の実行
    b. 追加ファイルのダウンロード
4. [持続性] ブートまたはログオン自動開始実行: レジストリ実行キー/スタートアップフォルダ (T1547.001)
    a. "1.log" および "1.vbs" ファイルの持続性の作成
5. [防御回避] ファイルまたは情報のデオブスクエート/デコード (T1140)
    a. "Base64" エンコードされたスクリプトのデコード
    b. 難読化の回避
6. [資格情報アクセス] パスワードストアからの資格情報: ウェブブラウザからの資格情報 (T1555.003)
    a. ブラウザからのログイン資格情報の抽出
    b. パスワードの復号化および情報の抽出

7. [発見] システム情報の発見 (T1082)
   a. システム情報の収集
   b. 仮想マシンの実行確認
8. [収集] 入力キャプチャ: キーロギング (T1056.001)
   a. キーロギング活動の実施
   b. クリップボードの監視
9. [コマンドと制御] アプリケーション層プロトコル: ウェブプロトコル (T1071.001)
   a. C2サーバーとの通信
   b. データのアップロードおよびダウンロード
10. [データ流出] C2チャネルを介したデータ流出 (T1041)
    a. データを "HTTP POST" リクエストで送信
    b. 収集された情報の圧縮および送信

11) SectorA05はBlueMoonSoftソフトウェアに偽装したマルウェアを使用しました (2025-04-11)

https://cti.nshc.net/events/view/14198

攻撃対象産業群: 健康、政府・行政、防衛、教育、エネルギー、シンクタンク

SectorA05グループは最近、韓国の複数の攻撃対象を狙った広範なサイバー攻撃キャンペーンを展開しました。彼らはソーシャルエンジニアリング技術、スピアフィッシング、ウォータリングホール攻撃を実行し、機密情報を盗むためにマルウェアを配布しました。彼らの攻撃ツールはWindowsとAndroidプラットフォームの両方を対象としており、使用されたマルウェアは韓国のソフトウェア会社「BlueMoonSoft」の署名を利用して合法的なソフトウェアに偽装されていました。主要な構成要素の一つは、動的ドメイン名を使用してコマンド＆コントロール（C2）サーバーに接続するバックドアで、感染したデバイスからシステムおよびネットワーク情報を収集し、追加のペイロードをダウンロードすることができます。最近のバージョンで追加された高度な機能には、特定のホスト名を持つデバイスでのみ完全に実行されるホストベースのターゲティングがあり、これは「Danam」のような特定の韓国企業を狙ったものと見られます。もう一つの重要な機能は、「regsvr32.exe」ユーティリティを使用してDLLマルウェアを活性化した後、攻撃の痕跡を消すための自己削除ルーチンです。今回のキャンペーンは非常に精密で進化する脅威を示しています。

攻撃の流れ

1. [初期アクセス] スピアフィッシング添付ファイル (T1193)
   a. スピアフィッシングメール送信
   b. 悪性添付ファイルの実行誘導
2. [実行] コマンドとスクリプトインタープリタ: Windowsコマンドシェル (T1059.003)

a. "regsvr32.exe"を使用した"DLL"マルウェアの実行
b. "msbuild.bat"の実行で自己削除開始
3. [持続性] ブートまたはログオン自動開始実行: レジストリ実行キー/スタートアップフォルダ (T1547.001)
a. "sc.exe"でサービス作成
b. 持続性のためにシステム起動時に実行
4. [防御回避] 偽装: 正当な名前または場所に一致 (T1036.005)
a. "BlueMoonSoft"署名使用
b. ファイル名およびパスの偽装
5. [資格情報アクセス] 入力キャプチャ: キーロギング (T1056.001)
a. キーボード入力記録
b. クリップボードデータ収集
6. [発見] システム情報発見 (T1082)
a. "systeminfo"コマンド使用
b. "ipconfig /all"コマンド使用
7. [収集] スクリーンキャプチャ (T1113)
a. スクリーンショットキャプチャ
b. 画像収集
8. [コマンドと制御] アプリケーション層プロトコル: ウェブプロトコル (T1071.001)
a. "POST"リクエスト送信
b. 動的ドメイン名使用
9. [データ流出] C2チャネル経由のデータ流出 (T1041)
a. 収集されたデータ送信
b. C2サーバーと通信してコマンド受信

12) SectorA05はMySpyマルウェアとRDPWrapを使用して持続的なアクセスを確保しました (2025-04-14)

https://cti.nshc.net/events/view/14425

攻撃対象産業群: エネルギー、金融、IT

2023年10月、精巧なサイバー脅威が韓国の「ソフトウェア」、「エネルギー」、「金融」産業を対象に発見されました。「フィッシング」メールは日本、アメリカ、中国、および複数のヨーロッパとアジアの国々にも送信されました。SectorA05グループは「リモートデスクトッププロトコル」（RDP）の脆弱性、特に「BlueKeep脆弱性」（CVE-2019-0708）を悪用して初期システムアクセスを試みました。侵入後、該当グループは「マイスパイ（MySpy）」Malwareと「RDPWrap」を利用して持続的なリモートアクセスを確立し、システム設定を変更しました。また、「KimaLogger」と

「ランダムクエリ（RandomQuery）」のようなキーロガーを配布してユーザーのキー入力を収集しました。このキャンペーンは「スピアフィッシングメール」を使用し、様々なハッキング技術を活用してネットワークに侵入しました。脅威に関連するインフラは「r-e[.]kr」や「kro[.]kr」といったドメインを活用しました。また、「RDP」脆弱性スキャナーがコマンドラインインターフェースおよびグラフィカルユーザーインターフェースで使用されましたが、感染したシステムに保存されたほとんどの事例は攻撃に積極的に使用されませんでした。

[攻撃の流れ]

1. [初期アクセス] スピアフィッシング (T1566.001)
   a. スピアフィッシングメール送信
   b. 攻撃対象産業群にメール送信
2. [実行] 公開アプリケーションのエクスプロイト (T1190)
   a. BlueKeep脆弱性(CVE-2019-0708)の悪用
   b. RDP脆弱性の悪用
3. [永続性] 外部リモートサービス (T1133)
   a. RDPWrapを使用してリモートアクセスを維持
   b. システム設定の変更
4. [収集] 入力キャプチャ (T1056)
   a. KimaLoggerの配布
   b. RandomQueryを使用してキー入力を記録
5. [コマンド＆コントロール] ツールの転送 (T1105)
   a. MySpyマルウェアの送信
   b. ドメイン "r-e[.]kr", "kro[.]kr" の使用
6. [発見] システムネットワーク接続の発見 (T1049)
   a. RDP脆弱性スキャナーの使用
   b. ネットワーク接続の探索

13) SectorA05は、著作権の詳細に偽装したURLマルウェアを使用しました (2025-03-25)

https://cti.nshc.net/events/view/13702

SectorA05グループは「著作権関連内訳.url」というファイル名を使用してハッキング攻撃を行いました。彼らが悪用した悪性ファイルは約1MBのインターネットショートカットファイルで、内部URLを操作してMalwareを実行するように設計されています。このグループはファイルアイコンをMicrosoft Edgeに設定し、攻撃対象がこれを正規のブラウザショートカットと誤認して実行するよう誘導する手法を使用しました。この攻撃はフィッシング技法を活用し、invoice-docs-file[.]siteというドメインを使用し、実際にはポート80のローカルサーバーに接続して「ready.pif」というファ

イルを実行しようとしました。このファイルはプログラム情報ファイル（Program Information File）に偽装してアンチウイルス検出を回避し、実行ファイル（.exe）のように動作します。このような手法は過去の2021年国防部報告書に偽装した攻撃と類似しています。彼らはURL操作、アイコン偽装、形式トリックなどの技術を通じてMalwareを効果的に拡散しています。

攻撃の流れ

1. [実行] ユーザー実行 (T1204.002)
   a. "저작권관련내역.url" ファイル実行
   b. マイクロソフト エッジ (Microsoft Edge) アイコンに偽装
2. [持続性] ファイルおよびディレクトリの権限変更 (T1222)
   a. .pif ファイル拡張子使用
   b. プログラム情報ファイル (Program Information) ファイルに偽装
3. [防御回避] 偽装 (T1036.005)
   a. マルウェア URL 操作
   b. フィッシングドメイン (invoice-docs-file[.]site) 使用
4. [コマンド＆コントロール] アプリケーション層プロトコル (T1071.001)
   a. ポート80ローカルサーバー接続試行
   b. 内部URLを通じてマルウェアをダウンロードおよび実行

14) SectorA07は、スパイ活動のために.docx文書に偽装したKonni RATを使用しました (2025-03-28)

https://cti.nshc.net/events/view/13883

攻撃対象産業群: 政府・行政、政党

Konni RATはSectorA07グループによって開発された高度なリモートアクセス型トロイの木馬であり、Windowsシステムを主な攻撃対象とし、多段階攻撃戦略を活用しています。このマルウェアは、Windowsエクスプローラーのファイル拡張子の非表示機能とWindowsショートカット（LNK）ファイルの260文字パス制限を悪用してシステムに密かに侵入します。攻撃の過程では、バッチファイル、PowerShellスクリプト、VBScriptを使用してシステム情報やユーザーデータを収集し、暗号化されたURLを通じてリモートサーバーに流出させます。初期配布は「folder.zip」のような圧縮ファイルで行われ、静的分析を回避するためにタイムスタンプベースのURL生成や複雑なスクリプト化などの難読化技術が使用されます。持続性はレジストリの修正を通じて確保され、一時ファイルは戦略的に削除されてフォレンジック分析を困難にします。これらの高度な機能により、Konni RATはデータ流出、システムコマンドの実行、長期的なアクセス維持などを可能にし、深刻なセキュリティ脅威となります。

攻撃の流れ

1. [初期アクセス] フィッシング (T1566)
   a. マルウェアが添付されたフィッシングメールの送信
   b. ユーザーが添付ファイルを実行してLNKファイルを有効化
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. LNKファイルを通じてcmd.exeを実行
   b. PowerShellスクリプトを通じて追加の悪意ある活動を実行
3. [持続性] レジストリ実行キー/スタートアップフォルダ (T1547.001)
   a. レジストリキーの修正による持続性の維持
   b. ユーザーログイン時に「start.vbs」を自動実行設定
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. ファイルパスおよびURLの難読化
   b. タイムスタンプに基づくURL生成で検出回避
5. [収集] ローカルシステムからのデータ (T1005)
   a. システム情報およびユーザーファイルの収集
   b. 収集されたデータを一時ファイルに保存
6. [流出] C2チャネルを介したデータ流出 (T1041)
   a. 暗号化されたURLを通じてデータを送信
   b. リモートサーバーへの機密情報の流出
7. [影響] データ破壊 (T1485)
   a. 一時ファイルおよびコマンドの削除で痕跡を除去
   b. フォレンジック分析を妨害するためにログをクリアリング

15) SectorA07は警察を装ったスピアフィッシングを使用しました（2025-03-31）

https://cti.nshc.net/events/view/13900

攻撃対象産業群: 非政府組織(NGO)、警察・法執行機関

SectotorA07グループは、2025年1月から3月の間に韓国の政府機関である「国家人権委員会」と「警察庁」を装ってスピアフィッシング攻撃を実行しました。この攻撃は主に北朝鮮の人権活動家とNGOを標的とし、不安と好奇心を刺激することで成功率を高めようとしました。脅威行為者は「C2」サーバーを利用して送信者アドレスを偽装し、メール内に悪意のあるファイルのダウンロードリンクを意図的に含めました。特に、WindowsショートカットファイルとAutoITスクリプトを使用してMalwareを配布する洗練された手法を使用しました。彼らは警察を装ったメールで受信者のメールアカウントが侵害されたと主張し、個人情報の提供を促しました。「EXE」、「MSI」、「LNK」などの様々な悪意のあるファイルが使用され、これらの高度な持続的脅威(APT)の進化した複雑さを示し

ました。攻撃に使用されたインフラと言語、特に特定の北朝鮮語の用語は、歴史的なサイバー活動に関連する既知の脅威キャンペーンとの関連性を示しました。

攻撃の流れ

1. [偵察] 情報を求めるフィッシング (T1598)
   a. 政府機関を装ったメール送信
   b. 不安心理を刺激して返信を誘導
2. [リソース開発] インフラの取得 (T1583)
   a. C2サーバーの設定
   b. PHPMailerで送信者情報を偽装
3. [配信] スピアフィッシング添付ファイル (T1566.001)
   a. LNKファイルの添付
   b. AutoITスクリプトの含有
4. [実行] ユーザー実行 (T1204)
   a. 受信者がLNKファイルをクリック
   b. PowerShellコマンドの実行
5. [持続性] システムプロセスの作成または変更 (T1543)
   a. タスクスケジューラへの登録
   b. AutoITスクリプトの繰り返し実行
6. [コマンドと制御] アプリケーション層プロトコル (T1071)
   a. C2サーバーとの通信
   b. AutoITスクリプトを通じたコマンドの伝達
7. [収集] ローカルシステムからのデータ (T1005)
   a. ユーザー情報の収集
   b. 機密データの窃取
8. [流出] C2チャネルを介したデータ流出 (T1041)
   a. 収集されたデータをC2に送信
   b. 外部サーバーにデータを保存

16) SectorB01はKeyPlugを使用してFortinetファイアウォールを悪用し、ウェブシェルを展開しました（2025-04-17）

https://cti.nshc.net/events/view/14469

攻撃対象産業群: IT

SectorB01グループが主要な日本企業の「フォーティネット(Fortinet)」インフラを対象にサイバー攻撃ツールを一時的に露出しました。露出されたサーバーは1日も稼働しておらず、フォーティネッ

トのファイアウォールとVPNサービスを悪用するためのスクリプト、「PHP」ベースのウェブシェル、そして企業の認証および内部ポータルを狙ったネットワーク偵察スクリプトが含まれていました。主要なツールには、フォーティネットのログインポータルとJavaScriptハッシュ値を識別して適切な脆弱性を見つけるフォーティネット偵察Pythonスクリプト、そしてフォーティネットの「WebSocket CLI」エンドポイントを自動的に悪用して権限のないコマンド実行を可能にするスクリプトがありました。「PHP」ウェブシェル「bx.php」は暗号化されたリモートコマンド実行を可能にし、PowerShellリバースシェル「client.ps1」はTCPベースの持続的なコマンド実行を可能にしました。これらのツールは、彼らの偵察、初期アクセス、悪用戦略に関する詳細な運用インサイトを提供し、彼らのインフラ目標、潜在的なラテラルムーブメント、事後悪用目標を示しています。

攻撃の流れ

1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. "Fortinet" ファイアウォールおよびVPNサービスの悪用
   b. "Fortinet" ログインポータルの偵察
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. "PHP" ベースのウェブシェル "bx.php" で暗号化されたコマンドを実行
   b. "PowerShell" リバースシェル "client.ps1" でTCPベースのコマンドを実行
3. [持続性] サーバーソフトウェアコンポーネント (T1505)
   a. "bx.php" を通じた持続的なウェブベースのアクセス
   b. "client.ps1" を通じた持続的なTCPセッションの維持
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. "Fortinet" の "WebSocket CLI" エンドポイントの悪用
   b. 管理者アカウント情報の収集と権限昇格
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. "bx.php" のAESおよびXOR暗号化の使用
   b. "client.ps1" のAES-128暗号化を通じた通信の隠蔽
6. [資格情報アクセス] 保護されていない資格情報 (T1552)
   a. "Fortinet" JavaScriptハッシュ値で脆弱なバージョンを識別
   b. ログインポータルおよび内部システム情報の収集
7. [探索] ネットワークサービススキャン (T1046)
   a. "fscan" でポートスキャンおよびサービスの列挙
   b. "script.py" でCDN保護の有無を確認
8. [収集] ローカルシステムからのデータ (T1005)
   a. システムおよびネットワーク情報の収集
   b. 認証および内部ポータルデータの収集
9. [コマンドと制御] 暗号化されたチャネル (T1573)

a. "bx.php" および "client.ps1" の暗号化されたコマンドおよび制御チャネル
b. "Server" を通じたHTTPベースのセッション管理
10. [データ流出] C2チャネルを介したデータ流出 (T1041)
a. TCPを通じた持続的なコマンドおよびデータの流出
b. HTTPベースのセッションを通じたデータ転送

17) SectorB01はDLLサイドローディングを通じて偽装されたSparrowDoorバックドアを使用しました (2025-03-26)

https://cti.nshc.net/events/view/13763

攻撃対象産業群: 金融、研究所

SectorB01グループは2024年7月にアメリカの金融産業の貿易団体とメキシコの研究所を攻撃しました。該当グループはまず「IISサーバー」にウェブシェルを展開して初期アクセスを達成し、これはサポートされていない「マイクロソフトExchangeサーバー」の脆弱性を悪用したものと見られます。彼らの主要なペイロードは2つのバージョンの「SparrowDoorバックドア」と「ShadowPadバックドア」でした。「SparrowDoor」の2つのバージョンはどちらも、モジュール式の構造とコマンドの並列実行を含むかなりの改善を示しました。彼らは「DLLサイドローディング」技術を使用して、「K7AntiVirus」や「VLCメディアプレーヤー」などの合法的なプロセスにマルウェアローダーを注入しました。攻撃キャンペーンは、「Microsoft Office IME」や「K7 Antivirus」などの合法的なサービスを模倣するインフラを使用して防御を欺く方法を明らかにしました。バックドアは、暗号化された通信とディスクに痕跡を残さない反射的ローディング技術を通じてコマンドを実行しました。これらの作戦は、グループが継続的にツールを開発し、洗練させていることを示しています。

攻撃の流れ

1. [初期アクセス] 公開されたアプリケーションのエクスプロイト (T1190)
a. IISサーバーにウェブシェルを配布
b. Microsoft Exchangeサーバーの脆弱性を悪用
2. [実行] コマンドラインインターフェース: PowerShell (T1059.001)
a. PowerShellセッションの使用
b. "SparrowDoor"の配布
3. [持続性] ブートまたはログオン自動開始実行: レジストリのRunキー/スタートアップフォルダ (T1547.001)
a. レジストリの"Run"キーを作成
b. "SparrowDoor"サービスを作成
4. [防御回避] 実行フローのハイジャック: DLLサイドローディング (T1574.002)
a. "K7AntiVirus"のサイドローディング

b. "VLCメディアプレーヤー"のサイドローディング
5. [コマンド＆コントロール] 非アプリケーション層プロトコル (T1095)
a. TCPソケットを通じたC&Cサーバーとの通信
b. RC4暗号化の使用
6. [データ抽出] C2チャネルを介したデータ抽出 (T1041)
a. C2チャネルを通じたデータの流出
b. 4kBチャンクでデータを分割して送信

18) SectorB02は、東南アジアでのスパイ活動のためにサイドロードされたマルウェアを使用しました（2025-04-18）

https://cti.nshc.net/events/view/14490

攻撃対象産業群: 政府・行政、通信、建設

SectorB02グループは、2024年8月から2025年2月にかけて、東南アジアの複数の機関を対象にサイバー諜報キャンペーンを実施しました。今回の攻撃の対象には、政府機関、航空交通管制組織、通信事業者、建設会社などが含まれ、他の東南アジア諸国のニュースエージェンシーや航空貨物組織も被害を受けました。該当グループは、「トレンドマイクロ」と「ビットディフェンダー」の合法的なソフトウェアを使用して、悪性DLLをロードするDLLサイドローディング技法を使用しました。具体的には、「tmdbglog.exe」や「bds.exe」といった実行ファイルを使用して、悪性DLL（「tmdglog.dll」、「log.dll」）をサイドローディングし、暗号化されたMalwareコンテンツを実行しました。また、「Sagerunex」バックドアの新しい変種を配布し、レジストリの修正によって持続性を確保しました。Chromeブラウザの資格情報を窃取するための「ChromeKatz」と「CredentialKatz」ツール、およびリモートアクセスのためのリバースSSHツールも使用されました。さらに、該当グループは「datechanger.exe」を使用してファイルのタイムスタンプを操作し、フォレンジック分析を困難にしました。

攻撃フロー

1. [実行] DLL サイドローディング (T1073.005)
a. "tmdbglog.exe"による"tmdglog.dll"のサイドローディング
b. "bds.exe"による"log.dll"のサイドローディング
2. [持続性] システムプロセスの作成または変更 (T1543.003)
a. レジストリの修正で"Sagerunex"バックドアの持続性を確保
b. サービスを通じてバックドアの実行を維持
3. [資格情報アクセス] OS 資格情報ダンピング (T1003)
a. "ChromeKatz"を使用してChrome資格情報を窃取
b. "CredentialKatz"を使用して追加の資格情報を窃取

4. [防御回避] 偽装 (T1036)
    a. "datechanger.exe"でファイルのタイムスタンプを操作
    b. 正当なソフトウェアに偽装して悪性活動を隠蔽
5. [コマンド＆コントロール] ツール転送の侵入 (T1105)
    a. リバースSSHツールを通じてリモートアクセスを取得
    b. 内部サービスの露出のためにP2Pツールを使用

19) SectorB21は正規のアプリに偽装したAndroidスパイウェアを使用しました (2025-04-09)

https://cti.nshc.net/events/view/14168

攻撃対象産業群: 市民

「MOONSHINE」と「BADBAZAAR」は、それぞれチベット人、ウイグル人、および台湾人を標的とするスパイウェアの亜種です。「MOONSHINE」は2019年に初めて識別され、「Telegram」と「WhatsApp」を通じて合法的なAndroidアプリに偽装し、チベット人を監視します。このスパイウェアは、ファイル抽出およびオーディオと画面録画機能を持ち、継続的に進化する管理インターフェースを通じて制御されます。「BADBAZAAR」はiOSとAndroidの両方に影響を与え、ソーシャルメディアやアプリストアでターゲットコミュニティに興味を引くアプリに偽装して拡散されます。このスパイウェアは、「BadSolar」や「BadSignal」といった亜種間で重複する機能を活用し、コマンド＆コントロール（C2）ドメインをクラスタリングします。両スパイウェアは、社会工学を利用して信頼されたネットワークを悪用できる悪性の特性をアプリケーションに組み込みます。技術的指標は、この作戦が以前に知られたフィッシャードメインおよびスクリプトと関連しており、仮想マシンと共有SSL証明書を含むかなりのインフラを持っていることを強調しています。これは、検出を回避し、リモートで機密データを収集して地政学的情報を得ようとする洗練された試みを示しています。

攻撃の流れ

1. [偵察] オープンウェブサイト/ドメインの検索 (T1593.001)
    a. オンライングループおよびフォーラムの検索
    b. 対象マッチンググループにマルウェアを共有
2. [リソース開発] インフラストラクチャの取得 (T1583.001)
    a. コマンド＆コントロール (C2) サーバー用ドメイン登録
    b. インフラの準備
3. [リソース開発] 能力の開発 (T1587.001)
    a. トロイの木馬アプリにマルウェアを挿入
    b. 悪性機能の開発
4. [リソース開発] 能力のステージング (T1608.001)
    a. トロイの木馬アプリをアプリストアにアップロード

b. 攻撃準備完了

5. [初期アクセス] ドライブバイ妥協 (T1189)
   a. アプリストアで悪性スクリプトを含むアプリをアップロード
   b. エンドユーザーがアプリをインストール
6. [実行] ユーザー実行 (T1204.002)
   a. ユーザーによるトロイの木馬アプリのインストール
   b. マルウェアペイロードの実行
7. [防御回避] 難読化されたファイルまたは情報 (T1027.009)
   a. マルウェアペイロードを合法的なアプリに隠す
   b. 検出回避の試み
8. [防御回避] 偽装 (T1036.005)
   a. 合法的な名前および位置でトロイの木馬ファイルを偽装
   b. ユーザーの信頼を確保
9. [収集] オーディオキャプチャ (T1123)
   a. マイクアクセス権限の要求
   b. オーディオデータの収集
10. [コマンド＆コントロール] アプリケーション層プロトコル (T1071.001)
    a. HTTPSおよびWebSocketを通じたC2通信
    b. データ送信およびコマンド受信
11. [データ流出] C2チャネルを介したデータ流出 (T1041)
    a. C2チャネルを通じたデータ抽出
    b. 機密情報の送信

20) SectorB53はBPFDoorバックドアを使用してLinuxサーバーでスパイ活動を行いました (2025-04-14)

https://cti.nshc.net/events/view/14369

攻撃対象産業群: 金融、小売、通信

SectorB53グループが利用したBPFDoorは、国家の支援を受けたバックドアであり、通信、金融、小売業など多様な攻撃対象産業を対象にサイバー諜報活動を行いました。このマルウェアは、韓国、香港、ミャンマー、マレーシア、エジプトなどの地域のLinuxサーバーを「バークレーパケットフィルタリング」（BPF）を利用したネットワークパケット検査を通じて悪用しました。特に、BPFDoorはリバースシェルを開くことができるコントローラーを活用して侵害されたネットワーク内で横方向の移動が可能であり、機密データにアクセスすることができました。このコントローラーはパスワードを要求し、TCP、UDP、ICMPなどの多様なプロトコルと設定可能なマジックシーケンスを使用してバックドアを活性化します。プロセス名の変更、非リスニングポートなどの技法を活用して検出ツ

ールを回避しました。BPFDoorは過去4年以上にわたり、アジア、中東、アフリカ地域の組織を継続的に攻撃してきました。攻撃ベクターとしては、「/tmp/zabbix_agent.log」のような隠されたパスに偽装する方法を使用し、MySQLのようなソフトウェアを実行するサーバーを主に狙いました。この点で、BPFDoorは洗練されており、適応力に優れたサイバー脅威と評価されています。

攻撃の流れ

1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. リナックスサーバーのネットワークパケット検査
   b. BPFを利用した脆弱性の悪用
2. [実行] コマンドとスクリプトインタープリター (T1059)
   a. リバースシェルを開いてリモートコマンドを実行
   b. コントローラーを通じたコマンド伝達
3. [持続性] ブートまたはログオン初期化スクリプト (T1037)
   a. 隠されたパスにファイルを偽装
   b. 最小限のログで攻撃を持続
4. [権限昇格] 権限昇格制御メカニズムの悪用 (T1548)
   a. パスワード要求による権限昇格
   b. バックドアの有効化手順
5. [防御回避] 偽装 (T1036)
   a. プロセス名の変更
   b. 非リスニングポートを使用して検出回避
6. [資格情報アクセス] 非安全な資格情報 (T1552)
   a. ネットワーク内の機密データへのアクセス
   b. サーバー内のアカウント情報の収集
7. [探索] システム情報の探索 (T1082)
   a. 侵害されたネットワーク環境の把握
   b. システム情報の収集
8. [横移動] リモートサービス (T1021)
   a. 横移動を通じたネットワーク拡張
   b. 他のシステムへのアクセス試行
9. [収集] ローカルシステムからのデータ (T1005)
   a. 機密データの収集
   b. データの圧縮と送信準備
10. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
    a. TCP、UDP、ICMPプロトコルの使用
    b. 設定可能なマジックシーケンスで通信維持

11. [データ流出] C2チャネル経由のデータ流出 (T1041)
    a. 収集したデータの送信
    b. C2チャネルを通じた情報流出

21) SectorB86によるIvanti ICSのポストパッチエクスプロイトを通じた標的化 (2025-04-04)

https://cti.nshc.net/events/view/14370

2025年4月、SectorB86グループが「Ivanti Connect Secure」（ICS）機器の脆弱性「CVE-2025-22457」を悪用する事例が観察されました。この脆弱性はICSバージョン「22.7R2.5」およびそれ以前のバージョンに影響を与え、バッファオーバーフローの欠陥を通じてリモートコード実行（Remote Code Execution, RCE）が可能になります。「Ivanti」は2025年2月にパッチ「22.7R2.6」を配布しました。しかし、SectorB86グループはそのパッチをリバースエンジニアリングしてパッチの修正内容を分析し、依然として更新されていないシステムを特定して脆弱性を再悪用しました。これはセキュリティパッチ分析に基づく後続攻撃（Post-Patch Exploitation）戦略の代表的な事例と評価されています。
これらは、「TRAILBLAZE」というメモリ常駐型ドロッパーを使用して検出を回避し、「/home/bin/web」プロセスに注入されるパッシブバックドア「BRUSHFIRE」を活用し、以前に知られている「SPAWN」エコシステムのMalwareコンポーネントを配布しました。また、Ivantiの整合性検査ツール「ICT」を改ざんして検出を避けました。この事件は、パッチ後の再悪用のリスクを強調し、彼らがセキュリティ修正を分析してまだ更新されていない脆弱なシステムを特定し攻撃する方法を示しています。「Ivanti」は、すべての顧客に最新のパッチを迅速に適用することを推奨しており、ICS「9.x」および「22.7R2.6」以前のバージョンのようなサポートされていないバージョンを実行しているシステムは特に危険であるため、即時の対応が必要です。

攻撃の流れ

1. [初期アクセス] 脆弱性の悪用 (T1190)
    a. "CVE-2025-22457" 脆弱性の悪用
    b. リモートコード実行 (RCE) の実行
2. [実行] コマンドとスクリプトインタープリター (T1059)
    a. システムコマンドの実行
    b. "TRAILBLAZE" ドロッパーの配布
3. [持続性] 内部バックドアのインプラント (T1504)
    a. "/home/bin/web" プロセスに "BRUSHFIRE" を注入
    b. C2サーバーとの接続なしでバックドアが動作
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
    a. メモリ常駐型ドロッパーの使用

b. "ICT" を改ざんして検出回避
5. [認証情報アクセス] 運用データの窃取 (T1003)
a. 認証情報の窃取
b. システムデータの収集
6. [発見] システム情報の発見 (T1082)
a. システム情報の収集
b. ネットワーク環境の探索
7. [収集] データの準備 (T1074)
a. 窃取データの収集
b. データの準備と送信
8. [流出] 他のネットワーク媒体を介した流出 (T1048)
a. データの外部送信
b. ネットワーク境界を通じたデータ流出
9. [影響] データ操作 (T1565)
a. システムの整合性の低下
b. データの改ざんと破壊

22) SectorB86はヨーロッパでのスパイ活動にBRICKSTORMバックドアを使用しました (2025-04-17)

https://cti.nshc.net/events/view/14420

SectorB86グループは2022年からヨーロッパの戦略産業群を対象に長期的なサイバースパイ活動を行っています。このグループは以前にLinux環境で発見されたことのある「BRICKSTORM」バックドアのWindowsバリアントを利用しています。「BRICKSTORM」はファイル管理とネットワークトンネリング機能を持ち、これを通じてグループはファイルシステムの探索、ファイル管理、ネットワーク接続のトンネリングなどを行い、ネットワーク内のラテラルムーブメント（Lateral Movement）を容易にします。このマルウェアはDNS over HTTPS（DoH）を通じてコマンド＆コントロール（Command & Control, C2）サーバーと通信し、ネットワーク通信を隠し、一般的なモニタリングソリューションを回避します。持続性はタスクスケジューラを通じて維持され、マルウェアはネットワークトンネリングと正当な資格証明を組み合わせてコマンドを実行することで検出を回避します。このグループのインフラは「Cloudflare」や「Heroku」などのクラウドサービスを活用し、合法的なトラフィックと混合されるため、検出と追跡が困難です。

攻撃の流れ

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
a. 精巧なフィッシングメールの送信

b. マルウェア URL クリック誘導
2. [実行] コマンドとスクリプトインタープリタ (T1059)
a. ネットワークトンネリング機能の使用
b. 正当な資格情報の活用
3. [持続性] スケジュールされたタスク/ジョブ (T1053)
a. スケジュールされたタスクの作成
b. 持続的なバックドアの実行
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. DoHを通じたC2サーバー通信
b. ファイルおよびネットワークトラフィックの暗号化
5. [資格情報アクセス] 有効なアカウント (T1078)
a. 正当な資格情報の確保
b. ネットワーク内移動
6. [探索] ファイルとディレクトリの探索 (T1083)
a. ファイルシステムの探索
b. ファイルリストの作成
7. [横方向移動] リモートサービス (T1021)
a. RDPおよびSMBプロトコルの悪用
b. ネットワーク内の横方向移動
8. [収集] ローカルシステムからのデータ (T1005)
a. ファイルのダウンロード
b. ファイルハッシュの確認
9. [流出] 代替プロトコルを介した流出 (T1048)
a. HTTP APIを通じたデータ送信
b. ファイルのアップロードおよびダウンロード
10. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
a. HTTPSを通じたC2サーバー通信
b. WebSocketアップグレードの使用

23) SectorB86はIvanti Connect Secure ExploitでRESURGEマルウェアを使用しました (2025-04-04)

https://cti.nshc.net/events/view/13901

SectorB86グループは、Ivanti Connect Secure (ICS) デバイスの特定のファームウェアバージョンである22.7.4.30859を標的に、高度なMalwareであるRESURGEを配布したと分析されています。RESURGEは32ビットLinux共有オブジェクトファイル（libdsupgrade.so）の形で抽出され、単一

のペイロード内にルートキット、ドロッパー、バックドア、ブートキット、プロキシおよびトンネリング機能をすべて統合した高リスクの複合モジュールです。この亜種は「SPAWNCHIMERA」Malwareと類似した機能を共有し、ファイルを改ざんし、整合性チェックを操作し、「Ivanti」ブートディスクにウェブシェルをインストールします。該当グループはXORで暗号化された秘密鍵を通じて接続し、トンネリングを使用して「me/runtime/tmp/.logsrv」ファイルと相互作用し、セキュアシェルにアクセスできます。「web」プログラムがアクティブな場合、Malwareは関数をフックし、暗号化されていないプロキシを使用してデータをデコードし、ネットワークを通じて通信します。「dsmdm」プログラムと共に、セキュアSSHスレッドを生成し、「ld.so.preload」に挿入し、検出を避けるためにPythonスクリプトを変更し、「coreboot」RAMディスクを操作します。「liblogblock.so」は「funchook」を使用してログをさらに悪用し、「dsmain」は「BusyBox」を通じて様々なシステムユーティリティを暗号化、復号化および実行します。

攻撃の流れ

1. [実行] コマンドとスクリプトインタープリター (T1059)
   a. "sed" コマンドを使用してファイル内容を修正
   b. "system()" を通じてスクリプトを実行
2. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. "ld.so.preload" に自身を挿入
   b. ウェブシェルを "compcheckresult.cgi" にインストール
3. [防御回避] ファイルまたは情報のデオブスクエート/デコード (T1140)
   a. XORで暗号化された秘密鍵を使用して通信
   b. "openssl" でファイルハッシュを計算および偽造
4. [資格情報アクセス] 保護されていない資格情報 (T1552)
   a. "private.pem" を生成してRSAキーのペアを作成
   b. "manifest" ファイルに署名
5. [探索] システム情報探索 (T1082)
   a. "proc" フォルダを列挙して "dslogserver" プロセスを検索
   b. "vmlinux" を抽出してカーネルコードを分析
6. [横移動] リモートサービス (T1021)
   a. SSHを通じてセキュアソケットシェルを生成
   b. トンネリングを通じたネットワーク接続およびデータ転送
7. [収集] ローカルシステムからのデータ (T1005)
   a. システムユーティリティを通じてファイルをコピーおよび改ざん
   b. "coreboot" RAMディスクを操作してデータを収集
8. [コマンドと制御] 暗号化されたチャネル (T1573)

a. 暗号化された通信経路を設定
b. トンネリングを通じたコマンドおよび制御チャネルを構築

24) SectorB94は、Linux攻撃のためにkworkerに偽装したSNOWLIGHTを使用しました (2025-04-15)

https://cti.nshc.net/events/view/14372

攻撃対象産業群: 防衛、エネルギー、技術、非政府組織(NGO)

SectorB94グループは2025年1月末に新しいサイバーキャンペーンを開始し、「SNOWLIGHT」マルウェアと「VShell」リモートアクセス型トロイの木馬（RAT）を活用しました。このキャンペーンは、アメリカ、カナダ、イギリスを含む西側諸国や複数の非政府組織（NGO）、重要なインフラ産業を対象としています。悪意のあるbashスクリプトが確認されており、これはバイナリをダウンロードして実行し、持続性を維持するために使用されました。ここには、F5機器の脆弱性を悪用したことで知られるSNOWLIGHTマルウェアの変種が含まれていました。SNOWLIGHTはファイルレスペイロードをドロップする役割を果たし、「VShell」はメモリ内メカニズムを通じて配布され、従来の検出方法を回避します。技術分析の結果、SNOWLIGHTはコマンド＆コントロール（C2）サーバーのためにWebSocketsを使用し、洗練された隠密な攻撃ベクトルを示しています。キャンペーンにはフィッシングのためのドメインスクワッティングが含まれており、これは馴染みのあるブランドを装って帰属を混乱させ、スパイ活動やアクセス権の販売を目的としていることを示唆しています。

攻撃フロー

1. [初期アクセス] フィッシング (T1566)
   a. ドメインスクワッティング
   b. フィッシングメール送信
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
   a. マルウェアbashスクリプト実行
   b. バイナリのダウンロードおよび実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. クーロンタブを通じた自動実行設定
   b. systemdサービスを通じた持続性維持
4. [防御回避] 偽装 (T1036)
   a. "[kworker/0:2]" プロセスとして偽装
   b. メモリ内実行を通じた検出回避
5. [コマンド＆コントロール] Webプロトコル (T1071)
   a. WebSocketsを通じたC2通信
   b. 暗号化されたトラフィックを通じたリアルタイムコマンド送信

6. [収集] 入力キャプチャ (T1056)
   a. 環境変数操作および収集
   b. リモートコマンド実行および情報収集
7. [データ流出] C2チャネルを通じたデータ流出 (T1041)
   a. WebSocketsを通じたデータ流出
   b. C2サーバーへの情報送信

25) SectorB95はESETの脆弱性エクスプロイトでDLLプロキシとBYOVDを使用しました（2025-04-07）

https://cti.nshc.net/events/view/14083

SectorB95グループは2024年初頭に複雑なサイバー脅威を実行しました。"TCESB"という名前の64ビットDLLファイルが、複数の攻撃対象システムの"temp"ディレクトリで発見され、保護ツールを回避する目的で設計されていました。この攻撃は、DLLプロキシ技法を利用して、マルウェアDLLが元のDLLの機能を再指定し、検出を避ける方法で行われました。マルウェアDLLをロードするためには、セキュリティが脆弱なコードを含むアプリケーションが必要でした。この活動は、CVE-2024-11859脆弱性を持つESETコマンドラインスキャナーコンポーネントが、セキュリティが脆弱な方法でライブラリをロードすることで可能になりました。TCESBは、オペレーティングシステムカーネル構造を修正する技術を使用し、脆弱なドライバ技術（BYOVD）を使用してCVE-2021-36276脆弱性を持つ"Dell DBUtilDrv2.sys"ドライバを活用しました。このツールはAES-128を使用してペイロードファイルを暗号化し、復号キーはこれらのファイルに内蔵されています。この事件は、既知のマルウェアとドライバ脆弱性を組み合わせて検出を回避する脅威の能力を強調しています。

攻撃の流れ

1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. ESETコマンドラインスキャナーの脆弱性(CVE-2024-11859)を利用
   b. マルウェアDLLロードのためのアプリケーションコードの脆弱性を活用
2. [防御回避] 実行フローのハイジャック (T1574)
   a. DLLプロキシ技法を使用してマルウェアDLLに機能を再指定
   b. セキュリティソリューションの回避および検出回避
3. [防御回避] 防御回避のためのエクスプロイト (T1211)
   a. 脆弱なドライバー技術(BYOVD)を使用
   b. "Dell DBUtilDrv2.sys"ドライバーのCVE-2021-36276脆弱性を活用
4. [実行] コマンドおよびスクリプトインタープリター (T1059)
   a. AES-128で暗号化されたペイロードファイルを実行
   b. ペイロードファイルから復号キーを抽出し、データブロックを実行

5. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. システムにドライバーをインストールして持続性を確保
   b. INFファイルを使用したドライバーインストール情報の提供

26) SectorC08は隠蔽と回避のためにDNSファストフラックスを使用しました (2025-04-08)

https://cti.nshc.net/events/view/14424

攻撃対象産業群: 政府・行政、国防、文化

SectorC08グループは2013年から活動しており、ウクライナ政府および市民団体を主な攻撃対象としています。また、西側の政府機関、アフリカ、NATO加盟国にもフィッシング戦略を通じて攻撃を拡大しています。このグループは「ファストフラックス（Fast Flux)」DNS技術を使用してインフラを隠蔽し、.ruドメインの背後でIPアドレスを動的に回転させて運営しています。これらのドメインは主に「REGRU-RU」を通じて登録され、ホスティングは主に「DigitalOcean」を通じて行われます。
このグループは攻撃活動を隠蔽し、持続的な運営の足跡を維持しようとする努力を示しており、彼らの脅威戦術とインフラ管理の複雑さを強調しています。

攻撃の流れ

1. [偵察] フィッシング (T1598)
   a. 西欧政府およびNATO加盟国を対象としたフィッシングキャンペーン
   b. ウクライナ政府および市民団体を対象としたフィッシングキャンペーン
2. [リソース開発] ドメイン生成 (T1584.001)
   a. "fast flux" DNS技法の使用
   b. ドメイン生成アルゴリズムの使用
3. [コマンド＆コントロール] 動的解決 (T1572)
   a. 動的DNSサービスの活用
   b. スプーフィングされたドメインの使用
4. [コマンド＆コントロール] トラフィックシグナリング (T1205)
   a. TLS証明書の模倣
   b. 制御されたアクセスポイントの維持
5. [実行] 共有モジュール (T1059)
   a. "ShadowPad" モジュール型バックドアの使用
   b. DLLサイドローディング技法の使用

27) SectorC08は、難読化されたPowerShellを使用してGammaSteelインフォスティーラーを使用しました（2025-04-10）

https://cti.nshc.net/events/view/14171

攻撃対象産業群: 政府・行政、防衛

2025年、サイバースパイキャンペーンがウクライナ内の西側諸国の軍事任務を狙って実施されました。攻撃は2月に始まり、感染した移動式ドライブを初期感染ベクターとして使用し、「GammaSteel」ツールの洗練されたバージョンを活用しました。「GammaSteel」は被害者システムから機密データを抽出するために設計された情報窃取ツールです。攻撃手法には、Webサービスを通じたデータ漏洩とTorプロキシをサポートする「cURL」コマンドが含まれていました。このキャンペーンはVBSスクリプトからPowerShellを利用した難読化に切り替え、悪意のあるスクリプトをレジストリに保存する方法を使用しました。技術的指標としては、「mshta[.]exe」と「wscript[.]exe」プロセスを使用した多段階攻撃チェーンを通じて持続性とコマンド＆コントロール（C&C）通信を確立しました。彼らは検出を避けるために洗練された技術を活用し、これにはPowerShellベースの偵察とHTTP POSTリクエストを通じたデータ窃取が含まれていました。C&Cサーバー通信はCloudflareトンネルを通じて行われ、難読化されたPowerShellコマンドでペイロードを実行し、システムデータを捕捉するなどの戦術調整が確認されました。

攻撃の流れ

1. [初期アクセス] リムーバブルメディア (T1091)
   a. 感染したリムーバブルドライブの使用
   b. "LNK"ファイルを通じた初期感染
2. [実行] スクリプティング (T1064)
   a. "mshta[.]exe"を通じたマルウェアの実行
   b. "wscript[.]exe"で"VBScript"を実行
3. [持続性] レジストリ実行キー / スタートアップフォルダ (T1547.001)
   a. "Run"レジストリキーに自身を登録
   b. レジストリを通じて悪性スクリプトを保存
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. PowerShellを利用した難読化
   b. "GammaSteel"ツールのコード修正
5. [資格情報アクセス] OS資格情報ダンピング (T1003)
   a. システム情報スクリプトの実行
   b. "systeminfo"コマンドの使用
6. [探索] システム情報探索 (T1082)
   a. システム情報の収集
   b. セキュリティソフトウェアの検出
7. [収集] ローカルシステムからのデータ (T1005)

a. 指定された拡張子のファイルを収集
b. "Desktop", "Documents", "Downloads"フォルダからファイルを列挙
8. [流出] 代替プロトコルを通じた流出 (T1048)
a. "cURL"とTorネットワークを通じたデータ流出
b. ウェブサービス"write[.]as"を通じた情報流出の試み
9. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
a. Cloudflareトンネルを通じたC&C通信
b. ハードコーディングされたC&Cアドレスの使用

28) SectorC08は、Officeドキュメントに偽装したLNKマルウェアを使用しました (2025-03-28)
https://cti.nshc.net/events/view/13821

SectorC08グループは2024年11月からウクライナを攻撃対象とし、マルウェアを含むWindowsショートカット（LNK）ファイルを利用したキャンペーンを展開しています。これらのファイルは「PowerShell」ダウンロードプログラムを実行し、ウクライナ侵攻をテーマにした「ロシア」という名前のファイルに偽装された「オフィス」ドキュメントを装っています。キャンペーンは「ロシア」と「ドイツ」に位置する地理的制限のあるサーバーを通じて、「Remcos」バックドアを含む第2段階の「ZIP」ファイルをダウンロードします。「DLLサイドローディング」を通じてバックドアを配布します。「メールフィッシング」がZIPファイルまたはリンクを添付して配布される可能性が高いです。メタデータによれば、わずか2台のマシンのみが使用されており、小規模な運用と見られます。「ダウンローダー」は「Get-Command」コマンドを使用して作業を実行し、これはアンチウイルス検出を回避するものと見られます。「GTHost」と「HyperHosting」でホスティングされている一部のペイロードサーバーは、ウクライナのIPアドレスにのみファイルを配信するようアクセスを制限しています。キャンペーンは「DLLサイドローディング」を活用し、合法的なアプリケーションが悪意のある「DLL」をロードするようにして「Remcos」バックドアをインストールし、その後146[.]185[.]233[.]96 IPの6856ポートを通じてC2サーバーと通信します。

攻撃の流れ
1. [初期アクセス] フィッシング (T1566)
a. ウクライナ侵攻をテーマにしたフィッシングメール送信
b. ZIPファイルやURLリンクを添付
2. [実行] ユーザー実行 (T1204)
a. マルウェア「LNK」ファイルの実行
b. 「PowerShell」ダウンロード実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. 「Get-Command」コマンドの使用

b. オフィス文書に偽装
4. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
a. 「Remcos」バックドアC2通信
b. 146[.]185[.]233[.]96:6856サーバーと接続
5. [持続性] DLLサイドローディング (T1574.002)
a. 正規のアプリケーションを通じてマルウェア「DLL」をロード
b. 「Remcos」バックドアのインストール

29）SectorC08は正規のファイルに偽装したPteroLNKマルウェアを使用しました（2025-04-16）

https://cti.nshc.net/events/view/14936

攻撃対象産業群: 政府・行政、軍事機関

SectorC08 グループは、2024 年末から 2025 年 3 月の間に「Pterodo」マルウェア系を配布し、ウクライナの政府、軍事、そして主要インフラを主なターゲットとしました。「PteroLNK」として知られる VBScript マルウェアを利用して、攻撃対象のシステムに侵入しようとしました。このマルウェアは、ウクライナのキーウなどの複数の都市で主にアップロードされ、攻撃対象のシステムを損傷させる意図を持っています。「PteroLNK」は、ダウンローダーおよび Windows ショートカット（LNK）ドロッパーペイロードを動的に構成し、スケジュールされたタスクや特定のアンチウイルスソフトウェアが検出された場合、無限ループを利用して持続性を確保します。C2 通信は、複雑なレジストリベースの持続性と Cloudflare トンネル、そして最新の C2 サーバーを指す Dead Drop Resolvers（DDR）を通じて維持されます。このマルウェアは、ローカルおよびネットワークドライブのショートカットを通じて拡散し、mshta.exe を通じて主なマルウェアを実行するリンクで既存のファイルを置き換えます。これらのキャンペーンは、過去の SectorC08 グループと関連する作戦と密接に一致しており、ウクライナの防衛を弱体化させようとする戦略的な焦点が明らかになっています。

攻撃の流れ

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
a. マルウェア VBScript ファイルのダウンロード
b. LNK ファイルを通じた初期アクセス
2. [実行] コマンドとスクリプトインタープリタ: VBScript (T1059.005)
a. mshta.exe を通じたマルウェアの実行
b. VBScript を通じたペイロードの実行
3. [持続性] スケジュールされたタスク/ジョブ (T1053.005)
a. スケジュールされたタスクを通じた持続性の確保
b. レジストリキーを通じた持続性の維持

4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. VBScript コードの難読化
   b. ファイルの隠し設定の変更
5. [資格情報アクセス] パスワードストアからの資格情報 (T1555)
   a. システム資格情報の収集
   b. 保存されたパスワードの抽出
6. [探索] システム情報の探索 (T1082)
   a. システム情報の収集
   b. ネットワークドライブの閲覧
7. [横方向移動] LNK ファイル (T1204.002)
   a. ネットワークドライブを通じた拡散
   b. リンクファイルを通じた移動
8. [コマンドとコントロール] アプリケーション層プロトコル: Web プロトコル (T1071.001)
   a. Cloudflare トンネルを通じた C2 通信
   b. DDR を活用した動的 C2 アドレスの発見
9. [影響] データ破壊 (T1485)
   a. ファイルの置換および削除
   b. データ破壊のためのリンクファイルの生成

30) SectorH03は、鉄道を攻撃するために偽装されたMicrosoft Installerを使用しました (2025-04-08)

https://cti.nshc.net/events/view/14130

攻撃対象産業群: ガス、政府・行政、防衛、石油、海上、鉄道

SectorH03 グループは、2024 年 12 月末から鉄道、石油・ガス、外務省を含む主要産業を対象とした攻撃で新しい戦略を使用しました。このグループは、「HTML Application」（HTA）ファイルの代わりに「Microsoft Installer」（MSI）パッケージを主な初期侵入メカニズムとして採用しました。DLL サイドローディング、リフレクションローディング（Side-Loading）、「Xeno RAT」や「Spark RAT」といったオープンソースツールの活用など、高度な技術が利用されました。新しい RAT である「CurlBack」は、DLL サイドローディングを使用して持続性を確保し、C2 サーバーとの接続を維持し、コマンドを実行する機能を備えています。スピアフィッシングメールは主な攻撃ベクターとして、政府機関に関連する文書で攻撃対象を誘引しました。また、電子政府ポータルを模倣した偽ドメインを通じて、資格情報フィッシングとマルウェアペイロードのホスティングが行われました。このキャンペーンは、Windows と Linux システムの両方を対象としており、カスタム RAT を配布してシステムデータを収集し、コマンドを実行し、情報を漏洩しました。

攻撃の流れ

1. [偵察] 被害者の身元情報収集 (T1589.002)
   a. 攻撃対象のメールアドレス収集
   b. 政府関係者を装う
2. [初期アクセス] フィッシング: スピアフィッシングリンク (T1566.002)
   a. スピアフィッシングメール送信
   b. リンクを通じたマルウェアファイルのダウンロード
3. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. マルウェア文書を開く
   b. MSI パッケージのインストール
4. [持続性] 実行フローのハイジャック: DLL サイドローディング (T1574.002)
   a. 正規のバイナリの隣に悪意のある DLL を配置
   b. 実行時に DLL サイドローディングが発生
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. Base64 エンコーディングの使用
   b. リフレクションローディング技法の使用
6. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. 資格情報の窃取
   b. 偽のログインページの使用
7. [コマンド＆コントロール] ツール転送の受信 (T1105)
   a. C2 サーバーとの接続
   b. コマンドの受信と実行
8. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. システムデータの収集
   b. C2 チャネルを通じたデータ流出

2. サイバー犯罪（Cyber Crime）ハッキンググループの活動

セクターJ113はRALordランサムウェアを使用しました（2025-04-02）

https://cti.nshc.net/events/view/13949

攻撃対象産業群: 学界 - 大学、製造、飲食店、工学

SectorJ113 グループは 2025 年 3 月に登場した新しい「ランサムウェア・アズ・ア・サービス（RaaS）」プラットフォームで、体系的な運営モデルを持ち、提携プログラムとデータ身代金メカニズムを含んでいます。このグループはサイバー犯罪フォーラムで活動しており、リーダーは「ForLord」という別名を使用しています。SectorJ113 グループが利用するランサムウェアは、以前の RaaS 運営経験を基に開発されており、これは類似した名前の他のグループとの潜在的な関連性を示唆しています。被害者情報は「データ漏洩サイト（Data Leak Site, DLS）」で公開され、このサービスはデータ仲介や広告を含むツールおよびサービスを有料で提供しています。提携メンバーは身代金収益の 85%を得ることができ、サイバー犯罪協力者を引き付けるための競争的な手数料構造を強調しています。このグループは被害者に身代金支払いを迫るためにカウントダウンを使用しました。

攻撃フロー

1. [初期アクセス] フィッシング (T1566)
   a. メールフィッシング
   b. マルウェアリンク配布
2. [実行] ユーザー実行 (T1204)
   a. 添付ファイル実行
   b. ダウンロードしたスクリプト実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. スタートアッププログラム登録
   b. レジストリ修正
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. 権限昇格脆弱性利用
   b. 管理者権限取得
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. コード難読化
   b. ファイル暗号化
6. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. メモリダンプ
   b. クレデンシャル収集
7. [探索] システム情報探索 (T1082)
   a. システム情報収集
   b. ネットワーク設定把握
8. [横移動] リモートサービス (T1021)
   a. RDP 使用
   b. SMB 活用

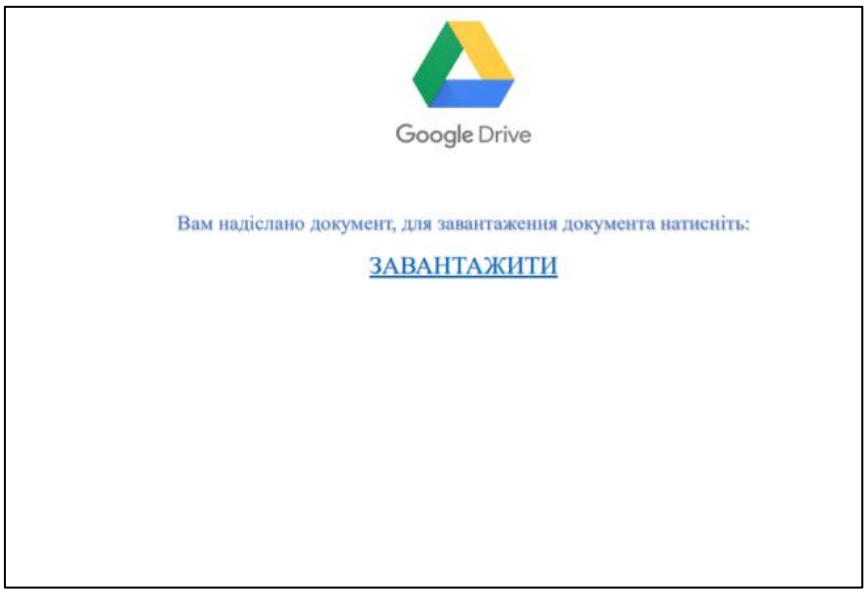
9. [収集] ローカルシステムからのデータ (T1005)
    a. ファイル収集
    b. スクリーンショットキャプチャ
10. [流出] C2 チャネル経由の流出 (T1041)
    a. 暗号化されたチャネルを通じたデータ送信
    b. C2 サーバーへの情報流出
11. [影響] 影響のためのデータ暗号化 (T1486)
    a. ファイル暗号化
    b. 身代金要求メッセージ表示

2) SectorJ149はフィッシングメールを通じてマルウェアを配布しました (2025-04-01)

https://cti.nshc.net/events/view/13913

攻撃対象産業群: 国防、エネルギー、ガス、政府・行政、銀行、非政府組織(NGO)、政党、メディア、保険、弁護士

SectorJ149 グループは、ウクライナおよび同盟国のエネルギー、政府、メディア産業を主な攻撃対象としてサイバー活動を増加させました。彼らは金融およびサイバー諜報目的のスパムキャンペーンを展開し、心理作戦として爆弾脅威を含むこともありました。攻撃はウクライナ、スイス、ドイツ、ポーランド、フランスの様々な組織を対象に行われました。ハッカーたちはキャンペーン全体を通じて Malware ツールを切り替え、「sLoad」や「NetSupport Manager」といった悪性ソフトウェアの配布に VBS スクリプトを使用しました。セキュリティ回避のために脆弱性を悪用し、受信者を損傷したリンクやメールに誘導するフィッシングメールを使用しました。攻撃セットは、複雑な法的フロントとオフショアのペーパーカンパニーで管理される違法ホスティングプロバイダーを活用して、検出とブロックを回避しました。例えば、「Railnet LLC」と「Global Connectivity Solutions LLP」はサイバー犯罪者の活動を支援し、ロシアを拠点とする偽情報およびランサムウェア攻撃と頻繁に関連付けられました。



[図 7: SectorJ149グループが悪用したフィッシング文書]

攻撃の流れ

1. [偵察] 被害者組織情報の収集 (T1591)
   a. 対象組織情報の収集
   b. ビジネス関係の把握
2. [リソース開発] インフラの取得 (T1583)
   a. ドメインの確保
   b. 仮想専用サーバー(VPS)の確保
3. [リソース開発] インフラの侵害 (T1584)
   a. ドメインの損傷
   b. サーバーの損傷
4. [初期アクセス] フィッシング (T1566)
   a. スピアフィッシング添付ファイルの使用
   b. スピアフィッシングリンクの使用
5. [実行] ユーザー実行 (T1204)
   a. マルウェアリンクの実行
   b. マルウェアファイルの実行
6. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. コマンドの難読化
   b. LNK アイコンのスモーリング
7. [コマンド＆コントロール] 非標準ポート (T1571)
   a. 非標準ポートの使用
   b. コマンド制御チャネルの構築

8. [データ流出] C2 チャネル経由のデータ流出 (T1041)
    a. C2 チャネルを通じた情報流出
    b. データ転送のセキュリティ回避
9. [影響] 金融窃盗 (T1657)
    a. 金融情報の窃取
    b. 不正金融取引の実行

3) SectorJ173は新しいドメインを使用してマルウェアを配布しました (2025-04-01)

https://cti.nshc.net/events/view/13931

SectorJ173 グループは、持続的ではあるが洗練されていないマルウェア「OUTLAW」を利用して、攻撃対象のシステムに積極的に侵入しています。このマルウェアは、SSH ブルートフォース攻撃、SSH キーの操作、cron を通じた持続性維持技術を組み合わせて感染を試み、主に弱いパスワードやデフォルトの資格情報が設定されたシステムを標的にして初期アクセスを確保します。アクセス権を得た後、修正された XMRIG ベースのマイニングツールを展開して暗号通貨のマイニングを行います。以下のマルウェアは、ワームに似た自己複製および拡散能力を基に、感染したホストを利用してローカルサブネット内で追加の SSH ブルートフォース攻撃を実行し、高度な技術がなくてもボットネットを急速に拡大させています。また、SectorJ173 グループは多段階感染手順を通じてマルウェアペイロードをダウンロードおよび実行し、競合するマルウェアを除去してシステムの支配力を高める戦略を併用しています。通信は IRC（Internet Relay
Chat）プロトコルを利用して C2 サーバーと接続され、これにより感染システムのコマンド制御権を持続的に維持します。

攻撃の流れ

1. [初期アクセス] ブルートフォース (T1110)
    a. SSH ブルートフォース攻撃
    b. 弱い資格情報のターゲティング
2. [実行] コマンドとスクリプトインタープリタ (T1059)
    a. "tddwrt7s.sh" スクリプトの実行
    b. "initall.sh" スクリプトの実行
3. [持続性] システムプロセスの作成または変更 (T1543)
    a. cron ジョブの作成
    b. SSH キーの操作
4. [防御回避] ホスト上のインジケータの削除 (T1070)
    a. 競合するブルートフォーサーおよびマイナーの削除
    b. ファイルおよびディレクトリの隠蔽

5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. SSH 公開キーの挿入
   b. ユーザーパスワードの変更
6. [発見] システム情報の発見 (T1082)
   a. システム CPU 情報の収集
   b. ユーザーおよび権限情報の収集
7. [横移動] リモートサービス (T1021)
   a. ローカルサブネットでの追加の SSH ブルートフォース攻撃
   b. 感染パッケージの拡散
8. [収集] ローカルシステムからのデータ (T1005)
   a. システムデータの収集
   b. SSH 詳細情報の収集
9. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
   a. IRC チャネルを通じたリモートコントロール
   b. "socat" プロセスの維持
10. [影響] リソースのハイジャック (T1496)
    a. 修正された "XMRIG" での暗号通貨のマイニング
    b. システムリソースの最適化

4) SectorJ174はフォーラムとTelegramを利用してマルウェアを販売していました (2025-04-14)

https://cti.nshc.net/events/view/14327

SectorJ174 グループは、当初は社会的利益を目的としたハッキング活動に集中していましたが、次第に金銭的利益を追求するサイバー犯罪へと活動の方向性を転換しました。彼らは様々なサイバー犯罪フォーラムでペルソナを開発し、能力を拡張し、ゼロデイ（Zero-day）脆弱性攻撃、ネットワークアクセスのターゲティング、ランサムウェアや情報窃取ツールのようなマルウェアを開発しました。また、グループはテレグラム（Telegram）を通じて「マルウェアサービス（MaaS）」や「ランサムウェアサービス（RaaS）」を広告し、ゼロデイ脆弱性を販売しました。金銭的利益を目的として運営されていたものの、腐敗防止の名目上の目標を維持し、腐敗の疑いがある団体を主な攻撃対象としました。彼らは他のハッカーやサイバー犯罪グループとの協力を通じて作戦範囲を拡大しました。複数のフォーラムでの活動禁止に対応し、メンバーや活動を調整し、データやデータベースの販売、新しいサイバー犯罪プロジェクトの立ち上げなど、収益を上げるための戦略的な変化を示しました。

攻撃の流れ

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
   a. ハッキングフォーラムで攻撃対象情報収集
   b. カスタマイズされたフィッシング攻撃で初期侵入試行
2. [実行] クライアント実行のためのエクスプロイト (T1203)
   a. ゼロデイ脆弱性を利用して実行
   b. リモートコード実行を通じたシステム掌握
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. Malware 自動実行設定
   b. 再起動時の持続的実行保証
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. システム権限昇格のための脆弱性悪用
   b. 管理者権限取得
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. コードを難読化して検出回避
   b. ファイアウォールおよびセキュリティソリューションの回避
6. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. システム内に保存された資格情報収集
   b. 認証情報の窃取による追加アクセス試行
7. [探索] ネットワークサービススキャン (T1046)
   a. ネットワークサービススキャンで環境探索
   b. 追加攻撃経路確認
8. [収集] ローカルシステムからのデータ (T1005)
   a. ローカルシステムからデータ収集
   b. 機密情報およびファイル確保
9. [流出] 代替プロトコルを介した流出 (T1048)
   a. 代替プロトコルを利用したデータ流出
   b. 検出回避のための転送経路設定
10. [影響] 影響のためのデータ暗号化 (T1486)
    a. ランサムウェアでデータ暗号化
    b. 金銭要求のためのデータアクセス遮断

5) SectorJ174は新しいドメインとソーシャルネットワークプラットフォームを使用しました (2025-03-30)

https://cti.nshc.net/events/view/13845

SectorJ174 グループは、オンライン上の特定の宣伝および情報拡散活動に対応することを目的として活動を開始し、匿名ベースのソーシャルネットワークプラットフォーム「Galaxy2」で仮名を使用して相互に接続されたユーザーから形成されました。その後、サイバー活動の拡大を通じて組織の構造が体系化されました。

このグループは人道的、宗教的、財政的な動機で他のハッキングキャンペーンも実行しました。彼らはソーシャルメディアやオンラインプラットフォームを運営に活用し、広報活動に関連する複数のドメインを保有していました。

該当グループは「ビットコイン寄付とクラウドファンディングを通じて資金を集め、新しいメンバーを募集し教育するプロジェクトを運営していた。様々な個人と以前のメンバーがこのグループと関連し、多様な作戦とハッキング活動を支援した。該当グループは運営方式と戦略的目標の違いにより内部で 2 つの派閥に分化したが、共通してウェブインフラの攪乱、データ露出防止、デジタル資産の非活性化を中心とした活動を継続した。また、一部の活動では人道的または社会的問題に基づくサイバー作戦も遂行され、これにより公開されたハッキングツールを修正したり、自動化されたスクリプトを活用して定期的な攻撃を行った事例が確認された。SectorJ174 グループは独自のドメインおよびオンラインチャンネルを運営し、作戦内容の公開、資金調達、新規参加者の募集など多方面でオンラインプラットフォームを積極的に活用した。ビットコイン寄付やクラウドファンディングを通じて資金を確保した状況があり、新規メンバーのための簡単な教育資料または参加ガイドラインを運営していたと見られる。様々な匿名の個人および過去の参加者がこのグループと連携し、多様なサイバー作戦および技術的支援活動に関与した事例も存在する。

攻撃の流れ

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
    a. フィッシングメール送信
    b. 悪意のあるリンクのクリック誘導
2. [実行] コマンドとスクリプトインタープリタ (T1059)
    a. スクリプトを通じたリモートコマンド実行
    b. マルウェア配布
3. [持続性] システムプロセスの作成または変更 (T1543)
    a. システムプロセスの作成
    b. プロセスの変更
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
    a. 脆弱性の活用
    b. 権限の昇格
5. [防御回避] ファイルまたは情報の難読化 (T1027)
    a. ファイルの難読化
    b. 情報の隠蔽

6. [資格情報アクセス] 資格情報ダンピング (T1003)
    a. 資格情報のダンプ
    b. ハッシュ値の抽出
7. [発見] システム情報の発見 (T1082)
    a. システム情報の収集
    b. 環境の探索
8. [横移動] リモートサービス (T1021)
    a. リモートサービスへのアクセス
    b. ネットワーク移動
9. [収集] ローカルシステムからのデータ (T1005)
    a. ローカルデータの収集
    b. ファイルの保存
10. [流出] C2チャネルを通じた流出 (T1041)
    a. C2チャネルを通じたデータ流出
    b. データの送信
11. [影響] データ破壊 (T1485)
    a. データの破壊
    b. ファイルの削除

6) SectorJ199はMicrosoft Management Consoleの脆弱性を悪用してマルウェアを配布しました (2025-03-28)

https://cti.nshc.net/events/view/13822

SectorJ199グループは、「MSC EvilTwin」ゼロデイ脆弱性（「CVE-2025-26633」）を悪用して攻撃対象システムに侵入し、データを窃取するサイバー脅威です。この攻撃は主に「プロビジョニングパッケージ」、署名された「.msiファイル」、「Windows MSCファイル」などを利用してマルウェアペイロードを配信します。「IntelliJ runnerw.exe」のような技術を利用してコマンドを実行します。また、「EncryptHub Stealer」亜種や「SilentPrism」、「DarkWisp」といったバックドアは持続性を維持し、データを窃取し、暗号化されたチャネルを通じてC&Cサーバーと通信し、分析回避戦略を使用します。この脅威アクターは「Living-off-the-Land Binaries」（「LOLBins」）と複雑な実行フローを通じて検出を回避し、攻撃対象の産業群や多様な部門をターゲットにして、動的なコマンド＆コントロール（Command and Control, C2）サーバー運営を通じて活発なインフラを活用します。このキャンペーンの複雑さは、多様なデータ窃取方法とペイロード配信メカニズムの適応性を通じて示されます。

攻撃の流れ

1. [初期アクセス] ドライブバイ妥協 (T1189)
   a. "MSC EvilTwin" 脆弱性の悪用
   b. "プロビジョニングパッケージ" および ".msiファイル" の配布
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. "IntelliJ runnerw.exe" を通じたコマンド実行
   b. "PowerShell" スクリプトの実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. "Windowsレジストリ" に自動実行項目を作成
   b. 予約タスクを通じた持続性維持
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. "Base64" エンコーディングを通じたデータ隠蔽
   b. "暗号化されたチャネル" を通じたC&C通信
5. [資格情報アクセス] OS資格情報ダンピング (T1003)
   a. "Wi-Fiパスワード" および "Windowsプロダクトキー" の抽出
   b. セッションデータの収集
6. [発見] システム情報の発見 (T1082)
   a. システムプロファイリング
   b. ネットワークアダプタおよび実行中のアプリケーション情報の収集
7. [収集] ローカルシステムからのデータ (T1005)
   a. 敏感なデータの収集
   b. ユーザーディレクトリからのファイル収集
8. [流出] C2チャネルを通じた流出 (T1041)
   a. "C&Cサーバー" へのデータ送信
   b. "HTTP" および "HTTPS" を通じた情報の窃取
9. [コマンドとコントロール] 暗号化されたチャネル (T1573)
   a. "AES" 暗号化チャネルの使用
   b. "C&Cサーバー" との持続的接続維持

7) SectorJ199はMicrosoft Windows Management Console (MMC)の脆弱性を悪用しました (2025-03-25)

https://cti.nshc.net/events/view/13752

SectorJ199グループが「Microsoft Management Console (MMC)」フレームワークのゼロデイ脆弱性「CVE-2025-26633」を利用してMalwareを実行するキャンペーンを発見しました。この攻撃は「MSC EvilTwin」技術を使用し、合法的な「.msc」ファイルを通じて悪意のある「.msc」ファイルを実行する方法です。該当グループは「MUIPath」を操作して検出されることなくペイロードを配

布および実行します。システムの言語機能を悪用し、合法的に見える「.msc」ファイルと共に悪意のあるバージョンを生成します。「MSC EvilTwin」ローダーはPowerShellで作成されており、悪意のあるペイロードをダウンロードして実行し、攻撃を初期化します。また、彼らは合法的なシステムパスに見える模擬ディレクトリを使用し、「MMC」に組み込まれた「ActiveX」コントロールを通じてコマンドを実行し、二次ペイロードをダウンロードします。このキャンペーンは持続性を維持し、機密情報を窃取することを目的としており、Microsoftの管理ツールに大きく依存する企業に影響を与えたと分析されています。

攻撃の流れ

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
    a. マルウェアが含まれたメールを送信
    b. ユーザーにダウンロードと実行を促す
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
    a. ユーザーが悪意のある ".msc" ファイルを実行
    b. "PowerShell" で "MSC EvilTwin" ローダーを実行
3. [持続性] ブートまたはログオン自動開始実行: レジストリ実行キー/スタートアップフォルダ (T1547.001)
    a. マルウェアファイルをスタートアップフォルダに保存
    b. システム再起動時に自動実行を設定
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
    a. ゼロデイ脆弱性を利用して権限を昇格
    b. "MUIPath" 操作で検出を回避
5. [防御回避] 偽装: 正当な名前または場所に一致 (T1036.005)
    a. 正当なパスに見える模擬ディレクトリを作成
    b. ファイル名およびパスを偽装
6. [資格情報アクセス] OS資格情報ダンピング (T1003)
    a. システム資格情報を収集
    b. メモリダンプを使用
7. [探索] システム情報探索 (T1082)
    a. システム構成情報を収集
    b. オペレーティングシステムのバージョンを探索
8. [横移動] リモートサービス: SMB/Windows管理共有 (T1021.002)
    a. ネットワーク共有を通じて移動
    b. リモートサービスを悪用
9. [収集] ローカルシステムからのデータ (T1005)
    a. ローカルシステムに保存されたデータを収集

b. 重要なファイルおよび文書をコピー

10. [流出] C2チャネルを介した流出 (T1041)
    a. 攻撃者のC&Cサーバーにデータを送信
    b. 暗号化されたチャネルを使用
11. [コマンド＆コントロール] アプリケーション層プロトコル: ウェブプロトコル (T1071.001)
    a. ウェブプロトコルを使用したC2サーバーとの通信
    b. HTTP/HTTPSを通じてコマンド受信およびデータ送信

8) SectorJ199はデータ窃盗とクリプトジャッキングのために悪性コードを使用しました（2025-04-03）

https://cti.nshc.net/events/view/14002

SectorJ199グループは2025年3月11日に、ロシアのフォーラムで「CVE-2025-26633」および「CVE-2025-24983」に関連するエクスプロイトを販売するために投稿しました。彼はキャンペーンの開発にChatGPTを広範囲に活用し、「Telegramボット」、「コマンド＆コントロール（C2）サーバー」、「フィッシングサイト」の構成が含まれていました。しかし、キャンペーンの実行過程でいくつかの重大なセキュリティミスが明らかになりました。主要アカウント全体でのパスワードの再利用、低いパスワードの複雑性、そして二要素認証の未適用により、資格情報に関するセキュリティが大きく脆弱でした。また、サーバーアクセスの制御が不十分で、重要なMalware構成ファイルが外部に露出し、これにより予期せずセキュリティコミュニティの調査を引き起こしました。Telegramベースのインフラの運用セキュリティも甘く、該当チャンネルを通じてグループの内部活動の一部が外部に露出し、これが一部の侵入につながったと見られます。彼らは一時的にホワイトハット活動への転換を検討したように見えましたが、ChatGPTとのインタラクション記録を分析した結果、セキュリティ業界の主要企業を対象とした攻撃シナリオの設計や、自身の公共イメージを再構築して合法的なサイバーセキュリティビジネスに偽装しようとする状況が共に捉えられました。これは潜在的に違法な目的を含んだ活動と見なされる可能性があります。

攻撃の流れ

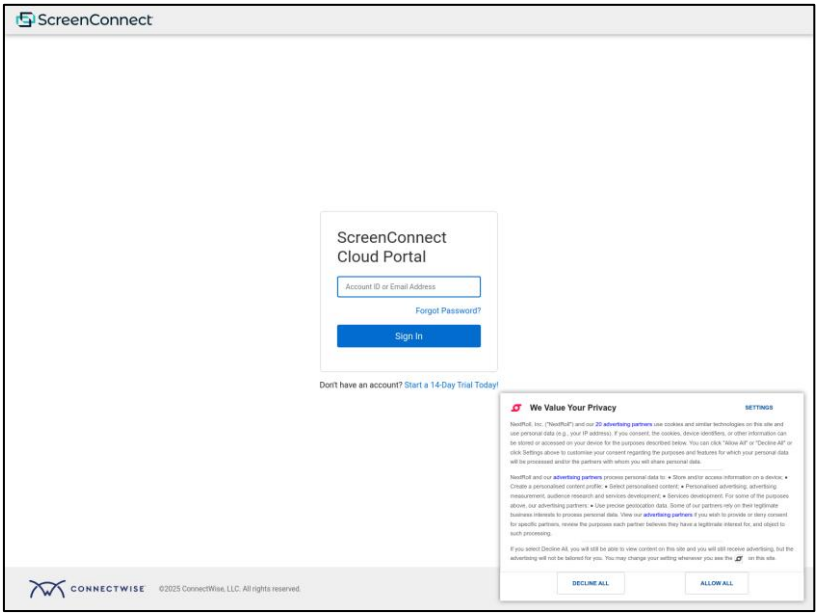
1. [初期アクセス] フィッシング (T1566)
    a. フィッシングサイトの作成
    b. "テレグラム" ボットで感染成功通知
2. [資格情報アクセス] パスワード推測 (T1110)
    a. パスワードの再利用
    b. 弱いパスワードの複雑性の使用
3. [コマンド＆コントロール] C2プロトコル (T1071)
    a. "C2サーバー" の構成

b. ディレクトリリスト化によるサーバー情報の露出
4. [防御回避] ツールの無効化または変更 (T1562)
a. 二要素認証の無効化
b. バックアップコードを .txt ファイルに保存
5. [探索] アカウント探索 (T1087)
a. アカウント資格情報の収集
b. 個人メールでサイバー犯罪アカウントを管理
6. [データ流出] 他のネットワーク媒体を介したデータ流出 (T1011)
a. 機密情報および設定ファイルの窃取
b. JSONファイルを通じてMalware構成の露出
7. [影響] データ破壊 (T1485)
a. 攻撃産業群に対する攻撃計画
b. セキュリティ大企業に対する攻撃的キャンペーンの準備

9) SectorJ209はQilinランサムウェアのためにフィッシングドメインを使用しました (2025-04-01)

https://cti.nshc.net/events/view/13926

SectorJ209グループは2025年1月、「Managed Service Provider」の管理者を対象に「スクリーンコネクト(ScreenConnect)」リモートモニタリングおよび管理ツールに関する偽の認証警告を利用したフィッシング攻撃を実施しました。この攻撃は管理者の資格情報を盗み、その後Qilinランサムウェアを配布することにつながりました。該当グループは「evilginx」中間者攻撃(Man-in-the-Middle, MitM)を使用して、実際の「スクリーンコネクト(ScreenConnect)」ドメインを模倣したフィッシングサイトを構築しました。フィッシング攻撃を通じて資格情報と多要素認証(MFA)トークンを傍受し、管理者権限で「スクリーンコネクト」ポータルに不正アクセスしました。彼らは新しいスクリーンコネクトインスタンス（「ru.msi」）を複数の顧客環境に配布し、「PsExec」や「WinRM」などの合法的なツールを使用して横方向の移動を行い、「Veeam」脆弱性(CVE-2023-27532)を悪用して機密データにアクセスしました。データは「WinRAR」を通じて「easyupload[.]io」に流出され、「インコグニート(Incognito)」モードを使用して防御を回避しました。Qilinランサムウェアはロシアでホスティングされたデータ流出サイトと接続されており、バックアップおよびイベントログを無効化して身代金の支払いを保証しました。



[図8: SectorJ209グループが利用したフィッシングサイト]

攻撃の流れ

1. [初期アクセス] フィッシング (T1566)
   a. "ScreenConnect" ログイン通知を装ったフィッシングメール
   b. フィッシングサイトへのマルウェアリダイレクト
2. [資格情報アクセス] 中間者攻撃 (T1557)
   a. "Evilginx"を使用した資格情報およびMFAトークンの傍受
   b. マルウェアドメインでのセッションクッキー収集
3. [持続性] システムプロセスの作成または変更 (T1543)
   a. "ru.msi"ファイルを使用した新しい"ScreenConnect"インスタンスの展開
   b. 顧客環境に攻撃者管理インスタンスをインストール
4. [横移動] リモートサービス (T1021)
   a. "PsExec"および"WinRM"を使用したリモートコマンド実行
   b. ネットワークおよびユーザーの探索
5. [データ流出] C2チャネル経由のデータ流出 (T1041)
   a. "WinRAR"を使用したデータ圧縮
   b. "easyupload[.]io"を通じたデータ流出
6. [影響] 影響を与えるためのデータ暗号化 (T1486)
   a. "Qilin"ランサムウェアの展開
   b. バックアップおよびイベントログの無効化

セクターJ210はCLFSの脆弱性を悪用してランサムウェアを配布しました（2025年4月8日）

https://cti.nshc.net/events/view/14131

攻撃対象産業群: 銀行、IT、小売、金融

SectorJ210グループは、「Windows Common Log File System (CLFS)」のゼロデイ（0-day）権限昇格脆弱性「CVE-2025-29824」を利用して、アメリカのITおよび不動産業界、ベネズエラの金融業界、スペインのソフトウェア会社、サウジアラビアの小売業界を対象に攻撃を行いました。該当グループは「PipeMagic」Malwareを通じてランサムウェアの配布を促進しました。初期アクセスは、改ざんされたウェブサイトから悪意のある「MSBuild」ファイルをダウンロードし、暗号化されたペイロードを配信する方法で行われました。その後、メモリ破損および「RtlSetAllBits」APIを使用して権限を昇格させ、「SYSTEM」プロセスにプロセスインジェクションを行い、「LSASS」メモリダンプを通じて資格情報を窃取しました。その結果、ランサムウェア活動が発生し、ファイルが暗号化され、身代金要求ノートがドロップされ、復旧を妨げるランサムウェアコマンドが実行されました。SectorJ210グループによって実行されたこのランサムウェアは、2つのオニオンドメインを使用し、独特な暗号化動作を示しました。この脆弱性は2025年4月8日のセキュリティアップデートで修正されました。

攻撃の流れ

1. [初期アクセス] ドライブバイ妥協 (T1189)
   a. 改ざんされたウェブサイトからマルウェア「MSBuild」ファイルをダウンロード
   b. 暗号化されたペイロードを送信
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. 「MSBuild」ファイルを実行
   b. 「EnumCalendarInfoA」APIを通じてペイロードを復号化および実行
3. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. メモリ内の「CLFS」脆弱性をエクスプロイト
   b. 「RtlSetAllBits」APIを使用してプロセストークンの権限を昇格
4. [資格情報アクセス] LSASSメモリ (T1003.001)
   a. 「procdump.exe」を使用した「LSASS」メモリのダンプ
   b. ダンプされた資格情報の収集
5. [防御回避] プロセスインジェクション (T1055)
   a. 「SYSTEM」プロセスにプロセスインジェクションを実行
   b. ランサムウェアペイロードを「winlogon.exe」にインジェクション
6. [影響] 影響のためのデータ暗号化 (T1486)
   a. ファイルを暗号化し、任意の拡張子を追加
   b. 身代金要求ノート !_READ_ME_REXX2_!.txt をドロップ
7. [影響] システム回復の抑制 (T1490)

a. 「bcdedit /set {default} recoveryenabled no」コマンドを実行
b. 「wbadmin delete catalog -quiet」および「wevtutil cl Application」を実行して回復を妨害

11) SectorJ211は公式メモに偽装したAmethyst Stealerを使用しました (2025-04-10)

https://cti.nshc.net/events/view/14162

攻撃対象産業群: エネルギー

SectorJ211グループが「Amethyst stealer」の更新版を使用してエネルギー産業を攻撃しました。彼らはフィッシングメールを通じてMalwareを配布し、HR担当者を装って公式メモに偽装した添付ファイルを送信します。メールには「Служебная записка .rar」という圧縮ファイルが含まれており、これはPDFアイコンに偽装された「Служебная записка .exe」実行ファイルを含んでいます。このファイルはC#ベースのMalwareで、.NET Reactorで保護され、.NETローダーとして動作します。Base64でエンコードされたPEファイルをデコードしてメモリにロードし、「Assembly.Load()」と「Invoke()」メソッドを使用して実行します。「Amethyst stealer」も.NET Reactorで保護されており、悪意のあるファイルをダウンロードし、システムが仮想化されているか確認した後、特定のURLにシステムデータを送信します。このスティーラーは高度な仮想化検査を特徴としており、文字列の暗号化にTriple DESアルゴリズムを使用します。さまざまなアプリケーションから資格情報やリモートデスクトップ、VPNクライアントのデータを抽出します。WMIを活用して広範なシステム情報を収集し、回避およびデータ抽出能力を強化します。

攻撃フロー

1. [初期アクセス] フィッシング (T1566)
   a. 人事担当者を装ったフィッシングメールの送信
   b. 公式メモに偽装した添付ファイルを含む
2. [実行] ユーザー実行 (T1204)
   a. PDFアイコンに偽装された実行ファイルの実行
   b. Base64でエンコードされたPEファイルをメモリ内にロード
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. .NET ReactorでMalwareを保護
   b. Triple DESで文字列を暗号化
4. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. 様々なブラウザとアプリケーションから資格情報を抽出
   b. リモートデスクトップおよびVPNクライアントの設定ファイルを収集
5. [探索] システム情報探索 (T1082)
   a. WMIを通じてシステム情報を収集
   b. 仮想化環境の検査

6. [データ流出] C2チャネル経由のデータ流出 (T1041)
    a. 特定のURLにシステムデータを送信
    b. IP確認および送信

12) SectorJ215は偽のポッドキャストを通じてマルウェアを配布しました (2025-03-24)

https://cti.nshc.net/events/view/14638

攻撃対象産業群: 金融、IT

SectorJ215グループは、高度なソーシャルエンジニアリング技術を活用して、暗号通貨ユーザーを対象としたサイバー脅威キャンペーンを実施しています。彼らは「Aureon Capital」というベンチャーキャピタル会社や「Aureon Press」、「The OnChain Podcast」などの関連団体を装い、信頼性を高めています。攻撃対象は主にTwitterのDMやメールを通じて「ポッドキャストインタビュー」という名目で最初に接触を受けます。このグループはZoom通話で画面共有を促し、その際にリモートアクセス制御を要求してユーザーの油断を突き、Malwareをインストールします。このMalwareは主に情報スティーラーやリモートアクセス型トロイの木馬（RAT）で、即時の機密情報漏洩や遅延したデータ抽出を可能にします。このような体系的なアプローチは、かなりの金銭的損失を引き起こしています。彼らは精巧なウェブサイトやソーシャルメディアプロフィールを構築し、有名人物を装って外見上の信頼性を維持する方法を使用しています。

攻撃の流れ

1. [偵察] 被害者の身元情報を収集 (T1589)
    a. TwitterのDMとメールを通じた初期接触
    b. 対象者にポッドキャストインタビューを提案
2. [リソース開発] アカウントの確立 (T1585)
    a. "Aureon Capital"および関連ウェブサイトの作成
    b. ソーシャルメディアプロファイルの設定と管理
3. [初期アクセス] サービスを介したスピアフィッシング (T1566.002)
    a. Zoomミーティングの招待
    b. ミーティングの詳細を最後の瞬間まで非公開
4. [実行] ユーザー実行 (T1204)
    a. 画面共有のリクエスト
    b. リモートアクセス制御のリクエスト
5. [持続性] 外部リモートサービス (T1133)
    a. マルウェアのインストールを通じたリモートアクセスの確保
6. [収集] 入力キャプチャ (T1056)
    a. 情報スティーラーのインストール

b. 機密情報の収集と流出

7. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. リモートアクセス型トロイの木馬を通じた持続的制御
   b. 遅延データ抽出の可能性を確保

13) SectorJ215はソーシャルエンジニアリングを利用してZoomのリモートコントロールを悪用しました (2025-04-17)

https://cti.nshc.net/events/view/14551

SectorJ215グループは、CEOを対象に「Bloomberg Crypto」メディアシリーズへの出演を促す詐欺招待を通じて、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。該当グループは2つの「Twitter」アカウントを使用して招待を提案し、非公式の「Calendly」ページを通じてスケジュール調整を操作しました。このキャンペーンは技術的なソフトウェアの脆弱性を利用せず、合法的な手続きを操作しました。主な攻撃ベクターは「Zoom」のリモート制御機能を悪用することで、この機能は参加者が他のユーザーのコンピュータを制御できるようにします。彼らは通常のシステム通知を装ってこの機能を悪用しました。このアプローチはユーザーのエラーとインターフェースの曖昧さに大きく依存し、ユーザーが定期的なプロンプトを承認する傾向を狙って、該当グループにマルウェアのインストール、データ抽出、暗号通貨の窃盗に広範なアクセスを許可しました。

攻撃フロー

1. [偵察] 情報を求めるフィッシング (T1598)
   a. 「Twitter」アカウントを通じてCEOに接触
   b. 「Calendly」ページを通じてスケジュールを操作
2. [初期アクセス] スピアフィッシングリンク (T1566.002)
   a. 偽の「Bloomberg Crypto」招待状を送信
   b. 詐欺的なスケジュール招待状を送信
3. [実行] ユーザー実行 (T1204)
   a. 「Zoom」リモート制御機能の要求
   b. システム通知に偽装してアクセス権を取得
4. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. マルウェアのインストール
   b. システム再起動時に自動実行設定
5. [資格情報アクセス] 入力キャプチャ (T1056)
   a. キー入力の監視
   b. 認証情報の窃取
6. [収集] 画面キャプチャ (T1113)

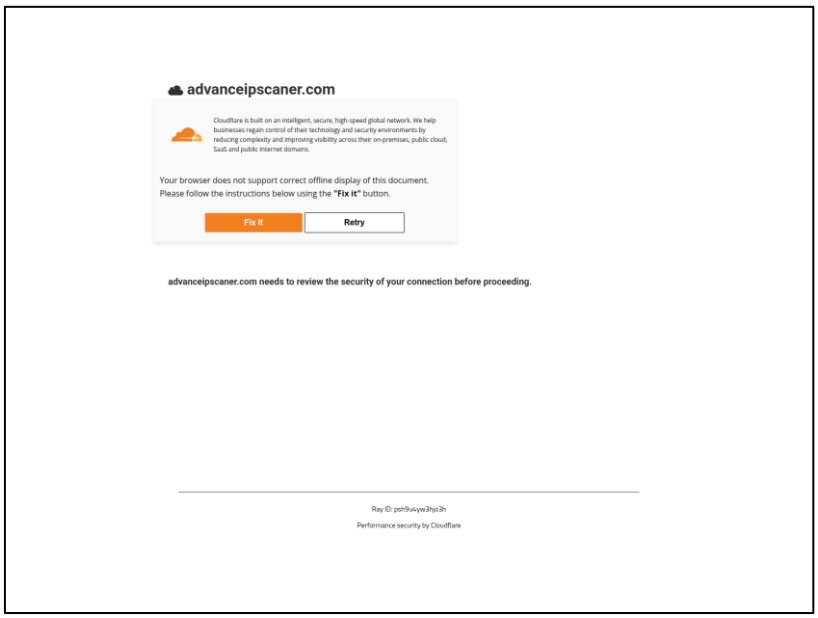
a. 画面キャプチャによる情報収集
b. 敏感情報のスクリーンショット保存
7. [流出] C2チャネルを介した流出 (T1041)
a. 収集されたデータをC2サーバーに送信
b. 暗号化されたチャネルを通じた情報流出
8. [影響] データ操作 (T1565)
a. データの改ざん
b. 暗号通貨取引の操作

14) SectorJ217はインターロックランサムウェアを使用しました (2025-04-16)

https://cti.nshc.net/events/view/14394

攻撃対象産業群: 健康、製造、政府・行政、技術

SectorJ217グループは2024年9月に初めて登場したランサムウェアグループで、「Big Game Hunting」および二重恐喝攻撃を行います。Interlockは従来の「Ransomware-as-a-Service」（RaaS）モデルではなく、「Worldwide Secrets Blog」というデータ漏洩サイトを運営し、被害者のデータを公開して交渉の場を提供します。彼らは他のランサムウェアグループに比べて被害者は少ないものの、北米とヨーロッパの様々な企業を攻撃対象としています。攻撃チェーンは合法的なウェブサイトを侵害することから始まり、これを通じてGoogle Chromeのような人気ソフトウェアに偽装した悪質なインストールファイルを配布します。これらの偽インストールファイルは、PowerShellバックドアを実行してLummaStealerやBerserkStealerのような資格情報窃取プログラムとカスタムリモートアクセス型トロイの木馬（RAT）を配布するために使用されます。2025年には「ClickFix」というソーシャルエンジニアリング戦術を利用して悪質なシステムプロンプトを生成し、これを通じてMalwareを実行しました。InterlockはRDPと資格情報窃取を通じた横方向の移動に重点を置き、マルチプラットフォームを対象とするランサムウェアを通じてWindowsとLinuxサーバーを攻撃します。このランサムウェアはAES暗号化を使用してファイルをロックし、暗号化されたメモを通じて身代金を要求します。グループの戦略は、継続的なデータ窃取と高度な難読化手法を活用することに重点を置いており、彼らの適応力と持続的な脅威を強調しています。



[図9: SectorJ217グループが利用したフィッシングサイト]

攻撃の流れ

1. [初期アクセス] ドライブバイ妥協 (T1189)
   a. 合法的なウェブサイトの損傷
   b. 偽のソフトウェアインストールファイルの配布
2. [実行] ユーザー実行 (T1204)
   a. PowerShellバックドアの実行
   b. LummaStealerおよびBerserkStealerの配布
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. レジストリキーの作成
   b. システム起動時の自動実行設定
4. [特権昇格] 特権昇格のためのエクスプロイト (T1068)
   a. 管理者権限の取得試行
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 難読化されたコマンドの使用
   b. Malwareペイロードの暗号化
6. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. 資格情報奪取ツールの使用
   b. キーロギング活動
7. [探索] システム情報探索 (T1082)
   a. システム情報の収集
   b. ネットワーク構成情報の取得
8. [横移動] リモートサービス (T1021)

a. RDPを通じた横移動
b. 奪取した資格情報の使用
9. [収集] ローカルシステムからのデータ (T1005)
a. ローカルシステムからのデータ収集
10. [流出] C2チャネルを介した流出 (T1041)
a. C2サーバーへのデータ送信
b. 暗号化されたチャネルの使用
11. [影響] 影響のためのデータ暗号化 (T1486)
a. ファイルのAES暗号化によるロック
b. 身代金要求メモの作成および配布

15) SectorJ220はTelegramを通じてスミッシングキットを販売しました (2025-04-10)

https://cti.nshc.net/events/view/14197

攻撃対象産業群: 金融、物流、政府・行政、通信、運送、小売

SectorJ220 グループは、さまざまな産業の組織を対象に大規模な SMS フィッシングキャンペーンを実施するサイバー犯罪グループです。彼らは、121 か国にわたって郵便、物流、通信、輸送、金融、小売、公共部門などの産業を攻撃対象としています。このグループは 20 日間で 100 万件を超えるページ訪問を生成し、同時に 25,000 のアクティブドメインを使用しています。毎日約 100,000 件のメッセージを送信し、2025 年 3 月 18 日には「Lighthouse」という新しいフィッシングキットを Telegram チャンネルを通じて発表しました。このキットは、西側諸国、オーストラリア、アジア太平洋地域の主要な金融組織をターゲットにしています。Telegram を通じて他の脅威行為者に販売され、300 人以上の世界中のフロントデスクスタッフが詐欺活動を支援していると主張しています。フィッシングサイトは主に「Tencent」と「Alibaba」の脆弱なサーバー構成を利用しており、さまざまなサーバー設定が発見され、複数のハッキンググループが類似の技術を使用していることが示されています。これらの情報は、グループのグローバルな範囲と技術的な洗練さを強調しています。

[図 10: SectorJ220グループが利用したフィッシングサイト]

攻撃フロー

1. [偵察] 被害者情報の収集 (T1592)
   a. 121か国の産業組織情報の収集
   b. 攻撃対象産業別情報の収集
2. [リソース開発] アカウントの確立 (T1585)
   a. テレグラムチャンネルおよびアカウントの作成
   b. フィッシングキット「Lighthouse」の開発と配布
3. [初期アクセス] フィッシング: スピアフィッシングリンク (T1566.002)
   a. SMSを通じたフィッシングリンクの送信
   b. フィッシングサイトへの誘導
4. [実行] ユーザー実行: 悪意のあるリンク (T1204.001)
   a. ユーザーがフィッシングリンクをクリック
   b. フィッシングサイトへのアクセス
5. [資格情報アクセス] アプリケーションアクセス トークンの盗難 (T1528)
   a. フィッシングサイトを通じたアカウント情報の窃取
   b. 金融情報などの機密データの取得
6. [コマンド＆コントロール] 非アプリケーション層プロトコル (T1095)
   a. C2サーバーへのフィッシングデータの送信
   b. フィッシングキャンペーンの管理と操作
7. [データの流出] データをクラウドアカウントに転送 (T1537)
   a. 窃取データのクラウドへの転送
   b. ドメインローテーションを通じた継続的なデータ転送

8. [影響] データ破壊 (T1485)
   a. 収集されたデータの破棄命令
   b. 記録の削除およびデータの削除

16) SectorJ72はC2インフラストラクチャに新しいTLDドメインを使用しました (2025-03-25)

https://cti.nshc.net/events/view/13739

攻撃対象産業群: 教育、金融、ガス、政府・行政、製造、石油、小売、技術、通信、輸送

SectorJ72 グループは 2024 年に、新しい「ローカル権限昇格」エクスプロイトを公開前に利用して攻撃対象システムにアクセスしました。これはエクスプロイトディーラーとのつながりを示唆しており、同グループが高度なエクスプロイトを使用するサイバー犯罪グループであることを示しています。彼らは QNAP および IoT デバイスを標的にして、コマンド＆コントロール（Command and Control,
C2）サーバーネットワークを構築しました。他の脅威グループがトラフィックを隠すために「オペレーショナルリレーボックス（Operational Relay
Box）」ネットワークを使用するのとは異なり、彼らは C2 インフラのためにエクスプロイトを購入または作成します。彼らの活動は「ファストフラックス（Fast
Flux）」技術と低評価のトップレベルドメイン（TLD）を使用したドメイン登録で観察され、IP アドレスとドメインを回転させて運用の隠密性を強化しました。トーア（Tor）ネットワークとオニオン（Onion）ドメインを使用して感染したデバイスと安全に通信しました。彼らは初期アクセスブローカーとして活動し、彼らのネットワークを他の悪意のある活動に提供しています。

攻撃の流れ

1. [初期アクセス] 脆弱性の悪用 (T1190)
   a. 「ローカル権限昇格」エクスプロイトの使用
   b. QNAP および IoT デバイスへの攻撃
2. [実行] コマンド＆コントロール (T1105)
   a. C2 ネットワークの構築
   b. 「ファストフラックス」技術の使用
3. [持続性] 外部リモートサービス (T1133)
   a. Tor ネットワークを通じた通信
   b. 「.onion」ドメインの使用
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. IP アドレスおよびドメインの回転
   b. 評判の低い TLD の使用
5. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)

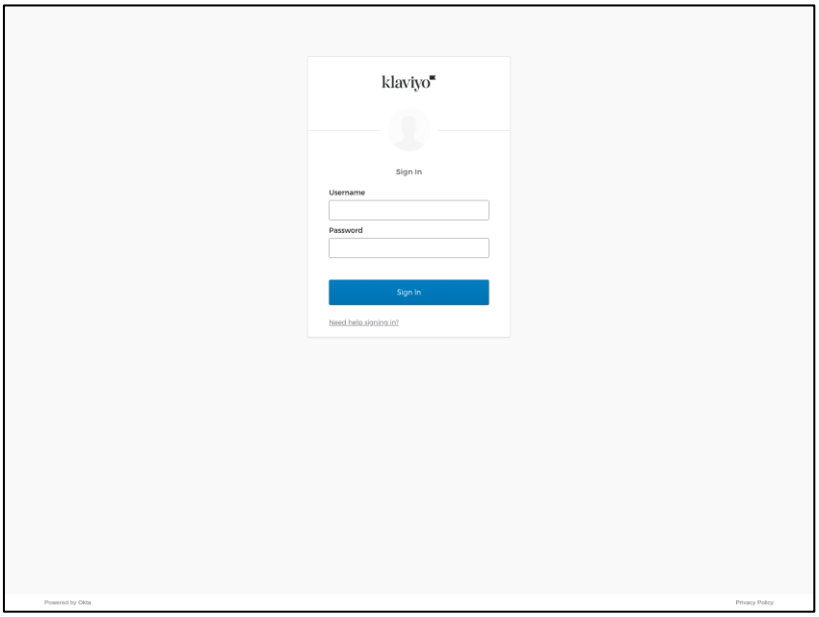
a. クラウドネットワークサーバーの使用
b. VPS およびサードパーティネットワークを通じた通信
6. [資格情報アクセス] ブルートフォース (T1110)
a. エクスプロイトディーラーとの接続
b. 初期アクセスブローカーとしての役割の遂行

17) SectorJ85は、ログインページに偽装したフィッシングドメインとRATマルウェアを使用しました（2025-04-08）

https://cti.nshc.net/events/view/14145

攻撃対象産業群: 金融、娯楽、小売、IT、通信

SectorJ85 グループは 2022 年から活動しているハッキンググループで、主要なサービスやブランドを対象に高度なソーシャルエンジニアリングおよびフィッシング攻撃を行ってきました。このグループは「Klaviyo」、「HubSpot」、「Pure Storage」、「Audemars Piguet」、「Twitter/X」などの複数の主要な攻撃対象を狙い、ログイン資格情報および多要素認証（MFA）トークンを取得するための精巧な方法を使用しました。彼らは複数のフィッシングキットを配布しており、これらのキットはコードおよび技術配布戦略を含めてかなり進化しています。2024 年には、このグループが「Twitter/X」が以前に所有していたドメインを取得し、それを攻撃に利用する可能性が指摘されました。このグループが使用した「Spectre RAT」の新しいバージョンは、侵害されたシステムに持続的なアクセスを維持する能力を示し、データの窃取やコマンド実行といった機能を提供します。2024 年から 2025 年にかけて、このグループは「BitLaunch」のようなサービスを活用し、「Cloudflare」のようなプラットフォームに配布してインフラを調整しました。



[Figure 11: SectorJ85 グループが利用したフィッシングサイト]

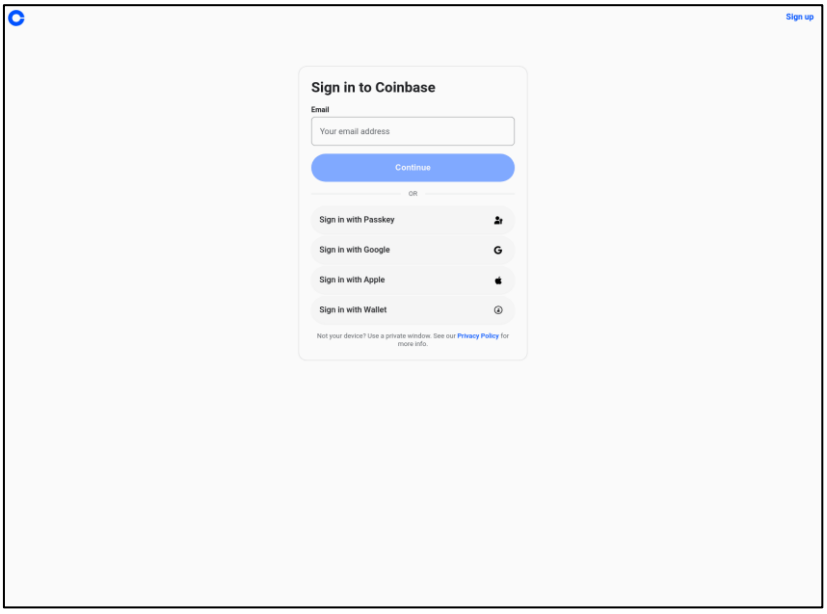
攻撃の流れ

1. [初期アクセス] フィッシング (T1566)
   a. フィッシングメール送信
   b. フィッシングページ作成
2. [実行] ユーザー実行 (T1204)
   a. ユーザークリック誘導
   b. マルウェア実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. 自動開始位置にマルウェア設置
   b. 持続的アクセス維持のための設定
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. コード難読化
   b. 高度なクライプター使用
5. [資格情報アクセス] 入力キャプチャ (T1056)
   a. ログイン資格情報収集
   b. MFA トークン奪取
6. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. HTTP プロトコル使用
   b. C2 サーバーとの通信設定
7. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. 収集されたデータを C2 サーバーへ送信
   b. コマンド実行結果送信
8. [影響] データ破壊 (T1485)
   a. データ暗号化
   b. データ削除または改ざん
9. [探索] システム情報探索 (T1082)
   a. システム情報収集
   b. ネットワーク構成探索

18) SectorJ85は、偽のCloudflare Turnstileを特徴とするフィッシングドメインを使用しました (2025-03-28)

https://cti.nshc.net/events/view/13882

SectorJ85 グループは最近のフィッシングキャンペーンで、新規登録されたドメインを利用して信頼できるサービスであるメールプロバイダーやクラウドプラットフォームを装いました。彼らは巧妙に操作されたフィッシングメールを通じて攻撃対象を主に狙い、一般的なトップレベルドメインと国別ドメインを活用して合法的なサービスを装い、ユーザーを欺いて資格情報を盗もうとしました。該当グループは DNS 偵察と登録ピボットを利用して強力なインフラを構築し、非標準設定のホスティングサービスを使用し、さまざまなファビコンハッシュを適用して検出を回避しました。これらのドメインはほとんどがサポートやログインポータルに偽装されており、主に「NICENIC」を通じて登録され、「Tucows」や「Web Commerce Communications」といった他の登録機関を通じても登録されました。これは高度な戦略を示しています。フィッシングの餌は主に暗号通貨、金融、モバイルサービスといったテーマを活用し、過去の類似キャンペーンとの関連性を示しています。これらの技術により、該当グループは迅速に資格情報を収集し、対象サービスの API を悪用して敏感なデータを効率的に流出させる自動化された後続作業を可能にしました。



[図 12: SectorJ85 グループが利用したフィッシングサイト]

攻撃の流れ

1. [偵察] DNS 偵察
   a. DNS 情報収集
   b. 新規ドメイン探索
2. [リソース開発] ドメイン登録
   a. NICENIC およびその他の登録機関の使用
   b. フィッシングに適したドメイン選択
3. [配信] フィッシングメール

a. メールプロバイダーおよびクラウドプラットフォームのなりすまし
b. 精巧なフィッシングメールの送信

4. [防御回避] 難読化
   a. 非標準ホスティング設定
   b. 多様なファビコンハッシュの活用
5. [資格情報アクセス] 資格情報収集
   a. ログインポータルに偽装したページの使用
   b. ユーザー資格情報の窃取
6. [収集] 自動データエクスポート
   a. API 悪用によるデータ抽出
   b. 敏感情報の効率的収集

今月のサイバー脅威の特徴

最近検出された一連のサイバー攻撃は、技術的な精巧さと社会工学的な巧妙さが組み合わさった高リスクレベルの作戦様相を示しています。該当キャンペーンで使用されたマルウェアと戦術・技法・手順（TTPs）を分析すると、ハッキンググループが様々な産業をターゲットにして体系的な戦略の下で攻撃を実行していることがわかります。特に、今回の攻撃は既存の防御システムを回避しつつ、ユーザーの心理的な弱点を巧みに狙う形で展開されており、これを通じて高度に隠密で持続的な侵入を達成しようとする意図が明確に現れています。

まず、マルウェアの観点から見ると、ハッキンググループはビーバーテイル（BeaverTail）、インビジブルフェレット（InvisibleFerret）といったカスタムマルウェアペイロードを戦略的に配置しました。これらのマルウェアはそれぞれ多様な機能を備えており、資格情報の窃取、システム情報の収集、コマンド＆コントロール（C2）サーバーとの通信、さらに追加ペイロードのダウンロード機能などを含んでいます。特に注目すべき点は、RSA 公開鍵に基づく暗号化技術が適用されていることで、これによりネットワークトラフィックの分析や静的分析で悪意のある行為を識別することが難しくなり、検出を効果的に回避します。一部のマルウェアは Golang 言語で作成されており、クロスプラットフォーム環境に対応し、アンチウイルス回避および難読化技術が併用されています。

攻撃ベクターも様々なソーシャルエンジニアリング手法と組み合わされて活用されました。最も顕著なベクターは、偽の採用メールとインタビュウェブサイトを利用したアプローチで、特に技術産業や暗号通貨、防衛産業の従事者を主要なターゲットとしました。メールは実際の企業を装ったり、採用担当者のプロフィールを偽造した形で作成され、リンクを通じてアクセスを誘導した後、マルウェアが挿入されたテストファイルまたはインストールパッケージをユーザーにダウンロードさせるように

誘導します。また、開発者コミュニティを中心とした侵入も試みられ、ハッキンググループは有名なツールやライブラリを提供するふりをしながらマルウェアプロジェクトを配布し、コードレビューやコラボレーションの依頼を通じて被害者との信頼を構築した後、ペイロードを実行する方法でアプローチしました。

感染経路においては、BitBucket のような正当なコードホスティングプラットフォームが利用された点が特徴です。ハッキンググループは、マルウェアを特定のプロジェクトの圧縮ファイル形式でアップロードし、これを採用テストファイルやソフトウェアリソースに偽装して配布しました。また、一部のケースでは、実行時にユーザーに管理者権限を要求する方法で、悪性ペイロードの権限昇格を誘導しました。この過程で、バックグラウンドでシステム情報を収集し、C2 サーバーから追加の命令を受信して二次感染やラテラルムーブメントを試みる行為が観察されました。

ハッキンググループの TTPs の観点から見ると、全体的に「ソーシャルエンジニアリングに基づくアプローチ–正当な行為の偽装–検出回避–
持続的侵入」という一連の流れが巧妙に設計されています。攻撃対象が自発的にマルウェアを実行するよう誘導したり、Windows の正規プロセスおよびツール（mshta、regsvr32 など）を悪用する Living off the
Land（LotL）技法が頻繁に活用され、これにより検出を最小限に抑えつつ権限を拡張する戦略が展開されました。一部の攻撃では、ポンプ・アンド・ダンプ（Pump and
Dump）といった金融詐欺手法が併用され、暗号通貨を対象とした市場の混乱や資産の奪取を目的としたものと分析されています。

今回のキャンペーンは、単なる侵入を超えて、業界別のカスタマイズされた脅威戦略が実際に適用されていることを示す代表的な事例です。ハッキンググループは、技術的多様性と戦術的精巧さを武器に、対象組織の防御システムを回避し、長期的な情報収集および資産の窃取を試みました。これに伴い、今後の類似脅威に備えるためには、マルウェアの特性分析、ソーシャルエンジニアリングベクターの識別、TTP に基づく検出ロジックの開発など、多角的なアプローチが必要であり、脅威インテリジェンスの共有と対応システムの高度化が不可欠です。

今月のサイバー脅威の示唆点

最近発生したサイバー攻撃は、組織全体のセキュリティ体制に複雑かつ重大な示唆を与えています。今回の攻撃は単なる技術的侵害を超えた、多層的で精巧に設計された複合攻撃の形態を持っていました。特にハッキンググループは、伝統的なセキュリティ境界を回避し、人間の心理を巧妙に利用するソーシャルエンジニアリング技法と共に、高度な資格情報の窃取手法、検出を回避するファイルレスおよびメモリベースの攻撃技法を複合的に活用しました。これは、従来のシグネチャベースまたは境界防御中心のセキュリティ戦略だけでは、組織を効果的に保護することが難しいことを如実に示して

います。技術的対応だけでは限界が明らかであり、人間中心のセキュリティガバナンスと政策的強化が切実に求められる時期です。

まず、メンバーに対するセキュリティ意識の向上は、技術的な対策と同じくらい重要な要素と見なされるべきです。今日発生するほとんどの侵害事故は、ユーザーのミス、不注意、またはソーシャルエンジニアリング技術によって引き起こされており、これは単純なメールフィルタリングや警告メッセージでは解決が難しいです。したがって、定期的なセキュリティ教育と実習に基づくトレーニングが並行して行われるべきであり、特にフィッシングメールや疑わしいリンクへの対応を超えて、メンバーが自ら脅威を認識し積極的に対応できるように促す参加型の教育方法が求められます。トレーニング時には、現実的なシナリオに基づく模擬攻撃を含め、セキュリティ感受性を体得させるアプローチが効果的です。

また、認証システムの根本的な再整備が不可欠です。ハッキンググループは依然として資格情報の窃取を通じて組織内の機密情報や上位アカウントへのアクセスを試み続けており、単一認証方式（Single Factor
Authentication）はこのような攻撃に非常に脆弱な構造です。したがって、マルチファクター認証（MFA）の全社的な導入はもはや選択ではなく必須です。特に高リスクアカウントや主要な管理者権限を持つユーザーの場合、生体認証、ワンタイムパスワード（OTP）、ハードウェアベースのトークンなど、さまざまな認証要素を組み合わせ、ユーザー行動分析による異常兆候の検出およびリアルタイム対応システムを連携させることが望ましいです。

技術的にも、従来のシグネチャベースのセキュリティソリューションだけでは、ハッキンググループの進化した攻撃を検出するのは難しいです。最近使用されているファイルレスマルウェアや Living off the
Land（LoL）手法は、オペレーティングシステムの正当な機能を悪用することで、検出回避を最大化しています。これらの脅威に効果的に対応するためには、行動ベースの検出技術、メモリフォレンジック分析、EDR（Endpoint Detection and
Response）ソリューションの活用が必須です。特に EDR は、リアルタイムの脅威の可視性と侵害指標を提供できるため、自動化された対応体制と組み合わせることで、攻撃の識別から対応までの時間を画期的に短縮することができます。

脆弱性管理体制も再度点検すべき要素です。ハッキンググループは依然として既知の脆弱性を悪用して組織内部に侵入する戦略を好んで使用しており、これはパッチ適用の遅延や脆弱性管理の不備につながる場合、致命的な結果を招くことがあります。したがって、セキュリティパッチを迅速かつ体系的に適用できる政策の策定が必要であり、資産ベースのリスク分析を通じてどのシステムにどの脆弱性が存在するのかを明確に把握し、パッチの優先順位を設定するアプローチが求められます。さらに、自動化されたパッチ配布システムを通じて脆弱性の露出時間を最小化することが効果的です。

最後に、外部の脅威インテリジェンスとの連携は、ハッキンググループの戦術変化に能動的に対応するための重要な戦略です。最新の脅威動向やハッキンググループの TTPs（戦術、技術、手順）をリアルタイムで把握し、それを内部防御システムに反映する先制的なセキュリティが必要です。特に、

類似産業内の他組織との脅威情報の共有は、攻撃シナリオを早期に識別し、共同で対応するのに大いに役立ちます。これにより、組織の回復力を高め、長期的な観点からサイバーレジリエンスを確保することができます。

総合的に見ると、今回の攻撃は断片的な防御戦略ではなく、人、技術、政策が有機的に統合された全方位的なセキュリティ体制の必要性を強調しています。ハッキンググループの高度化した攻撃に効果的に対応するためには、先制的かつ適応可能なセキュリティ戦略が求められ、これは最終的に戦略的思考に基づいた強力なセキュリティガバナンス体制の確立につながるべきです。

Recommendation

NSHC ThreatRecon チームは様々な目的のハッキンググループ(Threat Actor Group) 活動を分析し、組織内部のセキュリティチームがハッキング活動における被害をさらに減らせるように共通的に確認できる攻撃技術(technique)における MITRE ATT&CK の脅威緩和(Mitigations)項目を次のようにまとめた。

1. 脆弱性保護 (Exploit Protection)

ソフトウェアのエクスプロイト(Exploit)発生を誘導したり、発生の可能性を探知及びブロックするために脆弱性保護(Exploit Protection)のソリューション使用の検討が必要

- エクスプロイト(Exploit)の動作の緩和のため、 WDEG(Windows Defender Exploit Guard)及び EMET(Enhanced Mitigation Experience Toolkit)の使用の検討が必要
- エクスプロイトのトラフィックがアプリケーションに辿り着くことを防止するため、Web アプリケーションのファイアウォール使用の検討が必要

2. 脆弱性のスキャニング (Vulnerability Scanning)

外部に漏出したシステムの脆弱性を定期的に検査し、致命的な脆弱性が見つかった場合、速やかにシステムをパッチする手続きの検討が必要

- 潜在的に 脆弱なシステムを新たに識別するため、定期的な内部ネットワークの検査の検討が必要
- 公開となった脆弱性における持続的なモニタリングの検討が必要
- 実際のハッキンググループ(Threat Actor Group)が使用した脆弱性におけるセキュリティ強化案件の検討が必要
- このレポートの“Appendix”には実際の 実際のハッキンググループ(Threat Actor Group)が使用した履歴がある脆弱性の情報が含まれている

3. セキュリティ認識教育 (User Training)

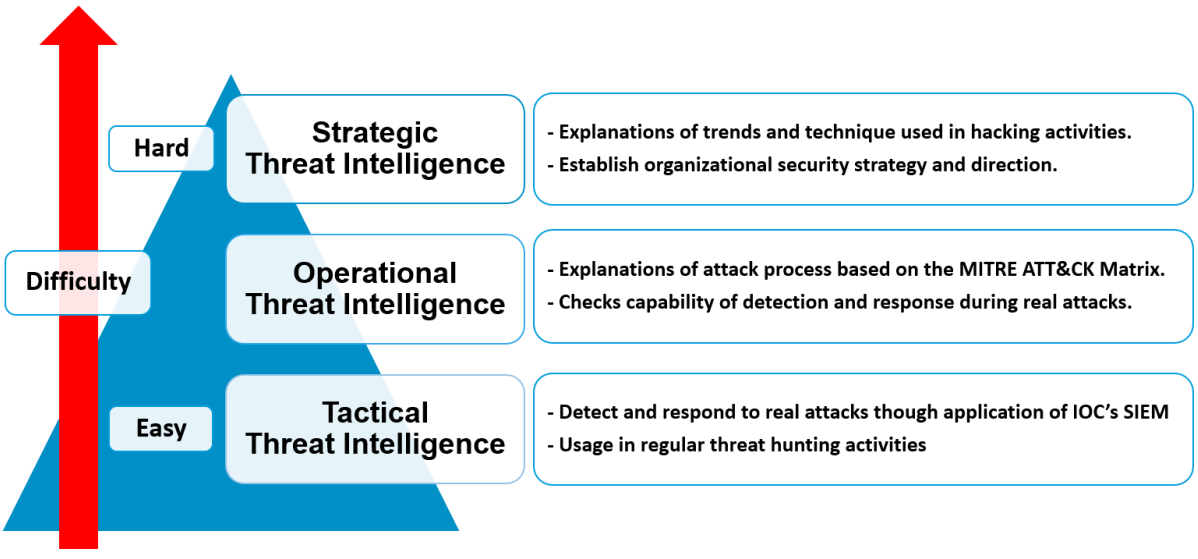
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

- ソーシャルエンジニアリング(Social Engineering)技法とスピアフィッシング(Spear Phishing)E-Mail を識別できる教育の検討が必要

- ユーザーと管理者が多数のアカウントに同一なパスワードを使用しないように資格証明情報の管理の重要性における教育の検討が必要
- システムに保存したパスワードの危険性における教育の検討が必要
- リポジトリにデータを保存する時に注意すべきの事項における教育の検討が必要
- ブラウザの悪性の拡張プログラムが実行されないようにブラウザ管理における教育の検討が必要
- SMS、通話履歴、連絡先リストなどの敏感な情報のアクセス権限を要請する Android アプリケーションについて注意喚起できるような教育の検討が必要
- 非公式ページからアプリケーションをダウンロードしないように教育の検討が必要

4. 脅威インテリジェンスプログラム(Threat Intelligence Program)

ハッキンググループが使用しているマルウェアハッシュ(Hash)、IP 及びドメイン(Domain)情報を含む IOC(Indicator of Compromise)が見つかった場合、通知を送信するように探知の設定の検討が必要



- IPS、IDS 及びファイアウォールのようなネットワークセキュリティ装備のログから IOC と同一な通信 IP が見つかった場合
- 組織内部の DNS サーバー、ウェブゲートウェイ(Web Gateway)及びプロキシ(Proxy)ウェブ関係のシステムのログから IOC と同一なドメインが見つかった場合
- EDR(Endpoint Detection and Response)のようなエンドポイントセキュリティソリューションのログから PC 及びサーバーから IOC と同一なファイルハッシュ(Hash)が存在する場合

- 組織内部の様々なシステムのログを収集する SIEM(Security Information Event Management)から設定したユーズケース(Use Case)とルール(Rule)に IOC と同一なファイルハッシュ、IP 及びドメインが存在する場合*

5. ネットワークにおける脅威緩和

1) ネットワーク侵入防止 (Network Intrusion Prevention)

組織のネットワークにアクセスする悪意的なトラフィックを事前にブロックするために侵入探知システム(Intrusion Detection System, IDS)及び侵入防止システム(Intrusion Prevention System, IPS)の使用の検討が必要

- ネットワークレベルからハッキンググループの攻撃活動を緩和するため AitM(Adversary in the Middle)のトラフィックパターンが識別できる侵入探知システム(Intrusion Detection System, IDS)及び 侵入防止システム(Intrusion Prevention System, IPS)の使用の検討が必要
- マルウェアが組織の内部ネットワークにアクセスしたり実行したりすることを防止するため、ホスト型の侵入防止システム(HIPS, Host Intrusion Prevention System)、アンチウイルス(Anti-Virus)などのソリューションの使用の検討が必要

2) ネットワーク細分化 (Network Segmentation)

組織の重要なシステム及び資産を隔離するため、ネットワークを物理的及び論理的ネットワークで分割し、セキュリティコントロール及びサービスがそれぞれの下位のネットワークごとに提供できるようにネットワーク細分化(Network Segmentation)の使用の検討が必要

- DMZ(Demilitarized Zone)及び別のホスティングインフラを使用して外部/内部ネットワークを分離する政策の使用の検討が必要
- ハッキンググループのターゲットになりやすい組織の重要なシステム及び資産を識別し、無断アクセス及び変造から該当のシステムを隔離し、保護する政策の使用の検討が必要
- ネットワークのファイアウォールの構成から必要なポートとトラフィック以外は通信できないようにブロックする政策の検討が必要
- ネットワークプロキシ、ゲートワイ及びファイアウォールを使用して内部システムにおける直接的な遠隔アクセスを拒否する政策の使用の検討が必要
- 侵入の探知、分析及び対応システムは別のネットワークから運営するように検討が必要

6. ユーザーアカウントの脅威緩和

1) 多要素認証 (Multi-factor Authentication)

組織の資産にアクセスできるパスワードが漏洩された場合＝にもハッキンググループがアクセスすることを防止するため、複数の段階で認証段階を構成する多要素認証(MFA, Multi-Factor Authentication)の使用の検討が必要

2) アカウント使用政策 (Account Use Policies)

アカウントのセキュリティ設定に関した政策設定の検討が必要

- 企業の内部から業務用として活用している Windows PC のログインユーザーアカウントのパスワードを英語のアルファベットの大文字、小文字及び記号を含んでなるべく 8 桁以上で設定するように検討が必要
- Windows のアクティブディレクトリ(Active Directory)として構成された環境では、グループ政策(Group Policy)通じて企業の内部ネットワークに繋がる Windows PC のゆーあーアカウントのパスワードを英語のアルファベットの大文字、小文字及び記号を含んでなるべく 8 桁以上で設定するように構成し、3 か月ごとにパスワードが変更されるように政策使用の検討が必要
- 承認済みではないデバイスもしくは外部の IP からログインを防ぐよう、条件付きアクセス政策使用の検討が必要
- パスワードが推測されることを防ぐため、いくつかの回数のログイン失敗のあと、アカウントを凍結する政策使用の検討が必要

3) 特権アカウント管理 (Privileged Account Management)

アカウント資格証明によるリスクを最少化するため、管理者のアカウント及び権限が割り当てられた一般アカウントに関しての管理の検討が必要

- リモートデスクトッププロトコル(Remote Desktop Protocol, RDP)を通じてログインできるグループリストからローカル管理者(Administrators)グループを取り除くことについて検討が必要
- 管理者のアカウント及び権限が割り当てられた一般のアカウントの間、資格証明の重複防止のための政策の検討が必要
- 低い権限レベルのユーザーが高いレベルのサービスを作ったり、実行できないように権限設定の検討が必要
- 資格証明の悪用による影響を最少化するため、サービスアカウントにおける権限の制限する政策の検討が必要

7. エンドポイントの脅威緩和

1) ソフトウェアアップデート(Update Software)

エンドポイント(Endpoint)及びサーバーの OS とソフトウェアが最新バージョンでアップデートされているか確認が必要であり、特に外部に漏出されたシステム及供給網の公的に繋がる恐れがあるファイルの配布システム(Deployment Systems)における定期的なアップデートの検討が必要

2) OSの構成 (Operating System Configuration)

ハッキンググループの晒された技術における被害を緩和するため、OS の構成の検討が必要

- NTLM(New-Technology LAN Manager)ユーザー認証プロトコル、Wdigest 認証無効化の検討が必要
- 業務及び運営に不要な場合、リムーバブルメディアを許容せず、制限する政策の検討が必要
- 署名済みではないドライバーがインストールされないよう、制限する政策の検討が必要

3) アプリケーション確認及びサンドボックス(Application Isolation and Sandboxing)

すでにハッキンググループが奪取した権限及び資格証明を通じてほかのプロセス及びシステムにアクセスすることを制限するため、アプリケーション隔離及びサンドボックスの使用の検討が必要

4) 実行防止 (Execution Prevention)

システムからマルウェアの実行を防ぐため、実行ファイル及びスクリプト実行のコントロールの検討が必要

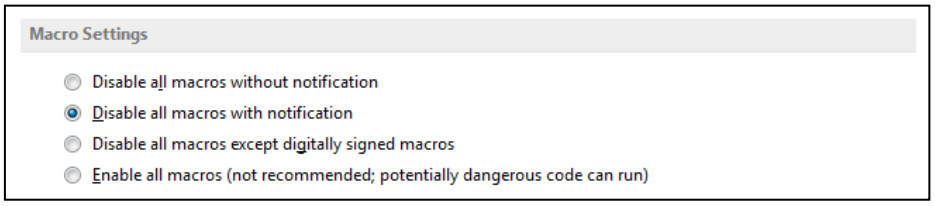
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

5) 機能の無効化及びプログラムの削除 (Disable or Remove Feature or

Program)

攻撃者の濫用を事前に防ぐため、潜在的に脅威となる恐れがある機能の無効化及びプログラムの削除の検討が必要

- Windows のシステムにインストールされている MS Office のセキュリティ設定の中、「マクロ設定」を「すべてのマクロを表示しない(通知表示)」の基本設定を変更できなくして、アクティブディレクトリ(Active Directory)から GPO Group Policy Object)の設定の上、配布する検討が必要



- DCOM(Distributed Component Object Model)の無効化の検討が必要
- 特定のシステムから MSHTA.exe が起動しないように検討が必要
- WinRM(Windows Remote Management)サービスの無効化の検討が必要
- 不要な自動実行機能の無効化の検討が必要
- ローカルパソコンのセキュリティ設定及びグループ政策から LLMNR(Link-Local Multicast Name Resolution)及びネットバイオス(NetBIOS)の無効化の検討が必要
- ローカルパソコンのセキュリティ設定及びグループ政策から LLMNR(Link-Local Multicast Name Resolution)及びネットバイオス(NetBIOS)の無効化の検討が必要
- PHP の eval()のようなウェブ技術の特定した関数を無効化する検討が必要

6) コード署名 (Code Signing)

信頼できないファイルの実行を防ぐため、コード署名情報を確認する政策設定の検討が必要

- 署名済みではないスクリプトの実行を防ぐパワーシェル(PowerShell)の政策設定の検討が必要
- 署名済みではないファイルの実行を防ぐ政策設定の検討が必要
- 署名済みではないサービスドライバーの登録及び実行を防ぐ政策設定の検討が必要

7) アンチウイルス (Antivirus)

マルウェアのダウンロード及び実行を通じたサイバー脅威を防止するため、これを探知しつつブロックできるアンチウイルス(Antivirus)の使用の検討が必要

- マルウェアのダウンロード及び実行の対応のため、ホスト型侵入防止システム(HIPS, Host Intrusion Prevention System)及びアンチウイルス(Anti Virus)などのソリューション使用の検討が必要

8) エンドポイントからの行為を防止 (Behavior Prevention on Endpoint)

エンドポイント(EndPoint)から潜在的な脅威になりやすい悪性行為が発生しないよう、事前に防止するために行為防止(Behavior Prevention)機能使用の検討が必要

- 信頼できないファイルの実行を防止するため、ASR(Attack Surface Reduction)ルールの有効化の検討が必要
- ファイルの署名が一致しないなど、潜在的な脅威になりやすいファイルを識別及び探知できるエンドポイント(EndPoint)ソリューション使用の検討が必要
- プロセスインジェクション(Process Injection)のような攻撃技術を探知及びブロックするため、行為防止(Behavior Prevention)機能使用の検討が必要

9) ハードウェア設置の制限 (Limit Hardware Installation)

USB デバイス及びリムーバブルメディアを含む承認済みではないハードウェアの使用を制限したり、ブロックしたりする政策を検討

- ¥承認済みではないハードウェアの使用を制限したり、ブロックするようにエンドポイントのセキュリティ構成及びモニタリングエージェントの使用の検討が必要

10) 企業モバイル政策 (Enterprise Policy)

モバイルデバイスの動作をコントロールするための政策設定のため、 EMM(Enterprise Mobility Management)/MDM(Mobile Device Management)システムの使用の検討が必要

- Android デバイスの業務文書及び内部システムのアクセスは制限付きの業務領域のみでアクセスできるように政策設定の検討が必要
- iOS からエンタープライズ配布用証明書で署名し、App Store ではないほかの手段から伝わってきた悪性アプリケーションをユーザーがインストールできないよう、プロフィールの制限設定の検討が必要

LEGAL DISCLAIMER

NSHC (NSHC Pte. Ltd.) takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuations. NSHC Research services are limited publications containing valuable market information provided to a selected group of customers. Our customers acknowledge, when ordering or downloading our publications

NSHC Research Services are for customers' internal use and not for general publication or disclosure to third parties. No part of this Research Service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, contact us. **service@nshc.net**

This document contains information that is the intellectual property of NSHC Inc. and Red Alert team only. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of NSHC. Nothing in this document constitutes a guaranty, warranty, or license, expressed or implied.

NSHC.

NSHC disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of NSHC.