NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI2025080602

# 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


**Jul 2025**

NSHC PTE. LTD.

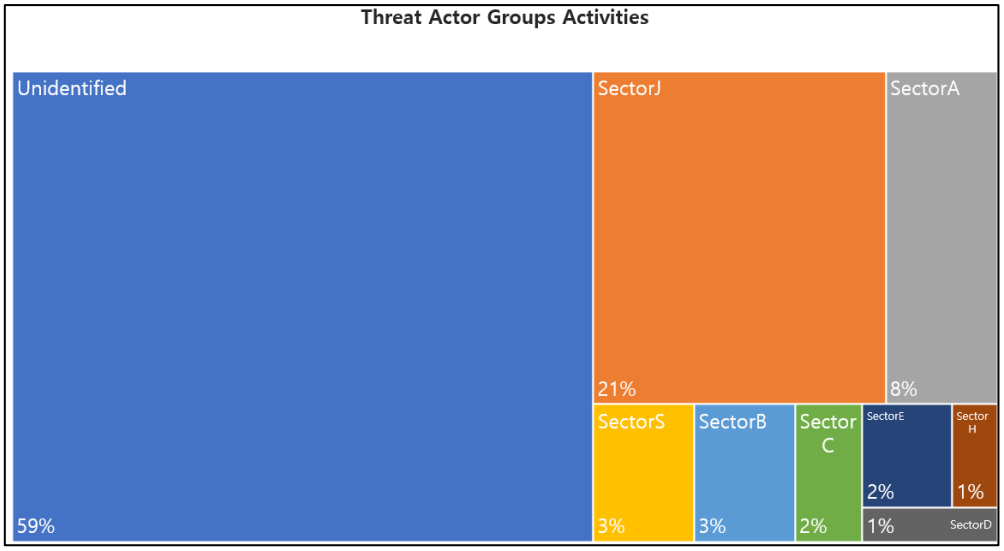
このレポートは 2025 年 6 月 21 日から 2025 年 7 月 20 日まで見つけた政府支援のハッキンググループ活動と関係あるイッシューを説明し、それに伴う侵害事故の情報と ThreatRecon Platform 内のイベント情報を含む。

## Table of Contents

## エグゼクティブサマリー

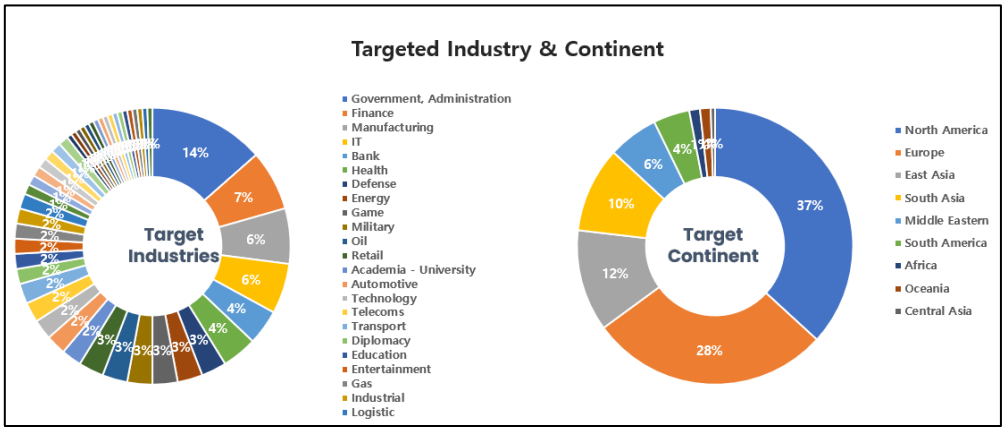
2025 年 6 月 21 日から 2025 年 7 月 20 日までの間に NSHC 脅威分析研究所（Threat Research Lab）が収集したデータと情報に基づいて分析したハッキンググループ（Threat Actor Group）の活動を要約した内容です。

今月 7 月には、合計 71 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 59%で最も多く、次いで SectorJ、SectorA グループの活動が続きました。




[図 1: 2025 年 7 月に確認されたハッキンググループ別活動統計]

今年 7 月に発見されたハッキンググループの活動は、政府機関や金融業界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。




[図 2: 2025 年 7 月に攻撃対象となった産業分野と国の統計]

SectorA グループは、開発者エコシステムを中心としたソフトウェアサプライチェーンへの侵入活動を集中的に行いました。正規のパッケージ名に似たスペルを偽装する手法を利用し、オープンソースパッケージマネージャー（npm）を通じてマルウェアローダーを配布し、これを基に段階的な情報窃取やバックドアのインストールを誘導しました。ローダーは難読化されたコマンドと条件付きロジックを通じて検出を回避し、システム情報や資格情報、暗号通貨ウォレットデータを収集する機能を含んでいます。また、フィッシングメールを通じて ClickOnce プロンプト、マルウェア LNK ファイル、画像に偽装した添付ファイルなどを利用した様々な初期侵入試行を並行して行い、GitHub やクラウドストレージをコマンド＆コントロールインフラとして活用し、識別を困難にする戦略を継続しています。一部のキャンペーンでは、Android デバイスを含むクロスプラットフォームベースのマルウェアが確認され、ユーザー行動誘導に基づく攻撃展開方式が全般的に強化されています。

SectorB グループは、多数の公開された高リスク脆弱性を迅速に悪用し、グローバルインフラを標的に侵入作戦を実行しました。SAP NetWeaver と Ivanti 機器の未パッチ脆弱性を利用してウェブシェルを配布し、ルートキットをインストールしてシステム内部への持続的なアクセス基盤を確保しました。また、ウイルス対策ソフトウェアの DLL サイドローディング脆弱性を利用したバックドアのロードや、地政学的な問題を利用したフィッシングメールを通じてユーザー基盤システムに侵入する事例も確認されました。各攻撃はカスタム暗号化アルゴリズム、難読化された命令、API ハッシングなどの高度な技術を伴い、一部のキャンペーンでは Beacon ベースのコマンド＆コントロール通信を通じてリアルタイム操作が可能なように構成されました。資格情報の窃取、システムコマンドの実行、ラテラルムーブメントが主要な戦術として観測されており、持続的なインフラの更新を通じて識別回避能力も強化されています。

SectorC グループは、東ヨーロッパおよび政府機関を標的に偵察および情報収集作戦を実施しました。マクロ文書、マルウェアスクリプト、偽装された LNK ファイルなどを含むメールベースの侵入手法を活用し、ユーザーの手動実行を誘導した後、スケジュールされたタスク、サービス登録、COM ハイジャックなどを通じて持続性を確保します。マルウェアは、システム情報、Office 文書、ブラウザ履歴などの収集機能を含み、収集された情報は暗号化されてコマンド＆コントロールサーバーに送信されます。コマンド＆コントロールインフラは、Dropbox、Telegram、Koofr、Icedrive などの正規サービスを基盤として構成され、検出を回避し、一部のキャンペーンでは Cloudflare Tunnel および fast-flux DNS まで組み合わされた形態も確認されています。マルウェアは、Python、PowerShell、AppleScript、Nim などのさまざまな言語で開発され、プラットフォームごとの攻撃環境に柔軟に対応することが特徴です。

SectorD グループは、中東およびイスラエル地域を中心に高度な社会工学に基づくフィッシングキャンペーンを展開しました。Havoc フレームワークに基づくバックドア、React ベースのフィッシングキット、精巧に操作されたマルウェア PDF などが連携した多段階攻撃方式が確認され、サイバーセキュリティ企業や政府関係者を装ったメッセージを通じて攻撃対象に接近しました。資格情報と 2 段階認証情報を窃取すると同時に、リアルタイムのキー入力送信を通じて攻撃者のバックエンドシス

テムに情報を収集する手法が適用されました。Linux および Windows 環境の両方をサポートする多様なペイロードが併用され、マルウェアの実行はファイルレス方式、逆解析手法、コマンド暗号化などを通じて検出可能性を最小化します。全体として、緊急度と信頼を操作した精巧な社会工学と技術的侵入が複合的に結合した様相を示しています。

SectorE グループは、外交、国防、NGO 分野の機関を対象に精巧な諜報活動を行いました。マルウェアは、正常な文書やアプリケーションに偽装された圧縮ファイルに含まれて配布され、実行時に予約タスクを生成したり、ユーザーアカウント権限で悪意のあるプロセスをインストールして持続性を確保します。収集対象は、システムユーザー情報、文書ファイル、ネットワーク環境などであり、これを HTTPS ベースのコマンド＆コントロールサーバーに暗号化して送信します。マルウェアは、文字列エンコーディング、API の動的ロード、仮想環境の回避などの分析妨害機能を含み、一部のキャンペーンではユーザーの相互作用なしに自動実行される形態も確認されています。初期侵入には Google ドライブのリンクや偽の会議招待メールが使用され、このグループは政治的に敏感な機関を長期的なターゲットとしていると見られます。

SectorH グループは、南アジアおよびインド内の防衛産業組織を中心に情報窃取を目的としたフィッシングキャンペーンを実施しました。メールには悪意のある PDF または Linux 環境の.desktop ファイルが添付されており、ユーザーがこれを実行すると、偽装されたドキュメントファイルと共に悪意のあるバイナリが実行される仕組みです。ペイロードには、システム情報の収集、スクリーンショットのキャプチャ、キーロギング機能などが含まれ、被害システムにはバックグラウンド実行、アイコン偽装、可視性の除去などの隠蔽技術が適用されます。コマンド＆コントロール通信は指定された悪意のあるドメインを通じて行われ、分析の結果、インド政府機関で使用されるオペレーティングシステム環境を特定ターゲットとしたカスタマイズ設計が確認されました。キャンペーンの展開方式は、技術的侵入とソーシャルエンジニアリングが複合された形態で、国家単位の戦略的目的が内包された脅威と評価されます。

SectorS グループは、ラテンアメリカ地域を中心に金融機関および公共インフラを対象としたフィッシングベースの侵入キャンペーンを実施しました。攻撃者は巧妙に構成されたフィッシングページを通じてユーザーの資格情報を盗み、初期感染には VBS、PowerShell、HTML スクリプトベースのペイロードを使用しました。感染後には、Remcos や AsyncRAT などのリモートアクセス型トロイの木馬を配布し、持続的な制御を試みました。また、WebDAV プロトコルを悪用した脆弱性ベースの侵入事例も確認され、ユーザーの操作なしにマルウェアをインストールする手法が含まれていました。コマンド＆コントロール通信は動的 DNS と非標準ポートを活用して運営され、短期間で廃棄されるインフラを通じて識別を回避しています。このグループは、迅速な配布と機敏なインフラ運営を通じて短期利益の最大化を追求する典型的なサイバー犯罪の行動を示しています。

SectorJ グループは、多様な偽装戦術とソーシャルエンジニアリング技法を組み合わせて、フィッシングを基盤とした侵入およびランサムウェアの配布活動を行いました。求職申請書、企業会議案内、採用問い合わせなどに偽装したフィッシングメールを通じて、ユーザーをクラウドストレージ基盤のランディングページに誘導し、これを通じてマルウェアの実行ファイルやスクリプトを配布しました

。一部のキャンペーンでは、ソーシャルメディアアカウントを侵害して信頼基盤を操作したり、偽のスタートアップウェブサイトを構築してユーザーにマルウェアをインストールさせたりしました。技術的には、Reflective Loading、View State 逆シリアル化、SYSTEM 権限昇格、証明書偽造、ルートキット基盤の持続性確保などの高度な侵入技術が観測され、ELF 基盤のランサムウェアおよびクロスプラットフォーム情報窃取ツールの使用も確認されています。収益目的の脅威であるにもかかわらず、高度化された戦術を活用する点が特徴です。

## 詳細情報

### 1. APT（Advanced Persistent Threat）ハッキンググループの活動

**1) SectorA01 used HexEval Loader disguised as npm packages (2025-06-24)**

https://cti.nshc.net/events/view/16393

攻撃対象産業群: 開発

北朝鮮の脅威アクターに関連するサイバー脅威キャンペーンは、サプライチェーン攻撃で Malware を配信するために npm パッケージを活用しています。この作戦は、24 のアカウントを通じて配布された 35 の悪意のある npm パッケージを含み、そのうち 6 つは依然としてアクティブで、ダウンロード数が 4,000 回を超えています。この攻撃は、ホストデータを収集し、北朝鮮の攻撃者に関連する 2 段階の情報窃取 Malware である BeaverTail を配布する 16 進数でエンコードされた HexEval ローダーを活用します。これにより、3 段階のバックドアである InvisibleFerret をさらにロードします。この作戦で使用される高度な手法は、静的分析と手動レビューを回避し、持続性を維持するために階層的な制御とプロセス注入を活用します。脅威アクターは LinkedIn でリクルーターを装い、求職者に悪意のあるコーディング課題を送り、彼らを操ってコンテナ化された環境外で Malware を実行するよう誘導します。注目すべき技術には、人気のある npm プロジェクトのタイプオスクワッティング（Typosquatting）があります。
クワッティング)とエンコードされた C2 エンドポイント通信の活用が含まれています。このキャンペーンは、特定の条件に応じてペイロードの配信を動的に変更できる能力を示しており、検出を困難にし、この脅威の進化する巧妙さを強調しています。

**[Attack Flow]**

1. [初期アクセス] フィッシング (T1566)
   a. LinkedIn でリクルーターを装う
   b. 求職者にマルウェアのコーディング課題を送信
2. [実行] ユーザー実行 (T1204.002)

a. 求職者がマルウェアを実行
b. コンテナ化された環境外でのコード実行を誘導
3. [持続性] イベントトリガー実行 (T1546.016)
a. HexEval ローダーを通じた持続性維持
b. プロセス注入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 (T1027.013)
a. 16 進数でエンコードされたスクリプトを使用
b. C2 エンドポイント通信のエンコード
5. [資格情報アクセス] 入力キャプチャ (T1056.001)
a. キーロギングによる入力キャプチャ
6. [探索] システム情報探索 (T1082)
a. ホストメタデータの収集
b. 環境変数およびシステム情報の収集
7. [収集] 自動化された収集 (T1119)
a. ローカルファイルシステムからのデータ収集
8. [コマンド＆コントロール] ツール転送の侵入 (T1105)
a. BeaverTail および InvisibleFerret マルウェアのロード
b. C2 サーバーからのペイロード受信
9. [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流出
b. 条件付きロジックを通じたペイロード配信の最適化

**2) SectorA01 used XORIndex Loader in npm Supply Chain Attack (2025-07-14)**

https://cti.nshc.net/events/view/16932

攻撃対象産業群: 開発

最近のサイバー脅威事件には、北朝鮮の脅威行為者が npm エコシステムを通じてソフトウェアサプライチェーン攻撃を行い、67 個の損傷したパッケージを通じてマルウェアを配布することが含まれています。そのうち 27 個は依然としてアクティブな状態です。これらのパッケージには、新たに識別された XORIndex ローダーと以前から知られている HexEval ローダーが含まれています。両方のローダーはホストのリモート情報を収集し、2 段階のマルウェアである BeaverTail を取得します。これは InvisibleFerret バックドアを参照します。XORIndex ローダーは XOR エンコードされた文字列とインデックスベースの難読化を使用して検出を回避し、BeaverTail は暗号通貨ウォレットディレクトリとブラウザ拡張機能を対象に、ハードコーディングされたコマンド＆コントロール（C2）エンドポイントにデータを流出させます。このキャンペーンは、暗号通貨または機密性の高い資格情報にアクセスする可能性のある開発者や個人を対象としています。Vercel のような合法的なプラッ

トフォームを C2 運用に活用し、脅威行為者は低い運用プロファイルを維持し、検出を回避するためにこれらのローダーを改良された難読化技術で継続的に繰り返します。攻撃は 2025 年 4 月から 7 月まで行われ、17,000 回以上のダウンロードを記録し、持続的で進化する脅威を示しています。

**[Attack Flow]**

1. [初期アクセス] サプライチェーンの妥協 (T1195.002)
   a. npm パッケージ 67 個の損傷
   b. HexEval および XORIndex ローダーを含む
2. [実行] コマンドおよびスクリプトインタープリタ: JavaScript (T1059.007)
   a. JavaScript コードの実行
   b. BeaverTail ローダーの実行
3. [防御回避] 難読化されたファイルまたは情報: 暗号化/エンコードされたファイル (T1027.013)
   a. XOR エンコードされた文字列の使用
   b. インデックスベースの難読化の適用
4. [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. ブラウザ拡張プログラムデータの収集
   b. 暗号通貨ウォレットディレクトリのターゲット
5. [収集] 自動収集 (T1119)
   a. システム情報の収集
   b. ホストのリモート情報の収集
6. [流出] C2 チャネルを介した流出 (T1041)
   a. ハードコーディングされた C2 エンドポイントへのデータ流出
   b. BeaverTail を通じたデータ転送
7. [影響] 金融窃盗 (T1657)
   a. 暗号通貨ウォレット情報の窃取
   b. 敏感な資格情報へのアクセス

### 3) SectorA03 used XSS Exploit for ClickOnce Phishing Emails (2025-06-23)

https://cti.nshc.net/events/view/16388

脅威グループがフィッシングキャンペーンに ClickOnce 技術を活用したサイバー脅威事件が発生しました。このグループはフィッシング成功率を高めるために、ウェブメールプラットフォームの XSS ゼロデイ脆弱性を悪用しました。被害者がフィッシングメールを開くと、ブラウザは自動的にメール更新を模倣した ClickOnce プロンプトをトリガーしました。攻撃チェーンはフィッシングメールから始まり、悪意のあるアプリケーションの配布とマルウェアの実行へと続きました。トロイの

木馬ファイルである csrss32.exe は、追加の悪意のある DLL をシステムに復号してロードしました。予約されたタスクは svchost.exe にプロセスインジェクションを通じて追加のマルウェアを実行し、コマンド＆コントロールサーバーwhocanis[.com と通信するためにシェルコードを実行できるようにエントリポイントを修正しました。マルウェアはシステム情報を収集し、サーバーと通信し、暗号化されたデータをローカルに保存しました。この事件は、脅威グループが Windows と Android プラットフォームの両方でゼロデイ脆弱性に集中していることを示しています。

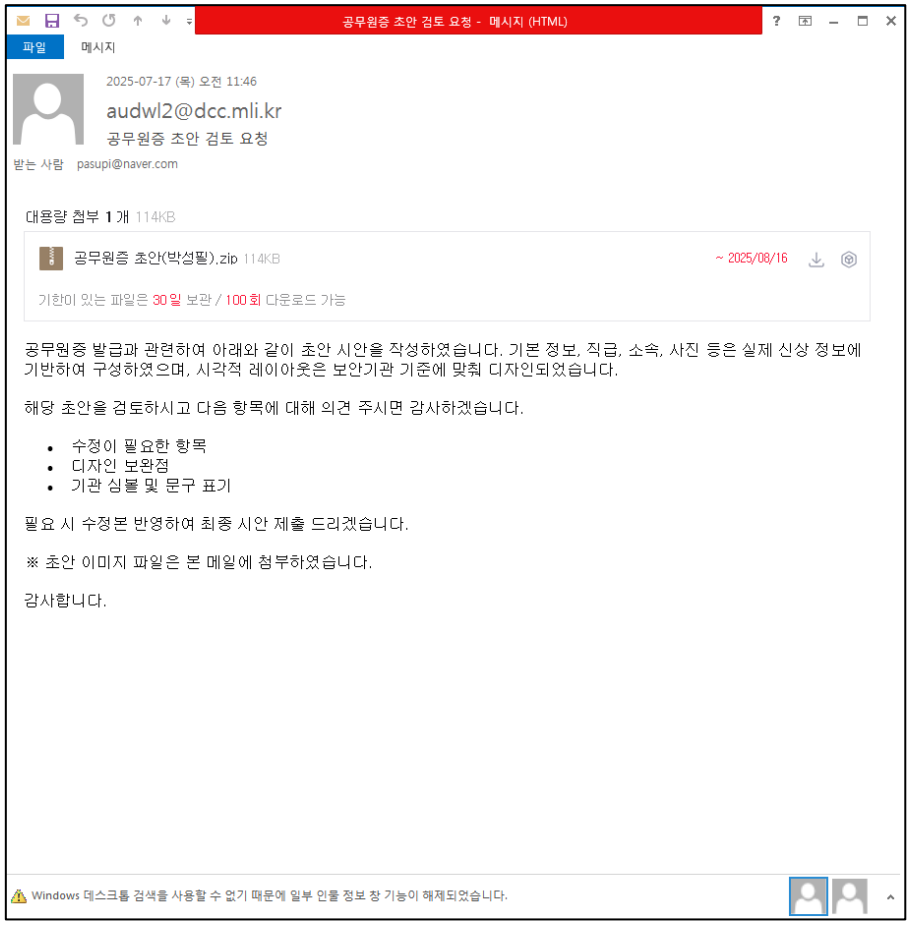
**[Attack Flow]**

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. Web メールプラットフォームの XSS ゼロデイ脆弱性の悪用
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. ClickOnce プロンプトでメール更新を模倣
   b. 悪意のあるアプリケーション実行
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. rundll32 を使用して cgfadb.pos の CreateObject 関数を実行
4. [権限昇格] プロセスインジェクション (T1055)
   a. explorer.exe プロセスの探索と権限昇格
   b. CreateRemoteThread を使用した explorer.exe へのスレッドインジェクション
5. [防御回避] プロセスインジェクション (T1055)
   a. svchost.exe にシェルコードをインジェクション
   b. svchost.exe のエントリーポイントを修正
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. whocanis[.com とソケット接続
   b. システム情報を収集し、暗号化後に送信
7. [収集] ローカルシステムからのデータ (T1005)
   a. システム情報を収集
   b. 暗号化されたデータをローカルに保存
8. [流出] C2 チャネルを介した流出 (T1041)
   a. 収集された情報を whocanis[.com に送信
   b. C2 サーバーからデータを受信し、復号化

**4) SectorA05 used AI-generated Image to Spread LNK Malware (2025-07-18)**

https://cti.nshc.net/events/view/17037

最近のサイバー攻撃では、生成型 AI で作成された画像を利用してマルウェアを拡散しており、ユーザーの特別な注意が求められています。このフィッシング攻撃は「公務員証草案のレビュー依頼」という件名のメールを通じて広まり、ユーザーが添付ファイルを確認するよう誘導します。添付ファイルは大容量ファイルで、ZIP アーカイブ内に画像アイコンに偽装された LNK ファイルを含んでいます。LNK ファイルをクリックすると、cmd.exe を通じて難読化されたコマンドが実行されます。復号化されたコマンドは PowerShell を使用して%TEMP%フォルダにおとりの PNG 画像をダウンロードして表示します。また、LhUdPC3G.bat ファイルがダウンロードされ、密かに実行され、7 秒間遅延してサンドボックス検出を回避する可能性があります。その後、curl を利用して CAB ファイルをダウンロードし、解凍して%ALLUSERSPROFILE%¥HncAutoUpdate に 2 つのファイルを生成します。アップデートに偽装した EXE ファイルは持続性を保証します。この設定は攻撃者の C2 サーバーと通信し、システム情報を収集し、追加のマルウェアをダウンロードします。この事件は AI 生成コンテンツで強化された社会工学的攻撃の巧妙さを強調しています。



[図 3: SectorA05 グループが送信したフィッシングメール]

**[Attack Flow]**

1. [初期アクセス] フィッシング (T1566)
   a. '公務員証草案の検討依頼'メール送信

b. 添付された LNK ファイルのクリック誘導
2. [実行] コマンドとスクリプトインタープリタ (T1059)
a. cmd.exe を通じて難読化されたコマンドを実行
b. PowerShell でおとりの PNG 画像をダウンロードおよび表示
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. LNK ファイルの画像アイコンに偽装
b. LhUdPC3G.bat ファイルを密かに実行
4. [防御回避] 実行ガードレール (T1480)
a. LhUdPC3G.bat ファイルを 7 秒遅延実行
5. [防御回避] 偽装 (T1036)
a. アップデートに偽装した EXE ファイルを作成
6. [持続性] スケジュールされたタスク/ジョブ (T1053)
a. HncAutoUpdateTaskMachine スケジューラを登録
7. [コマンドと制御] アプリケーション層プロトコル (T1071)
a. C2 サーバーと通信してシステム情報を収集および送信
8. [収集] ローカルシステムからのデータ (T1005)
a. 感染 PC のシステム情報を収集
9. [流出] C2 チャネルを介した流出 (T1041)
a. 収集されたシステム情報を送信
10. [影響] システム回復の抑制 (T1490)
a. 元の圧縮ファイルを削除して痕跡を除去

**5) SectorA05 used GitHub to distribute Malware with spearphishing (2025-06-22)**
https://cti.nshc.net/events/view/16328

高度なスピアフィッシング攻撃が検出され、GitHub が XenoRAT マルウェアの亜種を配布するための攻撃インフラとして使用されました。この作戦は 2025 年 3 月に開始され、特定の個人を対象に韓国の法律事務所を装ったメールを通じて攻撃が行われました。攻撃者はハードコーディングされた GitHub 個人アクセストークン（PAT）を使用して、マルウェア、餌ファイル、被害者情報を含む個人リポジトリにアクセスしました。初期のマルウェアは、攻撃目的で修正された RTF ファイルを Dropbox からダウンロードし、ファイルレス方式で PowerShell スクリプトを通じて実行されました。その後、ペイロードは GitHub で同じトークンを活用して収集された被害者データを流出させるために使用されました。キャンペーン中に作成されたリポジトリは、特定の被害者に合わせた餌ファイルを使用し、負債返済、委任状、暗号通貨シードフレーズなどのドキュメントテーマを活用しました。

**[Attack Flow]**

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. 韓国の法律事務所を装ったメール送信
   b. 添付ファイルに悪意のある RTF ファイルを含む
2. [実行] コマンドとスクリプトインタープリター: PowerShell (T1059.001)
   a. PowerShell スクリプトを通じたファイルレス実行
   b. Dropbox から Malware をダウンロードして実行
3. [持続性] スケジュールされたタスク/ジョブ: スケジュールされたタスク (T1053.005)
   a. タスクスケジューラに悪意のあるスクリプトを登録
   b. 30 分間隔でスクリプトを実行
4. [防御回避] 難読化されたファイルまたは情報: コマンド難読化 (T1027.010)
   a. PowerShell コマンドの難読化
   b. Malware 文字列の暗号化
5. [収集] 入力キャプチャ: キーロギング (T1056.001)
   a. キーロギングを通じた入力情報の収集
   b. 実行中のプロセスおよびウェブページのタイトルを記録
6. [データ流出] ウェブサービスを介した流出: コードリポジトリへの流出 (T1567.001)
   a. GitHub リポジトリを通じたデータ流出
   b. ハードコーディングされた PAT を使用したアクセス
7. [コマンド＆コントロール] ウェブサービス (T1102)
   a. GitHub と Dropbox を通じた C2 通信
   b. 非標準ポートを通じたデータ転送

### 6) SectorA05 used LNK Malware disguised as Bandizip Installer (2025-07-08)

https://cti.nshc.net/events/view/16747

攻撃対象産業群: 政府・行政、シンクタンク、高等教育

精巧なサイバー脅威事件は、韓国の機関を標的にして、マルウェアペイロードを偽の Bandizip インストールパッケージに偽装しました。このキャンペーンは諜報および情報窃取を目的としており、難読化されたマルウェアスクリプトをリモートでロードして HappyDoor トロイの木馬を配布しました。攻撃はフィッシングを通じて開始され、偽の Bandizip インストーラーは合法的なプログラムを実行するかのように見せかけながら、秘密裏に複数のマルウェアスクリプトをダウンロードし、VMProtect で難読化されたペイロードを配信しました。ペイロードは DLL ファイルで構成され、regsvr32 を通じて登録・実行され、mshta を使用してリモート VBScript をロードすることで、ユーザーおよびシステム情報を窃取し、隠しファイルやスケジュールされたタスクを生成して検出を回避しました。さらに、DLL はキーロギング、ファイル窃取、スクリーンショットキャプチャなどの情

報窃取活動を行うために複数のコンポーネントを登録しました。このキャンペーンの戦術、技術、インフラは、諜報に重点を置いた脅威アクターに関連する歴史的パターンと密接に一致していました。

**[Attack Flow]**

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 Bandizip インストールパッケージ
   b. マルウェアペイロード偽装
2. [実行] コマンドおよびスクリプトインタープリター: Windows コマンドシェル (T1059.003)
   a. マルウェアスクリプトのリモートロード
   b. mshta を使用して VBScript を実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. VMProtect で難読化されたペイロード
   b. 不要なコードで分析を妨害
4. [持続性] システムプロセスの作成または変更: Windows サービス (T1543.003)
   a. regsvr32 を通じた DLL 登録
   b. スケジュールされたタスクの作成
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. ユーザーのキー入力記録
6. [収集] スクリーンキャプチャ (T1113)
   a. スクリーンショットのキャプチャ
7. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. ユーザーおよびシステム情報の窃取
   b. ファイルの窃取および転送
8. [コマンドと制御] アプリケーション層プロトコル: Web プロトコル (T1071.001)
   a. C2 サーバーとの通信
   b. リモートコマンドの実行

**7) SectorA05 used Malware disguised as System Check Reports (2025-07-16)**

https://cti.nshc.net/events/view/17131

脅威行為者は少なくとも 2012 年からサイバースパイ活動を行っており、主に韓国、日本、アメリカの機関を標的にしています。このグループの活動は、悪意のあるリンクや添付ファイルを含むフィッシングメール、リモートアクセス型トロイの木馬（RAT）やバックドアといった Malware を配布し、サプライチェーン攻撃を実行するなど、進化する戦術の使用が特徴です。彼らの作戦は、侵害されたネットワーク内での水平移動や様々な方法を活用した広範なデータ窃取活動に拡大しています。2022 年 10 月、このグループは Android デバイスを標的とする戦略を採用し、モバイル Malware

である FastFire、FastViewer、FastSpy を使用し、Firebase をコマンド＆コントロールサーバーとして構成しました。Androspy のような既存のオープンソース RAT を改良し、主に韓国の特定の目標を侵入するための高性能なバリアントを作成しました。2023 年 5 月、彼らは敏感なシステム情報を抽出し、知的財産にアクセスするためのグローバルキャンペーンで ReconShark というアップグレードされた偵察 Malware を導入しました。

**[Attack Flow]**

1. [初期アクセス] フィッシング (T1566)
   a. マルウェアリンクが含まれたフィッシングメール送信
   b. マルウェア添付ファイルが含まれたメール使用
2. [実行] ユーザー実行 (T1204)
   a. ユーザーがマルウェアリンクをクリック
   b. ユーザーが添付ファイルを開く
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. マルウェア自動実行登録
   b. システム起動時にマルウェア活性化
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. 検出を避けるためのコード難読化
   b. アンチウイルス回避技術使用
6. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. システムから資格情報ダンプ
   b. パスワードハッシュ収集
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
   b. アクティブホスト識別
8. [横移動] リモートサービス (T1021)
   a. リモートデスクトッププロトコル使用
   b. SMB を通じた移動
9. [収集] ローカルシステムからのデータ (T1005)
   a. ローカルシステムからのデータ収集
   b. 文書およびファイル収集
10. [コマンドとコントロール] C2 プロトコル (T1071)
    a. Firebase を C&C サーバーとして使用

b. コマンド受信およびデータ送信

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送信
    b. 機密情報の外部送信
12. [影響] データ破壊 (T1485)
    a. データ破壊の試み
    b. データの完全性の損傷

**8) SectorA06 used an Infostealer disguised as a Zoom audio repair tool (2025-06-21)**

https://cti.nshc.net/events/view/16360

攻撃対象産業群: 金融、娯楽、ゲーム

最近、カナダのオンラインギャンブルプロバイダーに関与し、脅威行為者がソーシャルエンジニアリング戦術を使用して既知の連絡先を偽装し、信頼できるブランドドメインを使用して情報を窃取する Malware を配布しました。攻撃は予定された Zoom 会議から始まり、この時、被害者はオーディオ復旧ツールに偽装したスクリプトを実行するよう促されました。このスクリプトは合法的な Zoom コンポーネントを利用してダウンロードコマンドを実行し、ユーザーの資格情報とデータを窃取する Malware を配布しました。攻撃に使用されたドメイン zoom-tech[.]us は、合法的な Zoom インフラに似せて作られ、欺瞞を助けています。感染チェーンはスクリプトのダウンロードを含む複数のステップを経て、合法的なソフトウェアコンポーネントに偽装した Malware のインストールに至りました。この Malware はキーチェーンファイルやブラウザデータなどの機密情報を収集し窃取しており、金銭的動機があることを示唆しています。合法的なツールとサービスの利用および複雑な資格情報収集技術は、高度な運用的洗練を示しています。

**[Attack Flow]**

1. [初期アクセス] フィッシング (T1566)
    a. Zoom 会議のスケジューリング
    b. オーディオ復旧ツールに偽装したスクリプト実行の誘導
2. [実行] コマンドとスクリプトインタープリタ (T1059)
    a. 正規の Zoom コンポーネントを利用したコマンド実行
    b. curl および zsh コマンドを通じたスクリプトのダウンロードと実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
    a. LaunchDaemon 構成ファイルの作成
    b. 管理者権限での LaunchDaemon のインストール
4. [防御回避] 偽装 (T1036)

a. 正規のソフトウェアコンポーネントに偽装
b. オペレーティングシステムコンポーネントを偽装したパスの使用
5. [資格情報アクセス] 入力キャプチャ (T1056)
a. ローカルアカウント資格情報の入力誘導
b. ユーザーパスワードの窃取およびコマンドでの使用
6. [収集] 情報リポジトリからのデータ (T1213)
a. ユーザーのキーチェーンファイルおよびブラウザデータの収集
b. ウェブブラウザのプロファイルおよび拡張に関連する情報の収集
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. C2 サーバーとの通信のための IP アドレス使用
b. curl を通じた Malware インフラへの接続
8. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. curl を通じた資格情報およびデータの窃取
b. 圧縮されたデータファイルの外部送信

**9) SectorA06 used NimDoor Malware targeting Web3 Crypto sector (2025-07-02)**
https://cti.nshc.net/events/view/16548

2025 年 4 月、北朝鮮の脅威アクターによる標的型サイバー攻撃が Web3 スタートアップを対象に観察されました。この攻撃は、Nim でコンパイルされたバイナリと Web3 および暗号通貨関連の事業体を狙った複数の攻撃ベクターを活用した多面的なアプローチを使用しました。攻撃は、信頼できる連絡先を装って悪性ドメインにホスティングされた「Zoom SDK アップデートスクリプト」を配布するソーシャルエンジニアリング戦術で始まりました。初期の侵害は、NimDoor というカスタムマルウェアを含む複雑な攻撃チェーンにつながりました。このマルウェアは、macOS で珍しいプロセスインジェクションと TLS 暗号化 WebSocket プロトコル（wss）を通じたリモート通信を使用しました。Bash スクリプトは、Keychain 資格情報やブラウザデータなどの機密データを漏洩するために使用されました。攻撃者はまた、AppleScript およびシグナルベースのロジックを活用して持続性を確立し、長期的なアクセスを維持しました。

**[Attack Flow]**
1. [初期アクセス] フィッシング: サービスを介したスピアフィッシング (T1566.003)
a. テレグラムを通じた信頼できる連絡先のなりすまし
b. カレンダーでの会議招待
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
a. Zoom SDK アップデートスクリプトの実行
b. コマンド＆コントロールサーバーからの 2 段階スクリプトの実行

3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. AppleScript ファイルに 10,000 行の空白を追加
   b. Nim でコンパイルされたバイナリの使用
4. [持続性] ブートまたはログオン自動開始実行: Launch Agent (T1547.013)
   a. LaunchAgent を通じた持続性の維持
   b. Google LLC および CoreKitAgent のインストール
5. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. プロセスインジェクション技術の使用
   b. シグナルベースの持続性メカニズムの活用
6. [資格情報アクセス] OS 資格情報ダンピング: キーチェーン (T1555.001)
   a. キーチェーン資格情報の奪取
   b. ブラウザデータの収集
7. [収集] 情報リポジトリからのデータ (T1213)
   a. テレグラムデータベースの奪取
   b. システムおよびアプリケーションデータの収集
8. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
   a. wss を通じた C2 通信
   b. 多層の RC4 暗号化の使用
9. [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アップロード
   b. curl を通じたデータ転送

**10) SectorB01 used DLL Side-Loading with VIPRE Antivirus for DeedRAT (2025-07-18)**

https://cti.nshc.net/events/view/17038

新しいフィッシングキャンペーンが特定され、中国の脅威アクターに起因するモジュラー型バックドア DeedRAT を配布しています。このキャンペーンは、VIPRE Antivirus Premium のコンポーネントである MambaSafeModeUI.exe 内の DLL サイドローディング脆弱性を悪用しており、この攻撃での初めての使用例として記録されています。DeedRAT は、攻撃者がファイルの変更、ディレクトリのリスト作成、侵害されたシステムでのコード実行を可能にします。コマンド＆コントロール（C2）サーバーとの通信は主に TCP プロトコルを通じて行われ、HTTP、DNS、その他のプロトコルも利用可能です。このキャンペーンは、NetAgent という新しいモジュールを導入し、活発な開発と機能追加を示唆しています。Malware サンプルは MicRun.exe と悪意のある DLL を含む ZIP アーカイブで、シェルコードを使用して密かに実行され、Windows レジストリを通じて持続性を確保し、複数のインスタンスを防ぐためにミューテックスを生成し、ポート 80 と 443 を通じて C2 サーバ

ーと通信します。DeedRAT は、API ハッシュ化、疑似乱数文字列生成、カスタム暗号化アルゴリズムなどの高度な技術を使用して難読化と複雑性を増大させています。

**[Attack Flow]**

1. [初期アクセス] フィッシング (T1566)
   a. フィッシングメール配布
   b. マルウェア ZIP アーカイブ添付
2. [実行] DLL サイドローディング (T1574.002)
   a. MicRun.exe 実行
   b. SBAMBRES.DLL ロード
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. HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run¥MicRun 登録
   b. サービスとして MicRun 設定
4. [権限昇格] 権限昇格制御メカニズムの悪用 (T1548)
   a. svchost.exe プロセス内再実行
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. カスタム暗号化アルゴリズム使用
   b. API ハッシュ適用
6. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. システムボリュームシリアル番号でシード生成
   b. 疑似乱数アルゴリズム使用
7. [探索] システム情報探索 (T1082)
   a. システム情報収集
8. [横移動] リモートサービス (T1021)
   a. TCP、HTTP、DNS プロトコルを通じた C2 通信
9. [コマンド＆コントロール] 暗号化チャネル (T1573)
   a. ポート 80 および 443 を通じた通信
   b. NetAgent モジュールを通じたサーバー要求処理
10. [データ流出] C2 チャネルを通じたデータ流出 (T1041)
    a. C2 サーバーへのデータ送信
    b. Luckybear669.kozow[.com を通じた通信

**11) SectorB01 used Webshell via SAP NetWeaver Exploit CVE-2025-31324 (2025-07-09)**

https://cti.nshc.net/events/view/16760

攻撃対象産業群: 製造、IT、教育、観光、食品、自動車

SAP NetWeaver の脆弱性（CVE-2025-31324）は、2025 年 5 月から中国と関連する脅威アクターによって積極的に悪用されています。この脆弱性は 2025 年 1 月に初めて検出され、SAP NetWeaver Visual Composer Metadata Uploader における認証されていないファイルアップロードの脆弱性であり、CVSS スコアは 9.8 です。悪用されると、脅威アクターがウェブシェルを展開し、vshell や CobaltStrike Beacon のような Malware を仕込むことができます。アメリカ、中国を含む複数の国や様々な業種の 100 以上のエンティティおよび主要なクラウドサービスプロバイダーが被害を受けました。SAP は 2025 年 5 月にセキュリティ通知を通じてこの脆弱性に対処しましたが、2025 年 4 月までに公開レポートと Proof-of-Concept が既に提供されていました。この脆弱性は、攻撃者が悪意のあるファイルをアップロードしてネットワークに損害を与える可能性をもたらします。

[Attack Flow]

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. SAP NetWeaver Visual Composer Metadata Uploader での脆弱性悪用
    b. 認証されていないファイルアップロードの実行
2. [実行] コマンドとスクリプトインタープリター (T1059)
    a. Web シェルを通じてコマンドを実行
    b. マルウェア(vshell, CobaltStrike Beacon)のインストール
3. [持続性] Web シェル (T1505.003)
    a. ./apps/sap.com/irj/root/ および ./apps/sap.com/irj/work/ パスに Web シェルを配置
    b. JSP Web シェル(cache.jsp, shell.jsp など)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. Web シェルコードの難読化
    b. CobaltStrike Beacon の隠蔽機能の活用
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
    a. Mimikatz ツールの使用
    b. システム資格情報のダンプ
6. [探索] システム情報探索 (T1082)
    a. ネットワークおよびシステム情報の収集
    b. 内部資産のマッピング
7. [横移動] リモートサービス (T1021)
    a. リモートサービス接続を通じた移動
    b. ネットワーク内の他のシステムへの拡散
8. [コマンドと制御] アプリケーション層プロトコル (T1071)

a. HTTP/S を通じたコマンド制御トラフィックの生成
b. CobaltStrike Beacon を活用した C2 通信
9. [影響] データ操作 (T1565)
a. データの改ざんおよび削除
b. ビジネス運営の妨害

**12) SectorB22 used Phishing Lures Disguised as Tibetan Community Topics (2025-06-23)**

https://cti.nshc.net/events/view/16444

攻撃対象産業群: 政府・行政、軍事機関、外交

2025 年 6 月、中国と連携した脅威アクターがチベット共同体を対象にサイバー作戦を実施しました。このキャンペーンは重要なチベットのイベントと同時に行われ、Pubload マルウェアを利用したスパイ活動が含まれていました。脅威アクターは、チベット自治区の中国教育政策やダライ・ラマの書籍に関連するフィッシング誘因を使用して被害者を誘惑しました。これらの誘引物は、地政学的なテーマに関連するファイル名を持つ武器化されたアーカイブを含んでいました。アーカイブには、DLL サイドローディングに脆弱な無害な実行ファイルと「Claimloader」というマルウェア DLL が含まれており、これは Pubload バックドアをメモリに復号して注入しました。このバックドアはその後、Pubshell というリバースシェルを通じてアクセスを可能にしました。この作戦は、インド、アメリカ、日本を含む複数の国のチベット関連イベント、例えば第 9 回世界議会議員チベット会議を対象としました。脅威アクターは、DLL サイドローディング、暗号化、Google Drive リンクを含むフィッシングメールなどの高度な技術を使用して、洗練された能力と適応力を示しました。

**[Attack Flow]**

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. Google Drive リンクを含む
2. [実行] ユーザー実行 (T1204)
a. 武器化されたアーカイブの実行
b. DLL サイドローディングを誘発
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
a. レジストリキーの使用
b. Claimloader の実行自動化
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. ファイル名の混乱
b. 暗号化技術の使用

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. メモリ内のパスワード解読
6. [コマンド＆コントロール] ツール転送の侵入 (T1105)
   a. Publoadバックドアのダウンロード
   b. Pubshellリバースシェルの実行
7. [データ流出] C2チャネルを介したデータ流出 (T1041)
   a. C2サーバーを通じたデータ送信
   b. TLS 1.2データパケットの使用

**13) SectorB73 used ShortLeash Backdoor and Fake LAPD Certificates (2025-06-23)**

https://cti.nshc.net/events/view/16372

攻撃対象産業群: IT、IT - ISP、メディア・報道

「LapDogs」という新しいサイバー脅威ネットワークが確認され、主に世界中のLinuxベースの小規模オフィス/家庭オフィス（SOHO）デバイスを対象としています。主な攻撃対象地域はアメリカと東南アジアで、2023年9月に開始されました。LapDogsは「ShortLeash」というカスタムバックドアを使用してデバイスにアクセスし、高度な権限で秘密裏に作業を行います。1,000以上のデバイスが自己署名のTLS証明書を通じてネットワークセキュリティを強化し、損傷を受けました。この攻撃はインターネットに露出した脆弱性を利用し、中国と関連する脅威であり、地理的なターゲティングと中国語の開発者ノートがこれを裏付けています。このキャンペーンは日本、韓国、台湾、香港などの特定の国に焦点を当て、IT、ネットワーキング、不動産、メディア分野を対象に精密に組織されています。LapDogsは「PolarEdge」という類似ネットワークと一部のインフラ特性を共有していますが、独立した作戦です。

**[Attack Flow]**

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. インターネットに公開されたウェブおよびアプリケーションサーバーの脆弱性を悪用
   b. 古いバージョンのACME mini_httpdおよびその他のサービスを対象
2. [実行] コマンドおよびスクリプトインタープリター (T1059)
   a. マルウェアのBashスクリプトを通じてShortLeashバックドアを実行
   b. サービスファイルを通じて持続性を維持
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. システムディレクトリにサービスファイルを挿入
   b. 再起動時にバックドアを自動実行
4. [防御回避] 偽装 (T1036)
   a. Nginxウェブサーバーに偽装したサービスを実行

b. LAPD に偽装した TLS 証明書を生成
5. [資格情報アクセス] ファイル内の資格情報 (T1081)
a. システムディレクトリ内の機密情報および証明書を抽出
6. [探索] ネットワークサービススキャン (T1046)
a. ネットワーク内のサービスおよびポートをスキャン
7. [収集] ローカルシステムからのデータ (T1005)
a. 感染したデバイスからローカルデータを収集
8. [コマンド＆コントロール] 暗号化チャネル (T1573)
a. TLS を通じた暗号化された C2 通信を設定
b. 自己署名証明書を使用してノード間の接続を維持
9. [流出] C2 チャネルを通じたデータ流出 (T1041)
a. C2 チャネルを通じてデータを流出
b. ポートおよび時間に基づいて侵入セットを調整

**14) SectorB94 exploited Ivanti CSA zero-day vulnerabilities (2025-07-01)**

https://cti.nshc.net/events/view/16587

攻撃対象産業群: 金融、政府・行政、通信、運輸、メディア・報道

2024 年 9 月、フランスの政府、通信、メディア、金融、輸送部門に属する複数の機関が、Ivanti Cloud Service Appliance デバイスのゼロデイ脆弱性（CVE-2024-8190、CVE-2024-8963、CVE-2024-9380）を悪用したサイバー攻撃の標的となりました。この攻撃の目的は、PHP ウェブシェルを展開し、PHP スクリプトを修正し、時にはルートキットをインストールするなどの手法を通じて初期アクセスと持続的な足場を確保することでした。このキャンペーンは「Houken」という固有の侵入セットによって実行され、中国語を話す開発者が作成したオープンソースツールと高度なゼロデイ使用が混在する特徴を持っています。攻撃インフラは匿名化サービスと専用サーバーで構成され、出所を隠蔽しようとする努力が見られます。攻撃の目的は、潜在的に国家と連携した行為者に販売できる価値あるアクセス権を収集し、データ窃取や暗号通貨マイニングの配置を通じて直接的な利益を得ることと見られます。

**[Attack Flow]**

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. Ivanti CSA デバイスの脆弱性 CVE-2024-8190、CVE-2024-8963、CVE-2024-9380 の悪用
b. PHP ウェブシェルの配布
2. [持続性] ウェブシェル (T1505.003)
a. PHP ウェブシェルの作成と配布

b. 既存の PHP スクリプトの修正
3. [防御回避] ルートキット (T1014)
a. カーネルモジュールのインストール
b. ルートキットを使用してコマンド実行を偽装
4. [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. システムからの資格情報の収集
b. Python スクリプトを使用して管理者パスワードの復号化
5. [コマンド＆コントロール] 非標準ポート (T1571)
a. 非標準ポートを通じた C2 サーバーとの通信
b. 専用サーバーを使用したコマンド＆コントロール
6. [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 チャネルを通じて流出
b. 大量のメールの窃取
7. [影響] リソースのハイジャック (T1496)
a. 暗号通貨マイナーのインストールと運用
b. Monero マイニングのための C3Pool ツールの使用

**15) SectorB111 used DLL Sideloader and VELETRIX for Espionage Efforts (2025-07-02)**

https://cti.nshc.net/events/view/16729

攻撃対象産業群: 通信

最近のサイバー脅威キャンペーンである DragonClone は、中国の主要通信会社の子会社である China Mobile Tietong Co., Ltd.を標的にしました。この作戦は国家に関連するアクターによって実行され、通信インフラに侵入してデータトラフィックを監視することで、大規模なスパイ活動を目的としています。初期アクセスは、内部教育プログラムに偽装したバイナリが含まれた ZIP ファイルを利用したスピアフィッシングメールを通じて行われました。実行には、正常なソフトウェアである Wondershare の Recoverit を悪性 DLL である VELETRIX をロードするように操作する DLL サイドローディングが含まれていました。VELETRIX は動的 API ローディングとスタックストリングを使用して、暗号化されたシェルコードが含まれた IPv4 アドレスを復号化します。実行のために EnumCalendarInfoA を使用し、検出を避ける非伝統的なメモリ操作技術を活用します。中国にハードコーディングされたコマンド＆コントロールサーバーとの通信は、WinSocket を通じた暗号化されたデータ交換で行われます。この作戦は、スパイ活動のための VShell という攻撃セキュリティツールの配備を示唆しており、国家が後援するサイバー戦争で使用される持続的で複雑な能力を強調しています。

**[Attack Flow]**

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. ZIP ファイル内バイナリ
   b. 内部教育プログラムに偽装
2. [実行] DLL サイドローディング (T1574.002)
   a. Wondershare Recoverit の悪用
   b. 悪性 DLL VELETRIX のロード
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 動的 API ローディング
   b. スタックストリング技術
4. [実行] コマンドおよびスクリプトインタープリタ: Windows コマンドシェル (T1059.003)
   a. EnumCalendarInfoA の使用
   b. メモリ操作技法
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. WinSocket を通じた通信
   b. 暗号化されたデータ交換
6. [収集] ネットワーク共有ドライブからのデータ (T1039)
   a. 通信インフラの監視
   b. データトラフィックの収集
7. [流出] 代替プロトコルを介した流出 (T1048)
   a. VShell ツールの使用
   b. コマンド＆コントロールサーバーとのデータ転送

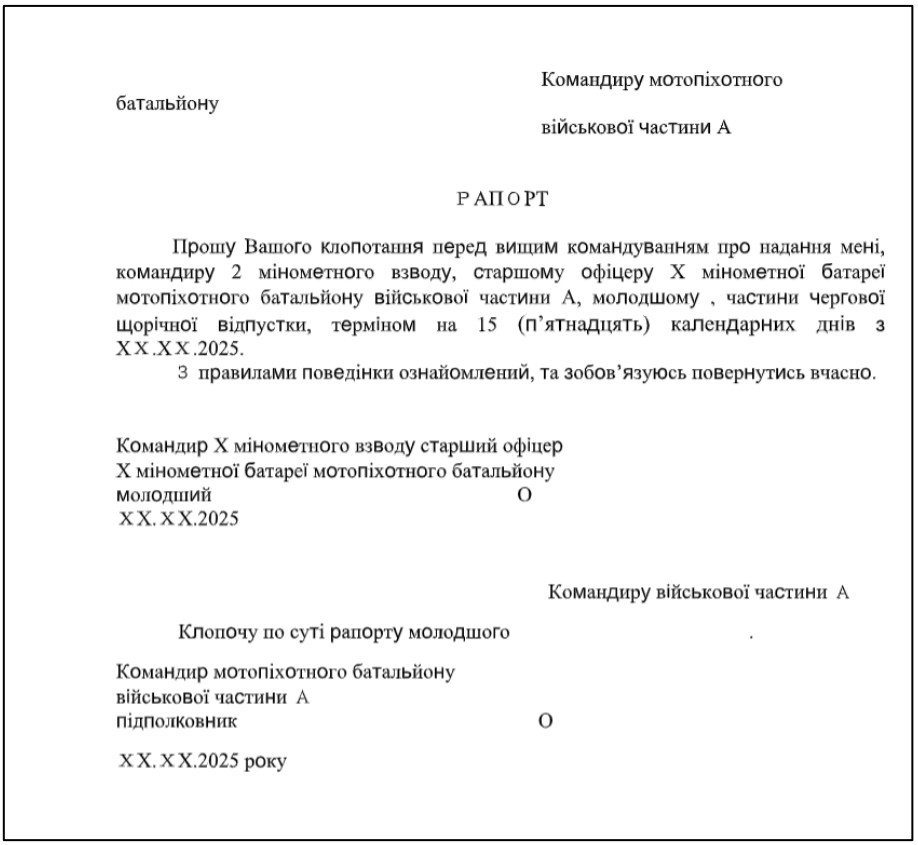
**16) SectorC01 used Covenant and Beardshell disguised as Word documents (2025-06-21)**

https://cti.nshc.net/events/view/16359

攻撃対象産業群: 政府・行政

2024 年 3 月頃、政府の IT システムの Windows サーバーでマルウェアが識別されました。検出された脅威には、BEARDSHELL と SLIMAGENT が含まれていました。C++で開発された BEARDSHELL は、Icedrive API を通じて PowerShell スクリプトを復号化（chacha20-poly1305 を使用）し、実行します。また、C++で開発された SLIMAGENT は、スクリーンショットをキャプチャし、ローカルストレージに保存するために AES+RSA で暗号化します。マクロが含まれた「Акт.doc」ドキュメントは、Signal を通じて配布され、COM ハイジャックを利用して COVENANT フレームワークに関連する PlaySndSrv.dll のようなファイルをロードしました。この作戦は、Koofr API を活用してシステム再起動時に BEARDSHELL バックドアを実行しました。この

攻撃は、ホスト保護を回避するために合法的なサービス API を利用し、隠密性と持続性を強化しました。



Командиру мотопіхотного
батальйону
військової частини А

РАПОРТ

Прошу Вашого клопотання перед вищим командуванням про надання мені, командиру 2 мінометного взводу, старшому офіцеру Х мінометної батареї мотопіхотного батальйону військової частини А, молодшому , частини чергової щорічної відпустки, терміном на 15 (п'ятнадцять) календарних днів з ХХ.ХХ.2025.
З правилами поведінки ознайомлений, та зобов'язуюсь повернутись вчасно.

Командир Х мінометного взводу старший офіцер
Х мінометної батареї мотопіхотного батальйону
молодший О
ХХ.ХХ.2025

Командиру військової частини А

Клопочу по суті рапорту молодшого .

Командир мотопіхотного батальйону
військової частини А
підполковник О

ХХ.ХХ.2025 року

[図 4: SectorC01 グループが利用したおとり文書]

**[Attack Flow]**

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. Signal を通じて「Акт.doc」文書を送信
   b. マクロの有効化を通じて初期アクセスを実行
2. [実行] コマンドとスクリプトインタープリター: PowerShell (T1059.001)
   a. BEARDSHELL を通じて PowerShell スクリプトを実行
   b. Icedrive API を使用してコマンドを送信
3. [持続性] システムプロセスの作成または変更: Windows サービス (T1543.003)
   a. tcpiphlpsvc サービスを作成し、自動起動を設定
   b. COM ハイジャックを通じて持続性を維持
4. [防御回避] 偽装: 正当な名前または場所に一致 (T1036.005)
   a. 正当なサービス API を利用
   b. Koofr API を通じた C2 通信の隠蔽
5. [資格情報アクセス] 入力キャプチャ: スクリーンキャプチャ (T1113)

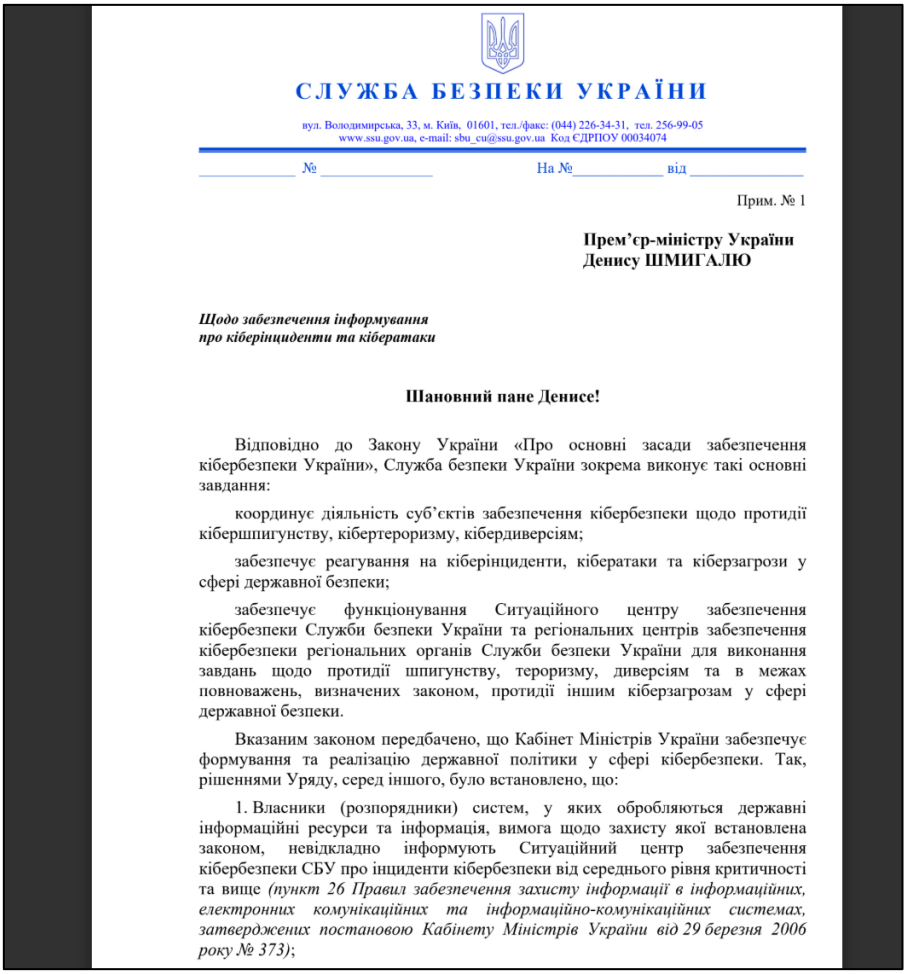
a. SLIMAGENT を利用したスクリーンショットのキャプチャと暗号化
b. ローカルストレージに暗号化されたスクリーンショットを保存
6. [データ流出] C2 チャネルを通じたデータ流出 (T1041)
a. Icedrive および Koofr API を通じたデータ送信
b. バックドアを通じた情報流出
7. [コマンドと制御] アプリケーション層プロトコル: Web プロトコル (T1071.001)
a. Koofr API を通じた C2 コマンドの送信
b. システム再起動時に BEARDSHELL バックドアを実行

**17) SectorC01 used Python LAMEHUG Malware in Phishing Email Campaign (2025-07-17)**

https://cti.nshc.net/events/view/16986

攻撃対象産業群: 政府・行政

2025 年 7 月 10 日、サイバー脅威は政府執行機関を対象とした詐欺メールの配布を含み、これは省庁の代表から送信されたかのように見えます。これらのメールには「Додаток.pdf.zip」という添付ファイルが含まれており、その中には Python コードから PyInstaller を使用して変換された「.pif」拡張子を持つ悪意のあるファイルが含まれており、これは LAMEHUG というマルウェアとして識別されます。データ漏洩方法に変形がある「AI_generator_uncensored_Canvas_PRO_v0.9.exe」と「image.py」という 2 つの追加バージョンが発見されました。このキャンペーンは配布のために侵害されたメールアカウントを使用し、コマンドインフラは合法的ですが侵害されたリソースで運営されています。LAMEHUG はコマンド実行の説明を生成するために大規模言語モデルを使用する特徴を持っています。システム情報を収集し、指定されたディレクトリで Office 文書を検索して保存します。漏洩は SFTP または HTTP POST リクエストを通じて発生します。



СЛУЖБА БЕЗПЕКИ УКРАЇНИ

вул. Володимирська, 33, м. Київ, 01601, тел./факс: (044) 226-34-31, тел. 256-99-05
www.ssu.gov.ua, e-mail: sbu_cu@ssu.gov.ua Код ЄДРПОУ 00034074

№ На № від

Прим. № 1

Прем'єр-міністру України
Денису ШМИГАЛЮ

*Щодо забезпечення інформування*
*про кіберінциденти та кібератаки*

**Шановний пане Денисе!**

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», Служба безпеки України зокрема виконує такі основні завдання:

координує діяльність суб'єктів забезпечення кібербезпеки щодо протидії кібершпигунству, кібертероризму, кібердиверсіям;

забезпечує реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки;

забезпечує функціонування Ситуаційного центру забезпечення кібербезпеки Служби безпеки України та регіональних центрів забезпечення кібербезпеки регіональних органів Служби безпеки України для виконання завдань щодо протидії шпигунству, тероризму, диверсіям та в межах повноважень, визначених законом, протидії іншим кіберзагрозам у сфері державної безпеки.

Вказаним законом передбачено, що Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки. Так, рішеннями Уряду, серед іншого, було встановлено, що:

1. Власники (розпорядники) систем, у яких обробляються державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом, невідкладно інформують Ситуаційний центр забезпечення кібербезпеки СБУ про інциденти кібербезпеки від середнього рівня критичності та вище *(пункт 26 Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373)*;

[図 5: SectorC01 グループが利用したおとり文書]

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 詐欺メール配布
   b. 省庁代表を装う
2. [実行] ユーザー実行 (T1204)
   a. 添付ファイル実行
   b. .pif ファイル使用
3. [持続性] 有効なアカウント (T1078)
   a. 侵害されたメールアカウント使用
   b. 合法的なリソースで運用
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. PyInstaller で変換
   b. Python コードベース
5. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. システム情報収集

b. Office 文書検索
6. [収集] ローカルシステムからのデータ (T1005)
a. システム情報保存
b. 指定ディレクトリに文書保存
7. [流出] 代替プロトコルによる流出 (T1048)
a. SFTP リクエスト
b. HTTP POST リクエスト
8. [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. コマンド実行説明生成
b. 大規模言語モデル使用

**18) SectorC08 used Spearphishing with Malicious LNK Files in Ukraine (2025-07-02)**

https://cti.nshc.net/events/view/16589

攻撃対象産業群: 政府・行政

2024 年初頭から、あるサイバースパイグループがウクライナ政府機関を集中的に標的にしています。このグループは以前に NATO 諸国に侵入しようとしたことがあり、スピアフィッシングキャンペーンを強化し、悪意のあるハイパーリンクや PowerShell スクリプトを実行する LNK ファイルなどの新しい方法を使用しています。PowerShell と VBScript を活用して、隠蔽、持続性、および横方向の移動のために 6 つの新しいマルウェアツールが導入されました。既存のツールは、強化された難読化および隠蔽戦術を含む大規模なアップグレードを受けました。このグループは Cloudflare トンネルを使用してコマンド＆コントロール（C&C）インフラストラクチャを効果的に隠し、Telegram や Dropbox などのサービスを統合して運用を保護しました。注目すべきことに、Telegram を通じてロシアのプロパガンダを拡散する異常な VBScript ペイロードが発見されました。このグループはネットワーク回避技術を継続的に適応させ、fast-flux DNS やサードパーティサービスを利用してインフラを隠し、動的に展開することで、地政学的な対立が続く中で持続的な脅威を示しています。

**[Attack Flow]**

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. スピアフィッシングメール送信
b. マルウェア LNK ファイルとマルウェアハイパーリンクを含む
2. [実行] コマンドとスクリプトインタープリタ: PowerShell (T1059.001)
a. LNK ファイルを通じた PowerShell スクリプトの実行
b. Cloudflare ドメインでの PowerShell コマンド実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
a. Microsoft Excel アドインを通じた異常な持続性方法の使用

b. スケジュールされたタスクを使用した持続性の維持
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. コード難読化と複雑な LNK ファイルの生成
b. レジストリベースの技術を活用したファイルおよび拡張子の隠蔽
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. 資格情報の窃取試行
b. ストアからの資格情報の抽出
6. [発見] システム情報の発見 (T1082)
a. システム診断データの収集
b. 配布されたマルウェアの状態確認
7. [横移動] リモートサービス: SMB/Windows 管理共有 (T1021.002)
a. ネットワークドライブを通じた拡散
b. USB ドライブの武器化
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: ウェブプロトコル (T1071.001)
a. Cloudflare トンネルを通じた C&C 通信
b. Telegram および Telegraph API を通じた通信チャネルの構築
9. [データ流出] C2 チャネルを通じたデータ流出 (T1041)
a. Dropbox API を通じたファイル流出
b. WMI イベントサブスクリプションを活用した USB ドライブの監視
10. [影響] データ操作 (T1565)
a. Telegram を通じたロシアのプロパガンダの拡散
b. 地政学的な対立を助長する活動

**19) SectorC08 used VBS Malware disguised as DOCX for Ukraine Attacks (2025-07-18)**

https://cti.nshc.net/events/view/17059

攻撃対象産業群: 政府・行政、軍事機関

2013 年から活動している APT グループが主にウクライナの政府部門と軍事機関を対象に情報窃取を試みています。このグループは、文書テンプレート、マクロ文書、自動解凍ファイルなど、さまざまなペイロードを使用して検出を困難にしています。最近の攻撃はウクライナ政府の機能に集中しており、ウクライナ語の文書を餌として使用しています。この文書を開くと、悪性マクロがリモートでロードされ、VBS スクリプトを復号および実行して基本ユーザー情報をアップロードし、追加のペイロードをダウンロードします。このグループは分析を妨害するために高度な VBS スクリプト難読化技術を使用し、主要な文字列を分割およびエンコードし、難読化セクションを挿入します。システムドライブのシリアル番号とコンピュータ名を組み合わせてユニークな識別子を生成し、User-

Agent をカスタマイズします。DNS クエリを通じてドメインの目的地を解決し、ペイロードダウンロードのための URL を構成し、これによりサーバーアドレスを変更することができます。この攻撃は、機密情報へのアクセスと主要インフラの妨害を目的としています。

**[Attack Flow]**

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. ウクライナ語文書の利用
   b. マクロ文書の添付
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. 文書を開くとマクロが実行
   b. VBS スクリプトの復号と実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. VBS スクリプトの難読化
   b. 文字列の分割とエンコード
4. [認証情報アクセス] 入力キャプチャ (T1056)
   a. ユーザーの基本情報をアップロード
   b. 追加ペイロードのダウンロード
5. [コマンド＆コントロール] 動的解決 (T1568)
   a. User-Agent に固有の識別子を生成
   b. DNS クエリでドメインを解決し、URL を構成

**20) SectorD16 used Havoc Backdoor (2025-06-23)**

https://cti.nshc.net/events/view/16420

中東の重要な国家インフラを対象としたサイバー侵入が、Microsoft Windows システムで Havoc フレームワークの亜種を使用して行われました。攻撃者はシステムのタスクスケジューラを利用して「conhost.exe」に偽装したリモートインジェクターを実行し、持続性を維持しました。インジェクターは DLL ファイルから復号化されたシェルコードを通じて「cmd.exe」プロセスで Havoc バックドア RAT を展開し、実行しました。Havoc フレームワークはリモートアクセス型トロイの木馬（RAT）として設計されており、C2 サーバーを通じて侵害されたシステムに対する完全なリモート制御を可能にします。このマルウェアは多様な通信プロトコルをサポートし、広範な制御コマンドを含み、デーモンを修正せずに機能を強化できるようにメモリ内実行のためのビーコンオブジェクトファイル（BOFs）を活用します。感染したシステムのメタデータは AES で暗号化され、登録プロセスで C2 サーバーに送信されます。

**[Attack Flow]**

1. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. タスクスケジューラの使用
   b. "conhost.exe"に偽装されたリモートインジェクタの実行
2. [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にインジェクタを追加
   b. 持続性の維持
3. [防御回避] 偽装 (T1036)
   a. "conhost.exe"に偽装
   b. 被害者を誤導
4. [実行] 共有モジュール (T1129)
   a. DLL ファイルからシェルコードを復号化
   b. "cmd.exe"プロセスで Havoc を実行
5. [収集] ローカルシステムからのデータ (T1005)
   a. システムメタデータの収集
   b. C2 サーバーへ送信
6. [コマンドとコントロール] 暗号化チャネル (T1573)
   a. AES 暗号化の使用
   b. C2 サーバーとの通信
7. [コントロール] C2 通信 (T1071)
   a. 多様な通信プロトコルのサポート
   b. C2 サーバーを通じた制御

**21) SectorD36 used Spear-Phishing with React-based Phishing Kits (2025-06-25)**

https://cti.nshc.net/events/view/16401

攻撃対象産業群: 政府・行政、軍事機関、学界 - 大学

イスラエルとイラン間の緊張の中で、現在進行中のサイバー脅威がイスラエルの個人を対象としています。この作戦は、攻撃者がサイバーセキュリティ会社の社員を装い、メールまたは WhatsApp を通じて AI で作成されたメッセージで攻撃対象に接触するスピアフィッシング戦術を使用します。フィッシングキャンペーンは、高官からジャーナリストまで様々な人物を利用して、被害者を資格情報の公開に誘導します。攻撃者は、Google、Outlook、Yahoo のログインプロセスを模倣したマルウェアフィッシングページに被害者を誘導し、React ベースのシングルページアプリケーション（SPA）で開発された精巧なカスタムフィッシングキットを使用します。このキットは認証インターフェースを反映し、被害者に資格情報と多要素認証コードを入力させ、これを POST リクエストと WebSocket 接続を通じたリアルタイムキーロギングで攻撃者のバックエンドに送信します。資格情報の盗用に加えて、攻撃者は緊張を利用して対面会議を提案し、キャンペーンの物理的な次元を示唆

します。多くのドメインとサブドメインが検出後すぐに設定され、解体され、脅威の敏捷性と持続性を維持します。

**[Attack Flow]**

1. [偵察] 動的解決 (T1590.005)
   a. ドメインおよびサブドメインの迅速な設定と解除
   b. 検出後のインフラストラクチャの持続性維持
2. [初期アクセス] スピアフィッシング (T1566.002)
   a. サイバーセキュリティ会社の社員を装う
   b. メールおよび WhatsApp の使用
3. [資格情報アクセス] 入力キャプチャ (T1056)
   a. Google、Outlook、Yahoo のログインページを模倣
   b. 資格情報および多要素認証コードの要求
4. [データ抽出] Web サービスを介したデータ抽出 (T1567)
   a. POST リクエストを通じた資格情報の送信
   b. WebSocket 接続を通じたリアルタイムのキーロギング

**22) SectorE01 used LNK Malware disguised as academic PDF files (2025-07-11)**

https://cti.nshc.net/events/view/16848

攻撃対象産業群: 産業、政府・行政、軍事機関、電力、外交、学界 - 大学、研究・革新機関

脅威アクターは 2009 年 11 月から活動を開始し、南アジアを背景にアジア全域の政府、軍事、エネルギー、産業、教育、外交および経済分野の組織を対象に攻撃を行っています。最近、彼らは偽の大学ドメインサーバーを通じて攻撃を実行するために悪意のある LNK ファイルを使用しました。攻撃には、エネルギー部門に関連する PDF ファイルをダウンロードし、Rust で作成されたローダーがシェルコードを解読して C# トロイの木馬を実行するプロセスが含まれています。C# トロイの木馬はシステム実行ファイルに偽装し、さまざまなシステムの詳細情報を収集し、コマンド＆コントロールサーバーとの通信を確立します。このマルウェアは、プロセスの終了、データ収集、コマンドの実行、ファイル管理など、システム操作のためのさまざまなコマンドをサポートしています。接続はサーバーに暗号化された識別子を送信することでセキュリティが維持されます。攻撃者は巧妙なドメイン名を使用してトラフィックを合法的に見せかけました。また、データ窃取機能を強化するために複数のオープンソース RAT を活用しました。

**[Attack Flow]**

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 LNK ファイルを添付したフィッシングメールの送信

b. 偽の大学ドメインサーバーを通じたダウンロード誘導
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 LNK ファイルを実行
b. PDF ファイルに偽装された LNK ファイルを実行
3. [持続性] スケジュールされたタスク/ジョブ (T1053)
a. GoogleErrorReport と名付けられたスケジュールタスクの設定
b. Winver.exe 実行のためのタスクをスケジュール
4. [防御回避] 偽装 (T1036)
a. システムファイルに偽装した C# トロイの木馬
b. 正常なトラフィックに偽装されたネットワーク通信
5. [収集] ローカルシステムからのデータ (T1005)
a. システム詳細情報の収集
b. ホスト名、ユーザー名、デバイス UUID の収集
6. [コマンドとコントロール] 暗号化されたチャネル (T1573)
a. 暗号化された識別子をサーバーに送信
b. C2 サーバーとの暗号化された通信の設定
7. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. 収集された情報を C2 サーバーに送信
b. C2 の応答に基づく追加コマンドの実行
8. [影響] システム回復の妨害 (T1490)
a. プロセス終了によるシステム回復の妨害
b. cmd モードでのコマンド実行と終了

**23) SectorE02 used LoptikMod Malware disguised as a PDF Document (2025-07-08)**

https://cti.nshc.net/events/view/16796

攻撃対象産業群: 政府・行政、国防、非政府組織(NGO)、外交

洗練されたサイバー諜報キャンペーンがヨーロッパの外交部を対象に多段階攻撃を実行しています。脅威行為者はヨーロッパの防衛関係者を装い、Google ドライブリンクを使用したスピアフィッシングメールで対象を誘導します。このリンクは悪意のある RAR アーカイブに接続されており、そこには実行ファイル notflog.exe が含まれています。実行時に、マルウェアは予約タスクを通じて持続性を確立し、コマンド＆コントロールサーバーと通信して機密データを流出させようと試みます。「LoptikMod」として知られるこのマルウェアは、バイナリ文字列の難読化、動的 API ローディング、アンチ VM 対策などの技術を使用して検出を回避します。システム情報を収集し、C2 サーバーとの通信を確立して潜在的な追加措置を実行します。このキャンペーンは外交機関に対する持続的な

脅威を強調し、初期マルウェア配布のためのクラウドサービス活用の進化を示し、これらの高度な脅威に対抗するための強力なセキュリティ態勢の重要性を強調しています。

**[Attack Flow]**

1. [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. ヨーロッパ防衛関係者を装ったスピアフィッシングメールの送信
   b. Google ドライブリンクを通じたマルウェア RAR アーカイブの配布
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 SyClrLtr.rar ファイルを開く
   b. notflog.exe の実行
3. [持続性] スケジュールされたタスク/ジョブ: スケジュールされたタスク (T1053.005)
   a. "PerformTaskMaintain"というスケジュールされたタスクの作成
   b. 10 分ごとに実行設定
4. [防御回避] 難読化されたファイルまたは情報: 暗号化/エンコードされたファイル (T1027.013)
   a. バイナリ文字列の難読化を使用
   b. 実行時にデコード
5. [発見] システム情報の発見 (T1082)
   a. システム情報の収集（ユーザー名、ホスト名など）
   b. 収集された情報を C2 サーバーに送信
6. [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: ウェブプロトコル (T1071.001)
   a. C2 サーバー totalservices[.]info と HTTPS 通信
   b. 敏感なデータの流出試み
7. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. 収集したデータを暗号化して C2 サーバーに送信
   b. 追加コマンドの受信およびデータ流出の可能性

**24) SectorH03 delivered Malware via a purchase order-themed PDF lure (2025-06-21)**

https://cti.nshc.net/events/view/16291

攻撃対象産業群: 防衛、自動車、製造

該当グループは、政府文書のように見えるように操作された Malware PDF 添付ファイルを使用したフィッシングキャンペーンを通じて、インドの防衛関係者を標的にしています。これらの PDF を開くと、受信者は国家情報センターを模倣した偽のログインページに誘導されます。ページをクリックすると、正式なアプリケーションに偽装した悪意のある実行ファイルを含む ZIP アーカイブがダウンロードされます。このキャンペーンは、資格情報を収集し、機密ネットワークへの長期的なアクセ

スを確立することを目的としています。攻撃者は、ファイルレス実行、プロセスインジェクション、アンチデバッグおよびアンチ仮想マシン対策を含むアンチ分析技術などの技術的手法を使用します。最近登録されたドメインから発生した脅威は、短期的な悪意のある使用を示唆しており、主要なクラウドプロバイダーにホスティングされたインフラストラクチャを通じて検出を回避します。キャンペーンの戦術には、誤解を招くファイル名とアイコン、広範な難読化の使用、ユーザー資格情報をキャプチャするためのキーロギングが含まれます。ネットワーク通信は、疑わしいドメインクエリと暗号化されたトラフィックを伴い、これはアクティブなコマンド＆コントロールチャネルを示しています。


[図 6: SectorH03 グループが利用したフィッシング文書]

**[Attack Flow]**

1. [初期アクセス] フィッシング (T1566)
   a. マルウェア PDF 添付ファイル送信
   b. フィッシングメール送信
2. [実行] クライアント実行のためのエクスプロイト (T1203)
   a. マルウェア PDF 実行時に ZIP アーカイブをダウンロード
   b. 偽のログインページへのクリック誘導
3. [持続性] ブートまたはログオン自動開始実行 (T1547)

a. レジストリの修正
b. スタートアッププログラムの登録
4. [防御回避] アンチ VM/アンチデバッグ (T1497)
a. デバッガー検出
b. 仮想マシン回避
5. [資格情報アクセス] キーロギング (T1056.001)
a. キーロギングの実行
b. 資格情報の収集
6. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
a. 暗号化された C2 通信
b. 疑わしいドメインクエリ
7. [影響] データ流出 (T1485)
a. データの流出
b. 資格情報の送信

**25) SectorH03 used ELF Malware disguised as Cyber-Security-Advisory (2025-07-04)**

https://cti.nshc.net/events/view/16709

攻撃対象産業群: 政府・行政、防衛

精巧なサイバー諜報キャンペーンがフィッシングメールを通じてインド防衛部門の人員を標的にしています。攻撃は ZIP 添付ファイル内に偽装された悪性の.desktop ファイルを使用し、実行時にユーザーを欺くために PowerPoint を開いて注意をそらしつつ、同時に BOSS.elf という悪性 ELF バイナリを静かに実行します。このバイナリは、インド政府機関で一般的に使用される BOSS Linux システムで不正アクセスと持続性を可能にします。キャンペーンは、目に見える餌と隠れたペイロードの実行を組み合わせ、社会工学と技術的な隠密性を活用し、攻撃者がシステム情報を収集し、スクリーンショットを検出されずにキャプチャできるようにします。インフラは攻撃者のコマンド＆コントロールサーバーに接続するために、既知の悪性ドメインと関連付けられています。このキャンペーンは、Linux 環境に対する標的型フィッシング戦術の進化を示し、政府、防衛、および主要インフラ部門で警戒を強化する必要性を強調しています。

**[Attack Flow]**

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. ZIP 添付ファイル内の.desktop ファイル偽装
2. [実行] スクリプティング (T1059)
a. .desktop ファイル実行で Bash スクリプト開始

b. PowerPoint ファイルのダウンロードと実行
3. [持続性] システムプロセスの作成または変更 (T1543)
a. BOSS.elf バイナリのダウンロードと実行
b. chmod コマンドで実行権限付与
4. [権限昇格] システムプロセスの作成または変更 (T1543)
a. nohup コマンドでバックグラウンド実行維持
b. 持続的なシステムアクセス維持
5. [防御回避] 偽装 (T1036)
a. LibreOffice アイコン使用で偽装
b. ターミナルウィンドウなしで実行
6. [探索] ソフトウェア探索 (T1518)
a. システム情報収集
b. スクリーンショットキャプチャ
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. マルウェアドメイン接続
b. C2 サーバーと通信

**26) SectorS01 used WebDAV Exploit Disguised as Microsoft File Access (2025-06-25)**

https://cti.nshc.net/events/view/16425

攻撃対象産業群: 銀行、社会基盤施設、政府・行政

2024 年 11 月から、精巧なサイバー脅威キャンペーンがコロンビアの組織を標的にしています。このキャンペーンは、パッチが適用された Windows の脆弱性（CVE-2024-43451）を悪用した悪意のある URL を含むフィッシングメールから始まります。パッチが適用されているにもかかわらず、攻撃者は最小限のユーザーの操作で HTTP ポート 80 を通じて WebDAV リクエストを開始し、悪意のあるペイロードのダウンロードと実行を誘導します。攻撃者は柔軟な C2 インフラのために動的 DNS サービスを使用しています。62.60.226.112 や 21ene.ip-ddns[.]com のようなマルウェアキャンペーンと関連する外部 IP およびドメインへの接続を含む異常なネットワーク活動が観察されました。マルウェアは標準のアプリケーション層プロトコルや偽装といった回避技術を活用しました。データ漏洩は設定された C2 チャネルを通じて発生しました。

**[Attack Flow]**

1. [初期アクセス] フィッシング (T1566.002)
a. マルウェア URL を含むフィッシングメールの送信
b. ユーザーの相互作用を最小限にして攻撃を開始
2. [実行] ユーザー実行 (T1204)

a. WebDAV リクエストを通じたペイロードのダウンロード
b. マルウェアペイロードの実行
3. [防御回避] 偽装 (T1036)
a. 標準アプリケーション層プロトコルの活用
b. 偽装技術の使用
4. [コマンド＆コントロール] 動的解決 (T1568.002)
a. 動的 DNS サービスの使用
b. 柔軟な C2 インフラの構築
5. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. 設定された C2 チャネルを通じたデータ流出
b. 外部 IP およびドメインとの異常な接続

**27) SectorS01 used phishing disguised as Colombian bank login pages (2025-06-27)**

https://cti.nshc.net/events/view/16452

攻撃対象産業群: 銀行、金融

サイバー脅威キャンペーンは、ラテンアメリカ全域の組織を積極的にターゲットにしており、主にコロンビアの金融機関に集中しています。このキャンペーンは、Visual Basic Script (VBS) ファイルを初期攻撃ベクターとして使用し、無料の動的 DNS サービスを活用し、Remcos や AsyncRAT のようなリモートアクセス型トロイの木馬（RAT）を第 2 段階の Malware として配布します。ロシアの違法ホスティングプロバイダーと関連するインフラは 2024 年夏から使用されており、一貫したドメインパターンと IP 関連性が特徴です。脅威行為者は、ユーザーの資格情報を盗むために、合法的なコロンビアの銀行を模倣したフィッシングページをホスティングしています。フィッシングサイトは、HTML、CSS、画像ファイルを使用して銀行のログインポータルを複製します。第 1 段階の VBS スクリプトは、PowerShell コマンドを実行し、Base64 文字列をデコードし、暗号化された実行ファイルをダウンロードして実行するために使用されます。ポルトガル語のユーザーインターフェースを持つウェブベースの損傷したボットネットパネルは、コマンドを実行し、ファイルを流出させ、追加のペイロードを配布することで感染したシステムを管理します。このキャンペーンは、隠密性よりも迅速な配布に重点を置き、アクセスしやすいインフラを活用しています。

**[Attack Flow]**

1. [初期アクセス] フィッシング (T1566)
a. フィッシングページ作成
b. コロンビア銀行模倣
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. PowerShell コマンド実行

b. Base64 文字列デコード

3. [持続性] システムプロセスの作成または変更: Windows サービス (T1543.003)
   a. 予約タスク作成
   b. 管理者権限で再実行
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. VBS ペイロード難読化
   b. 暗号化された実行ファイルダウンロード
5. [コマンド＆コントロール] リモートアクセスソフトウェア (T1219)
   a. Remcos および AsyncRAT 配布
   b. C2 パネルと接続
6. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. データ流出
   b. 感染システム管理
7. [影響] データ操作 (T1565)
   a. ユーザー資格情報窃取
   b. フィッシングサイトを通じた機密情報収集

## 2. サイバー犯罪（Cyber Crime）ハッキンググループの活動

### 1) SectorJ39 used TransferLoader Malware disguised as Job Applications (2025-06-30)

https://cti.nshc.net/events/view/16704

攻撃対象産業群: 国防

サイバー脅威行為者は、技術と高度なツールを組み合わせて、スパイ活動やサイバー犯罪作戦を実行しています。このキャンペーンは、侵害されたルーターを使用したフィッシングメールと、犯罪地下世界のサービスを活用しています。これらのメールは、求職申請をテーマにしており、ユーザーを OneDrive または Google Drive を模倣したランディングページにリダイレクトする悪意のあるリンクを含んでいます。このキャンペーンで使用される主要なペイロードは洗練されたダウンローダーであり、広範な難読化技術を示し、暗号化を使用してランサムウェアのような追加のマルウェアをロードします。両方のクラスターは非常に類似したインフラと配信戦術を使用しており、技術的な実行では区別されますが、歴史的な活動と特性を共有しています。これは、可能な物流または運用上の接続、または共有サービスの共通の使用を示しています。

**[Attack Flow]**

1. [初期アクセス] フィッシング (T1566)
   a. 求職申請を装ったフィッシングメール
   b. 損傷したルーターを通じたメール送信
2. [実行] ユーザー実行 (T1204)
   a. OneDrive または Google Drive を模倣したランディングページ
   b. マルウェアリンクをクリックしてペイロードをダウンロード
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 難読化技術の使用
   b. 暗号化を通じた追加のマルウェアロード
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. C2 サーバーとの通信
   b. IPFS サービスを通じたユーティリティホスティング
5. [影響] 影響のためのデータ暗号化 (T1486)
   a. ランサムウェアの配布
   b. データの暗号化および身代金要求

**2) SectorJ41 used ASP.NET View State deserialization to exploit IIS servers (2025-07-08)**

https://cti.nshc.net/events/view/16733

攻撃対象産業群: 金融、製造、ハイテク

初期アクセスブローカー（IAB）は、ASP.NET サイトから漏洩した Machine Keys を悪用してヨーロッパとアメリカの組織にアクセスし、そのアクセス権を他の脅威アクターに販売しました。IAB は 2024 年 10 月から 2025 年初頭にかけて、金融サービス、先端技術、輸送部門を対象にしました。この方法は ASP.NET View State の逆シリアル化を含み、IAB がフォレンジック証拠を最小化しながらサーバーメモリでペイロードを実行できるようにします。脅威は漏洩した Machine Keys を悪用してマルウェアペイロードに署名し、.NET アセンブリをメモリから直接リフレクティブローディングを通じて IIS ウェブサーバーを悪用しました。主要なツールには、逆シリアル化ペイロードを作成するための ysoserial.net と、持続性および権限昇格のためのポストエクスプロイトツールが含まれていました。攻撃は一般的な IIS の脆弱性と暗号キーの再利用を利用してリモートでコードを実行し、アクセスを維持しました。初期アクセスが行われた後、内部ネットワークを対象とした偵察活動が重要でした。システムシェル、ネットワーク構成、「updf」のようなユーティリティを使用して SYSTEM レベルのアクセスのためのローカル権限昇格コマンドが観察されました。

**[Attack Flow]**

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. 流出した Machine Keys を使用してアクセス
   b. ASP.NET View State の逆シリアル化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: Windows コマンドシェル (T1059.003)
   a. cmd.exe を使用したコマンド実行
   b. システムシェルでネットワーク構成コマンドを実行
3. [持続性] アカウント作成: ローカルアカウント (T1136.001)
   a. updf を使用してローカル管理者アカウントを作成
   b. 新しいアカウントに管理者権限を付与
4. [権限昇格] アクセストークン操作: トークン偽装/窃取 (T1134.001)
   a. GodPotato エクスプロイトを使用して SYSTEM 権限を取得
   b. updf で SYSTEM 権限のコマンドを実行
5. [防御回避] 偽装: 正当な名前または場所に一致 (T1036.005)
   a. updf バイナリファイルの名前を変更
   b. エクスプロイトモジュールの名前を変更
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. ウェブサーバー構成ファイルから資格情報を取得
7. [探索] システムネットワーク構成探索 (T1016)
   a. ipconfig /all コマンドでネットワーク詳細情報を収集
   b. 内部ネットワークマッピングのためのポートスキャンを実行
8. [収集] ローカルシステムからのデータ (T1005)
   a. ファイルダウンロードモジュールで機密データを収集
   b. HTTP リクエストでデータを送信
9. [コマンドとコントロール] ツールの転送 (T1105)
   a. wget, curl を使用してツールを転送
   b. 外部サーバーから追加のペイロードをダウンロード
10. [影響] データ操作 (T1565)
    a. ウェブページ設定の変更で認証を回避
    b. 悪性ペイロード実行のためのデータ改ざん

**3) SectorJ196 used Realst Stealer disguised as video meeting software (2025-07-10)**

https://cti.nshc.net/events/view/16826

2024 年 12 月、精巧なサイバー脅威キャンペーンが、偽のスタートアップ企業を含む巧妙なソーシャルエンジニアリング攻撃を通じて Web 3 の従業員を標的にしました。これらの脅威アクターは、AI、ゲーム、ビデオ会議ソフトウェアを専門とする合法的な企業になりすまし、Notion、Medium、

GitHub などのプラットフォームを使用して本物のように見せかけました。攻撃者は X アカウントを侵害して被害者に連絡し、ソフトウェアに偽装した Malware をダウンロードさせて暗号通貨を奪おうとしました。この攻撃には Windows と macOS の両方のバージョンが使用され、前者はシステムプロファイリングのために Electron アプリを使用し、後者は Atomic Stealer という情報窃取ツールが含まれた DMG を使用しました。検出を避けるために、逆解析技術や盗まれたソフトウェア署名証明書が使用されました。「Eternal Decay」のような企業は、ユーザーが悪意のあるソフトウェアをインストールするよう誘導するために完全に操作されました。このキャンペーンは、信頼性を示すために脅威アクターが使用する高度な技術、例えば難読化やソーシャルメディアの悪用の程度を強調しました。

**[Attack Flow]**

1. [偵察] 被害者の身元情報を収集 (T1589)
    a. X アカウントを利用して被害者に連絡
    b. ソーシャルメディアで活動
2. [リソース開発] インフラの侵害 (T1583)
    a. 偽のスタートアップ会社を作成
    b. 盗まれたソフトウェア署名証明書を使用
3. [実行] ユーザー実行 (T1204)
    a. 被害者にソフトウェアのダウンロードを誘導
    b. Electron アプリの実行でシステムプロファイリング
4. [持続性] システムプロセスの作成または変更 (T1543)
    a. macOS で LaunchAgent を使用して持続性を設定
    b. ログイン時に自動実行を設定
5. [防御回避] ファイルまたは情報の難読化 (T1027)
    a. 難読化されたスクリプトを使用
    b. 解析防止技術を使用
6. [収集] 入力キャプチャ (T1056)
    a. ブラウザデータおよび暗号通貨ウォレット情報を窃取
    b. クッキーおよび文書を収集
7. [指揮統制] アプリケーション層プロトコル (T1071)
    a. 収集されたデータを圧縮して送信
    b. 定期的なネットワークリクエストでデータを送信
8. [影響] データ操作 (T1565)
    a. 被害者システムで情報を操作
    b. 暗号通貨ウォレットから資産を窃取

**4) SectorJ217 used Interlock RAT PHP disguised in web-inject scripts (2025-07-14)**
https://cti.nshc.net/events/view/16889

2025 年 5 月から、リモートアクセス型トロイの木馬（RAT）の新しい亜種を含む広範なキャンペーンが実行されています。この Malware は、JavaScript の代わりに PHP を使用し、侵害されたウェブサイトを通じて HTML にスクリプトを注入する方法で開始されます。ユーザーは身元確認を求める悪意のある JavaScript の要求を受け、これにより PowerShell スクリプトが実行され、RAT が配布されます。PHP の亜種は 2025 年 6 月に初めて検出されました。感染すると、複数の偵察機能が実行され、プロセスリスト、マウントされたドライブ、ネットワークデータなどの包括的なシステム情報が収集されます。コマンド＆コントロール（C2）は TryCloudFlare の URL とハードコーディングされた IP アドレスを通じて維持され、攻撃者は追加のペイロードをダウンロードして実行するなどの様々なコマンドをリモートで実行できます。持続性はレジストリの修正によって設定され、RDP を使用して横方向の移動が促進されます。このキャンペーンは様々な産業を対象としており、脅威行為者の進化した能力と以前の戦術からの戦略的調整を示しています。

**[Attack Flow]**

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を通じてアクセス
   b. HTML にスクリプトを注入
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. PowerShell を通じてマルウェアスクリプトを実行
   b. ユーザーに身元確認を要求
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ー (T1547.001)
   a. レジストリの修正で持続性を維持
   b. Windows 起動時に自動実行を設定
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 非標準の場所からの config ファイルのロード
   b. ZIP 拡張機能の使用
5. [発見] システム情報の発見 (T1082)
   a. システム情報の収集
   b. プロセスリストとネットワークデータの収集
6. [コマンドと制御] アプリケーション層プロトコル: Web プロトコル (T1071.001)
   a. TryCloudFlare URL を通じたコマンドと制御
   b. ハードコーディングされた IP アドレスの使用
7. [横方向移動] リモートサービス: リモートデスクトッププロトコル (T1021.001)

a. RDP を通じた横方向移動
b. 追加ペイロードのダウンロードと実行
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のデータ収集
b. JSON 形式での情報収集

**5) SectorJ237 used ELF Ransomware with Double-Extortion Model (2025-07-15)**

https://cti.nshc.net/events/view/16936

攻撃対象産業群: IT

2025 年初頭、ランサムウェアグループは当初、ソフトウェアの脆弱性を隠して金銭を要求するグループと誤解されましたが、後に伝統的な二重恐喝戦術を使用していることが確認されました。彼らは被害者のデータを暗号化し、それを公に流出させると脅迫します。2025 年 3 月、彼らはアメリカの IT 企業を最初の被害者と主張しました。5 月までに、彼らは多くの待機ターゲットを理由に出版を中止し、「World Leaks」という恐喝プラットフォームを使用したと疑われました。技術的には、C/C++で開発された 64 ビット ELF バイナリは Linux システムを対象としており、ChaCha20 暗号化と ECDH キー交換を使用して攻撃者の協力なしには復号化が不可能です。このランサムウェアは、実行パスを定義し、バックグラウンドプロセスとして実行するなど、コマンドラインのカスタマイズオプションを特徴としています。暗号化プロセスは複雑なキーのペア生成を含み、ファイルは攻撃者の介入なしには復号化できないことを保証し、その精巧さと弾力性を強調しています。

**[Attack Flow]**

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. フィッシングメールの添付ファイル
b. マルウェア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: Linux (T1059.004)
a. ELF バイナリの実行
b. コマンドラインオプションの設定
3. [権限昇格] Sudo と Sudo キャッシング (T1548.003)
a. ルート権限の取得試行
b. 権限昇格後のシステムコマンド実行
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. ChaCha20 によるデータ暗号化
b. ECDH キー交換によるキーの隠蔽
5. [認証情報アクセス] 保護されていない認証情報 (T1552)
a. ネットワーク上の認証情報の窃取

b. 暗号化されたストレージへのアクセス

6. [探索] ファイルとディレクトリの探索 (T1083)
   a. ファイルおよびディレクトリ構造の探索
   b. 機密データの識別
7. [横移動] リモートサービス: SSH (T1021.004)
   a. SSH を通じた移動
   b. ネットワーク上の他のシステムへのアクセス
8. [収集] 収集データのアーカイブ: ユーティリティによるアーカイブ (T1560.001)
   a. データの圧縮および保管
   b. 抽出のための準備
9. [流出] C2 チャネルを介した流出 (T1041)
   a. C2 チャネルを通じたデータ流出
   b. 秘密裏の転送
10. [影響] 影響のためのデータ暗号化 (T1486)
    a. ファイルの暗号化
    b. ランサムノートの作成および配布

**6) SectorJ238 used OVERSTEP Rootkit on End-of-Life SonicWall Appliances (2025-07-17)**

https://cti.nshc.net/events/view/16978

財政的動機を持つサイバー脅威行為者が、SonicWall Secure Mobile Access (SMA) 100 シリーズの機器を標的にし、以前の侵入で奪取した資格情報とワンタイムパスワード（OTP）シードを活用して、セキュリティアップデートが適用された後も不正アクセスを再開しています。初期感染ベクターは、Malware がログ項目を削除できるため不明ですが、CVE-2024-38475 のような既知の脆弱性を利用したと考えられます。攻撃者は、システムのブートシーケンス中に自身を注入するバックドアを統合した新しいルートキット「OVERSTEP」を展開し、資格情報を奪取し持続性を維持します。直接的な最終段階の作業は観察されていませんが、今回のキャンペーンはデータ窃盗や恐喝といった過去のランサムウェア活動と一致する戦術を含んでいます。脅威行為者の方法論には、システムログの操作や不正なネットワーク設定の生成が含まれ、カーネル実行のためのソフトリブートメカニズムを活用したと考えられます。今回のキャンペーンは、過去数年間に観察された類似の攻撃の進化である可能性があります。

**[Attack Flow]**

1. [初期アクセス] 有効なアカウント (T1078)
   a. 盗まれた資格情報の使用

b. OTPシードの活用
2. [防御回避] ホスト上のインジケーター削除 (T1070.004)
a. ログ項目の削除
b. ログの操作
3. [持続性] ブートまたはログオン自動開始実行 (T1547.001)
a. システムブートシーケンスにバックドアを注入
b. /etc/ld.so.preloadファイルの追加
4. [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. 資格情報の窃取
b. /etc/EasyAccess/var/conf/persist.dbファイルへのアクセス
5. [実行] コマンドおよびスクリプトインタープリター (T1059)
a. リバースシェルの生成
b. コマンドの実行
6. [探索] システム情報の探索 (T1082)
a. システム情報の収集
b. ファイルの操作
7. [収集] 情報リポジトリからのデータ (T1213)
a. データの窃取
b. 機密情報の収集
8. [影響] データ破壊 (T1485)
a. ログの削除
b. 記録の除去
9. [流出] 代替プロトコルによる流出 (T1048)
a. 異常なネットワーク設定の生成
b. データの流出
10. [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サーバーとの通信
b. バッファ内のコマンド構文解析

## 今月のサイバー脅威の特徴

2025 年 7 月のサイバー脅威活動は、攻撃の精巧化、ソーシャルエンジニアリングに基づく初期アクセスの高度化、サプライチェーンを狙った侵入戦略の多様化、そして公開されたゼロデイ脆弱性の迅速な悪用という 4 つの主要な特徴で要約されます。特に、APT グループとサイバー犯罪グループの

両方が情報窃取と資格情報収集を中心とした侵入目標を維持しつつ、伝播媒体とインフラの活用においてますます複雑性と隠密性を強化する方向で戦術を進化させています。

まず、APT グループはサプライチェーン攻撃とソーシャルエンジニアリング技術を組み合わせた複合戦術を多数実行しました。いくつかの攻撃事例では、ソフトウェア開発エコシステム（npm、PyPI など）を直接狙ったマルウェアパッケージを配布し、この過程で HexEval、XORIndex、NimDoor のような多段階ローダーを活用してバックドアのロードおよび情報の窃取を行いました。彼らは検出回避のために XOR エンコーディング、難読化された命令およびエンコードされたコマンド＆コントロール（C2）チャネルを適用し、コード実行条件を環境に応じて動的に変更するなど、ペイロード配布構造の複雑化を通じて識別を困難にしています。特に開発者のような高価値ターゲットを対象に攻撃を集中させ、資格情報、暗号通貨ウォレットディレクトリ、ブラウザデータのような機密情報を主要な収集対象としていることが確認されました。

フィッシングを基盤とした侵入も活発に行われました。APT グループは、社会工学的な設計が施されたスピアフィッシングメールを通じて、悪意のあるリンクや添付ファイルを配布し、実際の組織名や職位を偽装して攻撃の成功率を高めようとしました。例えば、政府機関や法律事務所を装ったメールを通じて、悪意のある RTF または LNK ファイルを配布し、これを通じて PowerShell や VBScript ベースのスクリプトを実行して初期侵入に成功する方法が一般化しました。これらのペイロードはしばしばタスクスケジューラに登録され、持続性を確保し、キーロギングやスクリーンキャプチャなどの様々な情報窃取活動を行います。コマンド＆コントロール通信（C2）も Dropbox、GitHub、Koofr などの合法的なクラウドサービスを通じて行われ、検出を回避しており、最近では Firebase や Cloudflare Tunnel を利用した暗号化チャネルの構築事例も多く観測されています。

ゼロデイ脆弱性の迅速な悪用も顕著でした。APT グループは、SAP NetWeaver および Ivanti CSA 製品群の高リスク脆弱性を攻撃の初期段階で利用し、ウェブシェルのインストールやバックドアの設置などを通じて外部との持続的な接続を確保しました。この過程で攻撃者は、Mimikatz、Cobalt Strike Beacon、カスタム RAT などのツールを使用してシステムの資格情報をダンプしたり、ネットワークを探索して横方向の移動を試みたりしました。特に SAP 関連の脆弱性（CVE-2025-31324）は、業種を問わず様々な組織に対して大規模に悪用され、攻撃の波及力が非常に大きく、組織全体への深いアクセスを可能にしました。

一方で、サイバー犯罪グループは伝統的な情報窃取や金銭的利益を目的とした攻撃活動を継続しつつ、より巧妙で広範なインフラ活用を通じて運営の高度化を図る傾向を示しました。例えば、SonicWall 機器のような旧型機器を対象としたルートキット配布の事例では、資格情報の窃取とともにシステム起動時を狙った持続性確保の手法が伴い、ログ削除やシステム隠蔽技術を含む多層的な方法を通じて長期的なアクセスを確保しようとしました。

また、サイバー犯罪グループはクラウドサービス、DNS ベースのインフラ、ウェブシェルなどを組み合わせた複合インフラを構築し、多数の伝播経路とコマンド通信経路を柔軟に運用しています。彼らはソーシャルエンジニアリングに基づくフィッシングメールを通じてユーザーのクリックを誘導し、HTML、VBS、PowerShell スクリプトを含む様々な形態の初期ペイロードを実行します。攻撃チ

エーン上では、資格情報の収集、システム情報の窃取、RAT またはランサムウェアのダウンロードといった後続の活動が続き、最終段階ではデータの暗号化および二重恐喝（ダブルエクストーション）を通じて金銭要求を行います。
特に Web3、暗号通貨、ブロックチェーン関連の産業を対象とした攻撃が多数確認されており、macOS や Linux など様々なオペレーティングシステムをターゲットにしたカスタマイズされたペイロードも着実に登場しています。これらは社会的に信頼されている企業やプロジェクトを装ってマルウェアを含むインストールファイルを配布し、情報を盗んだ後には暗号化されたチャンネルを通じてデータを外部に流出させる手法を利用しています。また、証明書を盗用したり、正規のソフトウェアの実行ファイルを悪用することでユーザーの信頼を確保しようとする戦略も併用されています。
要約すると、7 月の 1 か月間、APT グループは情報収集を中心とした国家支援型スパイ活動に集中し、サプライチェーンを利用した侵入とソーシャルエンジニアリング手法を組み合わせた複合侵入を行いました。一方、サイバー犯罪グループは金銭の窃取と資格情報の収集を目的に、暗号通貨・IT サービス・金融をターゲットにした攻撃を強化しました。全体的に攻撃者は、検出回避と持続性の確保に非常に重点を置いており、オペレーティングシステム、プラットフォーム、クラウドサービスなど多様な環境に対する攻撃技術を精巧化していると分析されています。

## 今月のサイバー脅威の示唆点

2025 年 7 月に観測されたさまざまなサイバー脅威活動は、従来の攻撃手法の繰り返しではなく、複合化・精巧化・多様化された攻撃戦略が本格的に現実化していることを示唆しています。APT グループとサイバー犯罪グループの両方が明確な目標を設定しており、侵入後に迅速な情報収集と資格情報の窃取、持続性確保のための技術的装置を同時に駆使しています。これは、過去の一回性の侵入中心の攻撃から脱却し、長期的なアプローチと偵察、多段階の運用に焦点を当てた体系的な侵入活動に転換されたことを意味します。
最も目立つ示唆の一つは、サプライチェーンエコシステムに対する攻撃の試みが APT グループを中心により体系化されている点です。攻撃者は単に被害者のネットワークに侵入するだけでなく、開発者エコシステム（npm、GitHub など）内の人気パッケージや類似パッケージを汚染して伝播経路を確保します。この過程で、マルウェアローダーは静的分析を回避できるように構造的に設計され、様々な難読化およびエンコーディング技術を適用して検出を困難にします。攻撃者は特定の産業群または専門技術を持つユーザーを標的にし、インフラ全体への侵入可能性を確保した後、長期的に資格情報、暗号通貨ウォレット、開発環境情報などを収集します。このように、サプライチェーンに基づく攻撃は単一組織のセキュリティレベルを超えた脅威であり、セキュリティ体制全般の再点検の必要性を浮き彫りにします。

2 番目に、ソーシャルエンジニアリングに基づく侵入方法は依然として攻撃の初期段階で効果的に活用されており、その進化速度も非常に速いです。APT グループとサイバー犯罪グループの両方が、メール、メッセンジャー、SNS プラットフォームを通じてなりすましメッセージを送信し、外見上正常なファイルやリンクに偽装したフィッシング攻撃を行います。攻撃者は、メール署名、送信者情報、添付ファイル名、アイコンなどすべての視覚的要素を実際の組織の形式に近づけて操作し、受信者の疑念を最小限に抑えます。特に生成型 AI を活用して自然な文章を構成したり、画像ベースの添付ファイルを作成することで、ユーザーの注意を引きつけると同時にマルウェアの実行を誘導する方法が顕著でした。これらの戦術は攻撃成功率を高める主要な要素として作用し、人間のセキュリティ脆弱性を継続的に試すツールとして活用されています。

3 番目に注目すべき点は、公開されたゼロデイ脆弱性が APT グループの侵入経路として迅速に吸収されている点です。SAP NetWeaver や Ivanti CSA のような高リスクアプリケーションの脆弱性は、パッチが公開される前から Proof-of-Concept（PoC）と共に流通しており、これにより組織の対応余裕が著しく減少する結果を招いています。攻撃者は該当の脆弱性を利用して初期ウェブシェルをインストールした後、CobaltStrike Beacon やカスタム RAT などをロードし、内部ネットワークの探索および横方向の移動を行います。特にウェブベースの業務環境が増加する中で、このようなパッチ未適用システムは外部露出点として即座に悪用される可能性があるため、継続的な脆弱性管理とパッチポリシーの現実化が求められます。

サイバー犯罪グループの活動からも重要な示唆が得られます。彼らは金銭的利益を目的としながらも、APT グループに劣らない精巧な技術を駆使しています。特にルートキットの配布、カーネルレベルの侵入、資格情報の窃取後の持続性確保など、高度な技術を連続的に活用し、パッチが適用されたシステムでさえも以前の侵入を基に再侵入する場合があります。SonicWall 機器を狙った攻撃では、過去に窃取した OTP シードを通じて認証を回避し、システム起動時に自動実行されるバックドアをインストールして長期的な制御を狙ったことがあります。このような攻撃は単なるランサムウェア感染を超え、侵入基盤構築後の知能的活動により近づいており、そのため従来の対応体制では検出・遮断に限界が生じています。

情報漏洩経路の分散化もまた一つの示唆点です。攻撃者は合法的なインフラ（GitHub、Dropbox、Firebase など）を悪用したり、Cloudflare Tunnel、fast-flux DNS、Telegram API などのサービス型インフラを通じてコマンド＆コントロールチャネル（C2）を構築します。また、情報流出技術も HTTP POST、SFTP、WebSocket、IPFS、暗号化された WebShell などの様々な手段で並列化されています。これは侵害検出においてネットワークベースの検出の効果を急激に低下させる要因として作用し、異常行動検出に基づく行動中心のセキュリティ体制の確立が急務であることを再確認させます。

一方、macOS や Linux などの非 Windows 環境をターゲットにしたカスタマイズされたペイロードの増加も意味のある変化です。Nim、Rust、C++などさまざまな言語で開発された Malware は、オペレーティングシステムごとの機能の違いを考慮して作成され、システムリソースにアクセスするための高度な権限昇格技術を含む場合が多いです。これは特定の産業分野でオペレーティングシステム

の多様化が進むにつれ、攻撃者もそれを認識し、戦術を細分化していることを示しています。実際に、ELF ランサムウェアや macOS ベースの Infostealer が多数発見されており、プラットフォームベースのセキュリティポリシーの強化が求められています。

全体的に今月のサイバー脅威活動は、APT グループとサイバー犯罪グループの両方が、従来の攻撃手法の繰り返しではなく、さまざまな環境に適した高度な戦略を実行していることを示しています。特に、初期アクセス後の活動が多段階化しており、攻撃の速度と精密度が共に増加しています。これは、各組織が単純なセキュリティソリューションの導入だけでは不十分であり、侵害仮定に基づくセキュリティ運用体制の構築、脅威に基づく検出技術の高度化、攻撃面の最小化を目的としたアーキテクチャの再構築など、本質的な改善が並行して行われる必要があることを示唆しています。何よりも、技術的な対応を超えた組織全体のセキュリティ意識の向上と、サプライチェーン全体にわたる連携的なセキュリティ管理体制が切実に求められる時期です。

## 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)

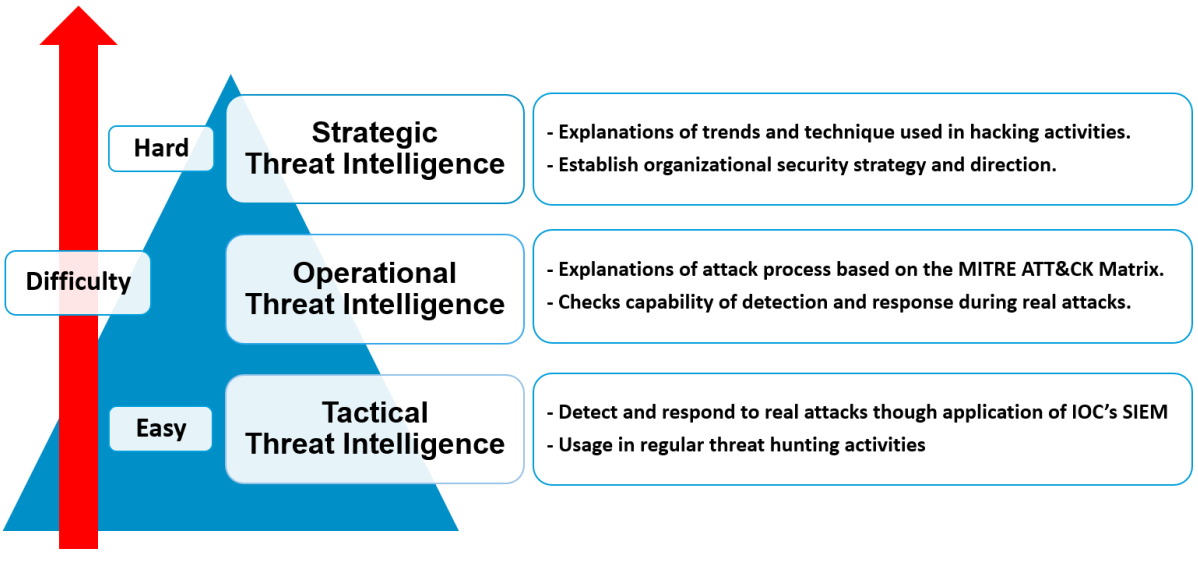
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

- 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

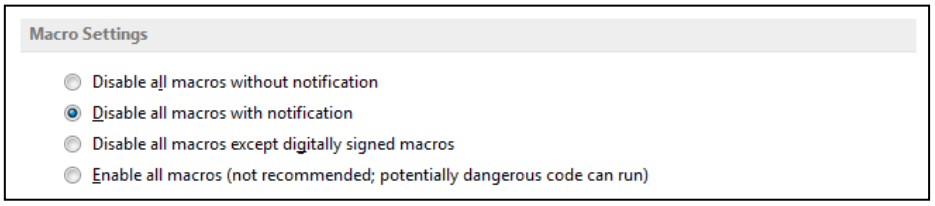
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

### 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.