NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI2025090204

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

Sep 2025

NSHC PTE. LTD.

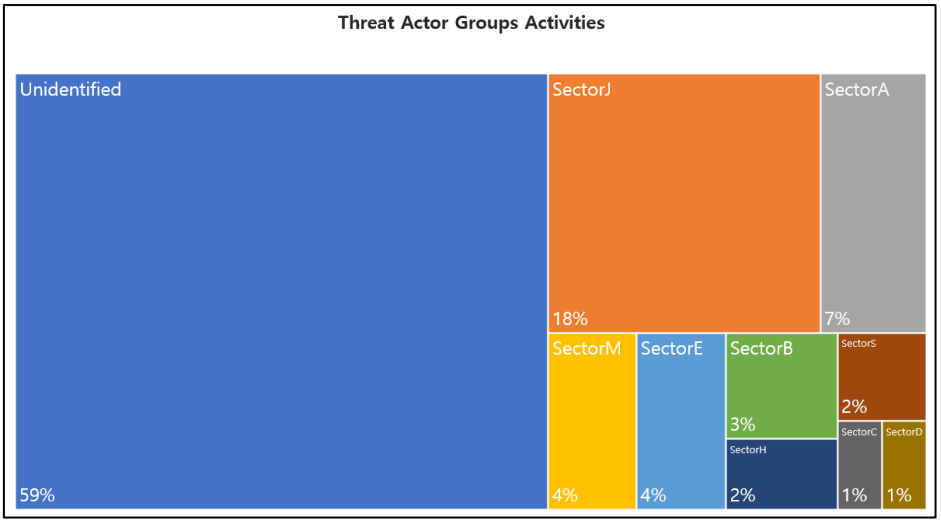
このレポートは 2025 年 7 月 21 日から 2025 年 8 月 20 日まで見つけた政府支援のハッキンググループ活動と関係あるイッシューを説明し、それに伴う侵害事故の情報と ThreatRecon Platform 内のイベント情報を含む。

Table of Contents

エグゼクティブサマリー

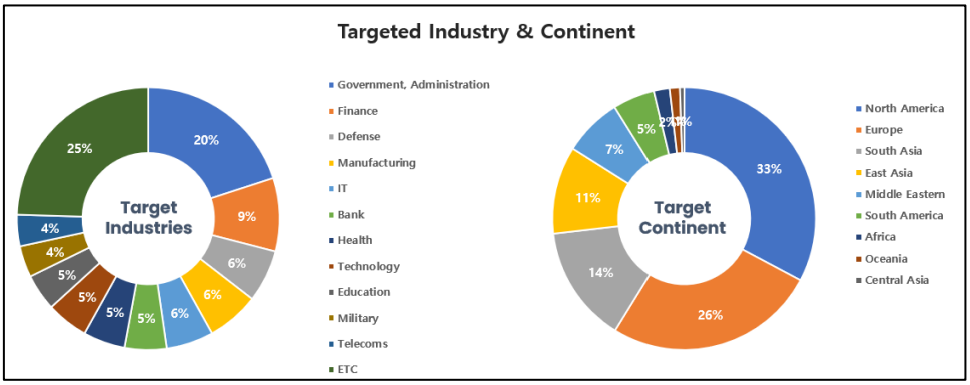
2025 年 7 月 21 日から 2025 年 8 月 20 日までの間に、NSHC 脅威分析研究所（Threat Research Lab）が収集したデータと情報に基づいて分析したハッキンググループ（Threat Actor Group）の活動を要約した内容です。

今月 8 月には合計 75 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 8 月に確認されたハッキンググループ別活動統計]

今年 8 月に発見されたハッキンググループのハッキング活動は、政府機関および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 8 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、金融および暗号通貨分野を主なターゲットとし、ファイルレス攻撃、悪性 LNK ファイル、ソフトウェアパッケージの悪用などを使用しています。「Contagious Interview」キャンペーンでは、BeaverTail、InvisibleFerret、OtterCookie などのさまざまなペイロードを配布し、Vercel.App ベースの C2 活動と eval 関数を利用したコード実行が顕著です。PyLangGhost RAT は、偽のインタビューを通じたソーシャルエンジニアリング攻撃と ClickFix 手法を組み合わせて、資格情報と暗号通貨ウォレットを盗みます。また、RokRAT はメモリベースのファイルレス構造とプロセスホローイングを活用して検出を回避し、外交任務対象のスピアフィッシングでは GitHub、Dropbox を C2 として活用します。

SectorB グループは、政府の IT、金融、通信、メディア分野を標的にし、Impacket モジュール、DLL サイドローディング、Cobalt Strike の実行などの高度な技法を駆使しています。SMB プロトコルを通じたマルウェアツールの転送、署名スプーフィング、画像ステガノグラフィを基にしたシェルコードの挿入などが活用され、GodRAT、AsyncRAT、CuVn などの様々な RAT が使用されました。SharePoint サーバーの脆弱性の悪用、SSH ブルートフォース攻撃、DirtyCoW・PwnKit を基にした権限昇格、FireWood 亜種 Linux バックドアの配布などのネットワーク拡張戦略が確認されています。

SectorC グループは、外交・軍事分野を狙って ApolloShadow、Kazuar、Capibar といったカスタムマルウェアを配布し、ネットワーク中間者攻撃とルート証明書のインストールによって長期的な侵入を維持しています。ウクライナ政府・防衛産業を対象としたキャンペーンでは、短縮 URL と VBScript・PowerShell ベースの攻撃が使用され、NATO 加盟国を対象としては、盗用された資格情報とタイポスクワッティングドメインが組み合わされました。Cisco IOS の脆弱性を悪用したグローバルなスパイ活動も検出され、SYNful Knock ファームウェアインプラントと GRE トンネルを通じたトラフィックキャプチャ技術が動員されました。

SectorD グループはスパイ活動を中心に、Android 監視ツール、PowerShell ベースの RAT、カスタムフィッシングキャンペーンを実施しました。Telegram、Firebase、VPN に偽装した配布が活用され、グローバルな金融幹部を対象としたスピアフィッシングでは、Rothschild & Co のリクルーターに偽装して NetBird、OpenSSH のインストールを誘導しました。彼らは難読化された PowerShell、ZIP・VBS ベースの配信チェーン、IP 変更およびインフラ再利用によって検出を回避します。

SectorE グループは、トルコの防衛産業、南アジアおよび中東の政府機関を対象に、ソーシャルエンジニアリングと LNK、DLL サイドローディングを活用しています。Netlify や Pages.dev を基盤とした偽のログインページが使用されており、複数のドメインを通じた資格情報の収集が確認されました。長期間にわたる攻撃は、持続性と政治的動機を同時に示しています。

SectorF グループは外交・貿易戦略の情報収集に集中しています。2025 年初頭、中国の第 15 次 5 カ年計画と中国・アフリカ協力を狙って、悪意のある LNK 添付ファイルを用いたフィッシングキャンペーンを展開し、精巧に設計されたマルウェアで貿易戦略に関する情報を収集しようとしました。

SectorH グループは、インド政府部門を対象に、.desktop ファイルを利用したフィッシング、cron ジョブを通じた持続性、Mythic フレームワークに基づく Poseidon バックドアなどを使用しました

。単一および二重の C2 インフラを運営し、ほとんどの場合、Alexhost インフラを基盤として中央制御を維持しています。
SectorT は、ウクライナとポーランドを標的としたスピアフィッシング XLS 文書とマクロベースの攻撃が中心です。LNK・DLL の実行、MacroPack による難読化、クラウドコラボレーションツールへの偽装、Slack ベースの C2 など、カスタマイズされたアプローチが特徴であり、各国ごとに異なる感染チェーンを用いながらも、一貫した戦略を維持しています。
SectorJ グループは、Trojan.Updatar シリーズ、Meterpreter、RDP ベースの横移動を通じて政府・企業インフラを掌握します。RockYou パスワードリストの難読化、Linux・macOS・Windows の同時攻撃、Steam・WinRAR の脆弱性の悪用などで活動を拡大しています。AES、ChaCha-20 暗号化に基づく C2 通信が適用され、データの窃取と監視活動に集中しています。

詳細情報

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

1) SectorA01 used Eval Function in New Payload Delivery Techniques (2025-07-30)
https://cti.nshc.net/events/view/17402

「Contagious Interview」キャンペーンは、ペイロード配信メカニズムにおいてかなりの進展を示し、迅速に検出を回避しています。BeaverTail、InvisibleFerret、OtterCookie として識別された主要なペイロードは、革新的な技術を通じて配信されます。最初の方法は、外部ソースから POST リクエストを通じてコードを取得し、eval()関数を使用して実行することで、直接的なコード挿入を避け、従来のスキャニングツールを回避します。第二に、攻撃者は断片化された URL や Vercel.App のような合法的なプラットフォームを C2 サーバーとして活用し、コード分析と静的検出フレームワークを複雑にします。また、try/catch メカニズムを導入し、eval 関数をエラーハンドリング技法で置き換えてペイロードを実行し、検出の可能性をさらに減少させました。これらの技術の洗練に注力するグループは、AI を通じたコード自動化に依存し続けており、これはパターン認識にのみ依存する既存の検出方法に課題を提起し、強化された防御戦略の必要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. マルウェアペイロードを含むメール送信
   b. ユーザーがメールの添付ファイルをダウンロードして実行
2. [実行] コマンドとスクリプトインタープリタ: JavaScript (T1059.007)
   a. 外部アドレスへの POST リクエストを実行

b. eval()関数を通じたコード実行

3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. URL の断片化と合法的なプラットフォームの活用
   b. コードの try/catch ブロックの使用
4. [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. Vercel.App を C2 サーバーとして活用
   b. 通信アドレスの分割と URL 結合方式の活用
5. [影響] データ操作 (T1565)
   a. API 通信を通じて 500 エラーを返す
   b. エラー処理関数でマルウェアを受信して実行

2) SectorA01 used Script Malware disguised as interview exercises (2025-07-31)

https://cti.nshc.net/events/view/17474

北朝鮮の精巧なキャンペーンは、開発者を対象にマルウェアソフトウェアパッケージを配布し、暗号通貨や機密情報を窃取しました。12 個のマルウェアパッケージは、合法的なオープンソースソフトウェアに偽装されて発見されました。これらのパッケージには、クラウド-バイナリ、ジェイソン-クッキー-CSV、クラウドメディア、ノードメーラー-エンハンサーが含まれており、難読化技術と暗号化されたペイロードを使用し、頻繁に再利用される C2 インフラを活用しました。マルウェアは、テスト駆動開発（TDD）実践を悪用し、開発者インタビュー中に単体テストが実行される際に動作して開発者を欺きました。主要な手法の一つは、合法的なパッケージのスペルミスを利用してユーザーを欺くことでした。マルウェアの技術的特徴には、システム情報の列挙、暗号ウォレットおよび機密ファイルの漏洩、WebSocket を介した任意のコマンド実行が含まれていました。Beavertail マルウェアの亜種は、主要なオペレーティングシステム全体で能力を拡張しました。

[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. インタビュー課題中にマルウェア実行
   b. テスト駆動開発(TDD)演習の悪用
2. [実行] コマンドおよびスクリプトインタープリター: JavaScript (T1059.007)
   a. JavaScript ファイルを通じたマルウェア実行
   b. 暗号化されたペイロードを復号化後、eval で実行
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. postinstall フックを使用した持続性確保
   b. 2 段階ペイロードのダウンロード試行

4. [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 の使用
   b. AES-256 でペイロードを暗号化
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. システム情報およびユーザー名の列挙
   b. macOS キーチェーンから秘密ファイルの流出試行
6. [探索] システム情報探索 (T1082)
   a. オペレーティングシステムおよびプラットフォーム情報の収集
   b. 暗号ウォレットおよびブラウザー拡張の検索
7. [収集] ローカルシステムからのデータ (T1005)
   a. Word、PDF、スクリーンショット、環境変数ファイルなどの機密ファイルの検索および流出
   b. ログイン中のユーザーの秘密ファイル収集試行
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: WebSocket (T1071.001)
   a. WebSocket を通じた任意のシェルコマンド実行
   b. C2 サーバーとの通信のための多様な IP アドレス使用
9. [流出] 代替プロトコルによる流出 (T1048)
   a. バックアップ C2 サーバーへの流出資料のアップロード
   b. キャンペーン成功の追跡のためのクライアント識別子使用
10. [影響] データ操作 (T1565)
    a. 開発者のコンピューターからの秘密情報の窃取
    b. 暗号通貨の窃取を通じた制裁国への資金調達試行

3) SectorA01 used Python Malware disguised as camera fix script (2025-08-06)

https://cti.nshc.net/events/view/17533

攻撃対象産業群: 金融、技術

北朝鮮の国家支援攻撃者は、金融および暗号通貨部門を標的に、新しい Python ベースの Malware である PyLangGhost RAT を使用して攻撃を実行しました。この脅威は、偽の就職面接のような高度なソーシャルエンジニアリング戦術を利用して、技術、金融、暗号通貨業界の従業員を騙し、システムで悪意のあるスクリプトを実行させました。スクリプトは攻撃者にリモートアクセスを許可し、「ClickFix」という技術を通じて配布されました。被害者は偽の技術的問題を解決するために、コマンドをターミナルに貼り付けるように誤誘導されました。PyLangGhost RAT のローダーである nvidia.py は、コマンド実行、データ漏洩、回避のための複数のモジュールと共に動作し、主にブラウザに保存された資格情報と暗号通貨ウォレットデータを盗むことに重点を置いていました。この Malware は暗号化されていないチャネルを通じて C2 サーバーと通信し、弱い暗号化を使用してデータ転送を行い、検出を困難にしました。この Malware は以前の Go ベースの RAT の Python 完全実

装版と見られ、開発は AI の助けを受けた可能性があります。複雑な方法と低い検出率は、金融損失およびデータ漏洩といった深刻なリスクを引き起こしました。

[Attack Flow]

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
   a. 偽の就職面接を利用したソーシャルエンジニアリング
   b. ClickFix 技術を通じた悪性コマンド実行誘導
2. [実行] コマンドとスクリプトインタープリタ: Python (T1059.006)
   a. nvidia.py ローダー実行
   b. 悪性スクリプトを通じたリモートアクセス許可
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. レジストリキー登録
   b. UUID を通じた固有識別子割り当て
4. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. ブラウザに保存された資格情報の窃取
   b. 暗号通貨ウォレットデータの窃取
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 弱い RC4/MD5 暗号化を通じたデータ送信
   b. csshost.exe を通じたファイル名偽装
6. [収集] 情報リポジトリからのデータ (T1213)
   a. Chrome 拡張プログラムの設定データ収集
   b. ユーザープロファイルディレクトリの探索と圧縮
7. [流出] 暗号化されていない/難読化された非 C2 プロトコルを通じた流出 (T1048)
   a. RC4 暗号化を使用したデータ送信
   b. 暗号化されていないチャネルを通じた C2 サーバーとの通信
8. [コマンドとコントロール] 非アプリケーション層プロトコル (T1095)
   a. 生の IP アドレスを通じた C2 サーバー通信
   b. 継続的な C2 サーバーコマンドの受信と実行

4) SectorA01 used Malware disguised as Web3 Interview Projects (2025-08-12)

https://cti.nshc.net/events/view/17733

攻撃者は 2025 年 8 月 9 日、ウクライナの Web3 チームを装って、ある個人を GitHub リポジトリである EvaCodes-Community/UltraX を複製するよう誘導しました。このリポジトリには、以前に削除されたマルウェアパッケージ redux-ace@1.0.3 を置き換えたマルウェア NPM パッケージ rtk-logger@1.11.5 が含まれていました。このパッケージには、暗号通貨ウォレットファイルや

Chrome、Brave、Opera、Firefox などのブラウザのユーザーデータを収集し、攻撃者のサーバーにアップロードするコードが含まれていました。AES-256-CBC 復号化をハードコーディングされたキーと共に使用して難読化されたコードを解除しました。パッケージは、構成とウォレットデータを含む主要なファイルを窃取の対象としました。また、環境データを監視および分析するさまざまな機能を実行し、攻撃者制御サーバーとコマンド実行のために相互作用しました。追加の分析の結果、リポジトリフォークも元のマルウェアパッケージを使用してデータ漏洩の潜在的可能性を高めました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング (T1566)
   a. GitHub リポジトリ EvaCodes-Community/UltraX の複製を誘導
   b. 面接過程で個人を欺く
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
   a. パッケージ rtk-logger@1.11.5 の実行
   b. LICENSE ファイルの読み取りおよびコード実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. AES-256-CBC 復号化の使用
   b. 難読化されたコードの解除
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. ブラウザに保存されたログインデータの窃取
   b. キーチェーンからのパスワードおよび証明書の盗難
5. [収集] ローカルシステムからのデータ (T1005)
   a. ブラウザおよび暗号通貨ウォレットデータの収集
   b. 構成ファイルのスキャンおよび収集
6. [流出] C2 チャネルを介した流出 (T1041)
   a. 攻撃者サーバーへのデータアップロード
   b. 144[.]172[.]112[.]106 への送信
7. [コマンドと制御] アプリケーション層プロトコル (T1071)
   a. サーバーとのコマンドメッセージの受信および実行
   b. システム情報の報告およびコマンド実行
8. [影響] データ操作 (T1565)
   a. ファイルのダウンロードおよび実行
   b. キーロギング、画面キャプチャおよびクリップボードの監視の実行

5) SectorA02 used RoKRAT Malware (2025-08-04)

https://cti.nshc.net/events/view/17485

北朝鮮と関連があると推定されるハッキンググループが、高度に精巧で多層的な攻撃方法を使用してRokRAT マルウェアを配布しました。攻撃は「National Intelligence and Counter-espionage Manuscript.zip」といったターゲットの関心を引く名前の ZIP ファイルから始まります。ユーザーがこのファイルを解凍すると、通常のドキュメントアイコンに偽装された.lnk ファイルが現れます。この LNK ファイルは異常に大きなサイズで、悪意のある PowerShell スクリプトと多段階に暗号化されたシェルコードを秘密裏に含んでいます。ユーザーが LNK ファイルを実行すると、暗号化された最初の段階のシェルコードをメモリ上で XOR 演算を通じて解読し、実行可能にします。その後、Paint(mspaint.exe)プログラムを実行し、「Process Hollowing」技法を使用して Paint プロセスのメモリ空間に侵入し、第二の暗号化されたペイロードを秘密裏に注入します。Paint プロセスのメモリに成功裏に注入されたデータは、さらに別の XOR 解読を経て、最終攻撃ペイロードである RokRAT マルウェアを明らかにします。このすべての過程はシステムメモリ内でのみ展開され、ハードドライブにファイルを生成せず、従来のファイルベースのアンチウイルスプログラムでは検出が困難です。システムに対する完全な制御権を獲得した後、RokRAT は重要なシステム情報とユーザーファイルのリストを収集します。収集されたデータは、Dropbox や pCloud のような合法的なクラウドサービスを通じて攻撃者のサーバーに流出し、ネットワークレベルの監視を避けるために通常のユーザーファイルアップロード活動に偽装します。

[Attack Flow]

1. [初期アクセス] フィッシング: スピアフィッシング添付ファイル (T1566.001)
   a. 関心を引くためのファイル名を使用
   b. ZIP ファイル内に LNK ファイルを含む
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. LNK ファイルの実行
   b. PowerShell スクリプトの呼び出し
3. [防御回避] 偽装: 正当な名前または場所に一致 (T1036.005)
   a. ドキュメントアイコンに偽装
   b. プロセスホローイング技法の使用
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. XOR 演算による暗号化
   b. メモリベースのファイルレス攻撃
5. [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. シェルコードをメモリで復号および実行
6. [防御回避] プロセスインジェクション (T1055)
   a. Paint プロセスにペイロードを注入
   b. 正常なプロセスに偽装

7. [収集] ローカルシステムからのデータ (T1005)
   a. システム情報の収集
   b. ユーザーファイルリストの収集
8. [流出] Web サービスを介した流出: クラウドストレージへの流出 (T1567.002)
   a. クラウドサービスを使用してデータを流出
   b. 正常なファイルアップロード活動に偽装

6) SectorA02 uses malware to conduct information theft and ransomware attacks against South Korean users (2025-08-08)

https://cti.nshc.net/events/view/17649

北朝鮮の APT グループは「郵便番号更新通知」に偽装した新しいマルウェアキャンペーンを展開しました。攻撃は圧縮されたアーカイブ内に含まれるマルウェアショートカット（LNK）ファイルから始まりました。ユーザーがこれを実行すると、スクリプトが追加のマルウェアをダウンロードするようにトリガーされました。主な特徴は、合法的なリアルタイムメッセージングサービスである「PubNub」の API を C2（コマンドアンドコントロール）チャネルとして使用し、悪意のあるトラフィックを隠し、検出を回避することです。攻撃には 9 種類以上のさまざまなタイプのマルウェアが使用されました。「NubSpy」バックドアは AutoIt および PowerShell で作成され、PubNub を通じてコマンドを受信しました。情報窃取マルウェア「LightPeek」と「FadeStealer」は、ファイルリスト、スクリーンショット、キー入力、オーディオ録音などのデータを収集しました。特に、以前は PowerShell スクリプトでのみ確認されていた「CHILLYCHINO」バックドアが検出を回避するために新たに Rust 言語に移植され、特定のディレクトリを対象としたカスタム「VCD ランサムウェア」も使用されました。

[図 3: SectorA02 グループが悪用した HTML ファイル]

[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. 「郵便番号更新通知」に偽装
   b. LNK ファイルを含む圧縮アーカイブ
2. [実行] ユーザー実行 (T1204.002)
   a. ユーザーが LNK ファイルを実行
   b. スクリプトトリガー
3. [防御回避] 偽装 (T1036)
   a. 正当なサービスである「PubNub」を使用
   b. C2 トラフィックを隠す
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. PubNub API を C2 チャネルとして使用
   b. コマンドの受信および送信
5. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. NubSpy バックドアの持続性
   b. システム再起動後に自動実行

6. [収集] 入力キャプチャ (T1056)
   a. キー入力およびスクリーンショットの収集
   b. オーディオ録音
7. [データ流出] C2 チャネルを介した流出 (T1041)
   a. 収集されたデータの送信
   b. PubNub を通じて送信
8. [影響] 影響のためのデータ暗号化 (T1486)
   a. VCD ランサムウェアの使用
   b. 特定のディレクトリをターゲットにする

7) SectorA02 used RokRAT Malware disguised as a Grain Sales Report (2025-08-11)
https://cti.nshc.net/events/view/17622

悪性 HWP ファイル「250615_양곡판매소 운영 현황.hwp」が北朝鮮関連の業務や研究に従事する個人を対象に配布されました。このファイルは北朝鮮平壌の穀物配分に関する文書に偽装してユーザーを誘引しました。文書を開くと、外部 URL に接続するハイパーリンクが含まれており、「ShellRunas.exe」プログラムの実行を警告するメッセージが表示されます。このプログラムは文書内の OLE オブジェクトとして挿入されており、実行時にマルウェア感染が進行します。また、文書には「credui.dll」をシステムの TEMP ディレクトリに挿入する別の OLE オブジェクトも含まれています。これらの技術は、関心を引くための本物のようなテーマを利用してマルウェアを密かに配布する方法です。

[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. マルウェア HWP ファイル配布
   b. 北朝鮮研究文書に偽装
2. [実行] ユーザー実行 (T1204)
   a. 文書閲覧時にハイパーリンククリック誘導
   b. ShellRunas.exe 実行警告メッセージ表示
3. [持続性] スケジュールされたタスク/ジョブ (T1053)
   a. ShellRunas.exe OLE オブジェクト挿入
   b. credui.dll OLE オブジェクト挿入
4. [防御回避] 偽装 (T1036)
   a. 正常な文書に偽装
   b. TEMP ディレクトリにファイル作成
5. [コマンド＆コントロール] 標準アプリケーション層プロトコル (T1071)

a. 外部 URL への接続
b. C2 サーバーとの通信試行

8) SectorA03 used Malware disguised as Input Method Installer (2025-07-23)
https://cti.nshc.net/events/view/17184

攻撃者は 2024 年 10 月から「hana9.30_x64_9.exe」という実行ファイルを通じて攻撃を開始しました。このファイルは北朝鮮の入力プログラムのインストーラーであることが確認されており、6 月には感染したユーザー数が急増しました。また、「winrar-x64-540.exe」という新しい Malware が登場しました。この Malware は Baidu Disk、WeChat、USB ドライブを通じてユーザーシステムに侵入し、最近数年間頻繁に使用されている DarkSeal という 2 段階ペイロードを配布します。攻撃は Malware インストールインターフェースがインストーラーおよびペイロードを抽出して実行し、正当なファイルをスタートアッププログラムとしてコピーし、スケジュールされたタスクを通じて持続性を確立することから始まります。dllhost.exe プロセスを生成してシェルコードを注入し、正常なプログラムを Malware インストーラーに置き換えます。DarkSeal は DLL ハイジャックを通じて正当なプロセスを介して実行され、追加のペイロード、主に Meterpreter や Thinmon コンポーネントを復号化してロードします。Malware はハードコーディングされたキーを使用して復号化し、シェルコードを実行して主機能を含む PE ファイルを反射的にロードします。攻撃は通常、初期アクセス、機能的中間段階、数年間 DarkSeal を最終ペイロードとして継続的に使用する段階を含みます。現在の活動は攻撃者の目標が単純化され、最初の 2 つのペイロード段階のみを含みます。

[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. Baidu Disk、WeChat、USB ドライブを通じた初期アクセス
   b. マルウェアインストールインターフェースの実行
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. インストールプログラムおよびペイロードの抽出と実行
   b. dllhost.exe プロセスの生成とシェルコードの注入
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. 正当なファイルをスタートアッププログラムとしてコピー
   b. スケジュールされたタスクを通じた持続性の確立
4. [防御回避] DLL 検索順序ハイジャック (T1574.001)
   a. DLL ハイジャックを通じた正当なプロセスの使用
   b. Meterpreter または Thinmon ペイロードの復号化とロード
5. [コマンドとコントロール] 暗号化チャネル (T1573)
   a. ハードコーディングされたキーを通じたファイルの復号化

b. シェルコードを通じた PE ファイルの反射ロード
6. [影響] データ操作 (T1565)
a. 攻撃者の目標に応じたペイロードステージの調整
b. DarkSeal を最終ペイロードとして継続的に使用

9) SectorA05 used LNK Malware disguised as Security Email (2025-07-22)

https://cti.nshc.net/events/view/17238

2025 年 7 月に悪意のある LNK ファイルがクレジットカード会社のセキュアなメール認証画面に偽装して配布されました。これらのファイルはユーザー情報を盗むために配布されました。以前は PowerShell スクリプトを利用してキーロギングや情報窃取を行っていましたが、今回の攻撃では DLL ファイルをダウンロードしてこれらの作業を行いました。LNK ファイルが実行されると、HTA ファイルとデコイ HTML ドキュメントをダウンロードしてユーザーを混乱させます。HTA ファイルは悪意のある DLL（sys.dll）とダウンロード URL が含まれたテキストファイルを生成し、3 つの DLL ファイル（app、net、notepad.log）をダウンロードします。これらの DLL ファイルはリフレクティブローディング技法を使用しているため、検出が困難です。これらのファイルは Chrome、Edge、Firefox などのウェブブラウザを対象にクレデンシャル窃取を行い、「notepad.log」はバックドアとしてリモートシェルコマンドの実行やファイル流出を可能にします。これらの巧妙な LNK ファイルは信頼できる機関を模倣してユーザーを欺き、実行されるように仕向けています。

[Attack Flow]

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
a. クレジットカード会社のセキュリティメール認証画面に偽装
b. マルウェア LNK ファイル配布
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
a. LNK ファイル実行後、HTA ファイルとデコイ HTML ドキュメントをダウンロード
b. HTA ファイル実行でマルウェア DLL(sys.dll)とテキストファイル生成
3. [防御回避] リフレクティブ DLL インジェクション (T1620)
a. リフレクティブローディングで DLL ファイル検出回避
b. app、net、notepad.log DLL ファイルをメモリ内で直接実行
4. [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. Chrome、Edge、Firefox ブラウザ情報の窃取
b. オンラインサービスのクレデンシャル窃取
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)

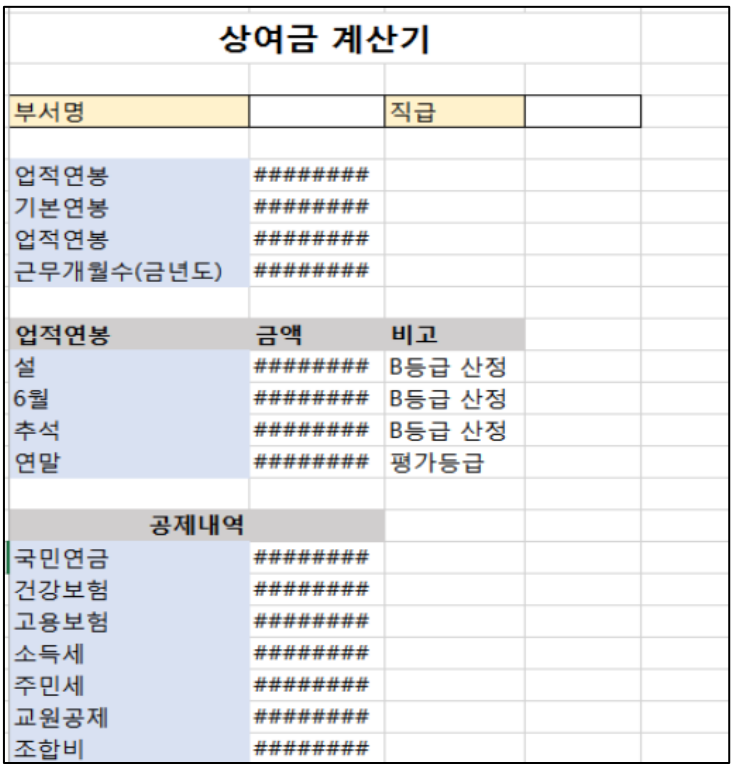
a. notepad.log ファイルを通じたリモートシェルコマンド実行
b. ファイルのダウンロードおよび流出の実行
6. [収集] キーロギング (T1056.001)
a. キーロギングデータの収集
b. C:¥Users¥{ユーザー名}¥AppData¥Local¥netkey パスに保存

10) SectorA05 used Malware disguised as Bonus Calculation Excel (2025-07-25)

https://cti.nshc.net/events/view/17242

攻撃対象産業群: 市民

「상여금처리산식.xls」という名前のマルウェア Excel ファイルが 2022 年 11 月にマクロベースの手法を使用して配布されました。このファイルはボーナス計算を助けるふりをしながら、悪意のあるマクロを隠しており、主に韓国のユーザーを対象としていました。マクロは Windows レジストリの定数を定義し、API 宣言を通じてシステム設定を変更し、レジストリを活用して持続性を確保しました。Excel シート内の特定のセルから動的 URL を抽出し、cmd.exe を通じたカスタムコマンドでリモートサーバーから実行ファイルをダウンロードしました。コマンド構造を操作してコマンドエラーを回避しました。ファイルはダウンロードした実行ファイルが既に存在するかを確認し、存在しない場合はシステムの一時ディレクトリにダウンロードし、ユーザーインターフェースに最小限の妨害を与えるようにしました。ダウンロードされたファイルはその後実行されました。このようなマクロベースの攻撃は 2023 年以降減少しましたが、北朝鮮を含む一部の国家支援アクターが様々な対象を無差別に攻撃しているため、継続的な警戒が求められます。



상여금 계산기

부서명		직급	
업적연봉	########		
기본연봉	########		
업적연봉	########		
근무개월수(금년도)	########		
업적연봉	금액	비고	
설	########	B등급 산정	
6월	########	B등급 산정	
추석	########	B등급 산정	
연말	########	평가등급	
공제내역			
국민연금	########		
건강보험	########		
고용보험	########		
소득세	########		
주민세	########		
교원공제	########		
조합비	########		

[図 4: SectorA05 グループが使用したマルウェア文書]

[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. マルウェアの Excel ファイル添付
   b. ボーナス計算を装って誘引
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. マクロ実行
   b. ユーザー実行誘導
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. レジストリ定数定義
   b. API 宣言使用
4. [防御回避] 偽装: 正当な名前または場所に一致 (T1036.005)
   a. 正常なファイルに偽装
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: Web プロトコル (T1071.001)
   a. 動的 URL 抽出
   b. cmd.exe を通じたコマンド実行
6. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. コマンド構造操作
   b. コマンドエラー回避
7. [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. curl を使用してファイルダウンロード
b. 一時ディレクトリにファイル保存
8. [実行] ネイティブ API (T1106)
a. ダウンロードされたファイル実行
b. システム内実行保証
9. [防御回避] ホスト上のインジケータ削除: ファイル削除 (T1070.004)
a. ダウンロードされたファイル実行後削除
b. 痕跡除去試行

11) SectorA05 used LNK Malware disguised as government notices (2025-08-11)

https://cti.nshc.net/events/view/17620

攻撃対象産業群: 政府・行政、防衛

北朝鮮政府が支援するサイバー諜報キャンペーンが、体系的に韓国の機関を標的にしました。この攻撃は、Windows ショートカット（LNK）ファイルを初期攻撃ベクターとして使用しました。キャンペーンの背後にいるグループは、カスタマイズされたソーシャルエンジニアリング技術と高度な Malware フレームワークを活用してアクセスを確保し、持続性を維持しました。攻撃は、信頼できるシステムユーティリティが悪意のある LNK ファイルから難読化されたスクリプトを実行することで開始されました。これは、韓国政府の通知を模倣した資料でペイロードを配布するための餌文書戦術を使用しました。内部に侵入した後、Malware は徹底的なシステムプロファイリングを行い、資格情報を盗み、ユーザーのキー入力を監視し、正常なウェブトラフィックを通じてデータを密かに盗みました。持続的なコマンド＆コントロール接続を維持し、リアルタイムのデータ窃盗とリモートコマンド実行を可能にしました。キャンペーンの段階は、適応型仮想化回避検査と反射的 DLL インジェクションを含み、セキュリティ防御を回避し、メモリ内で検出されずに運用を続けました。戦略的目標への集中とこれらの技術的手法の組み合わせは、高度な国家関連サイバーアクターがもたらす進化する脅威環境を強調しています。

[Attack Flow]

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
a. 誤解を招く LNK ファイルの送信
b. 韓国政府の通知を模倣した資料の使用
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. 信頼できるシステムユーティリティの使用
3. [持続性] ショートカットの変更 (T1547.009)
a. ショートカットファイルの修正

b. 持続的なアクセスの維持

4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 難読化されたスクリプトの使用
   b. 検出回避
5. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. 資格情報の奪取
   b. システムプロファイリング
6. [収集] 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の監視
   b. 継続的な情報収集
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 (T1071.001)
   a. 正常なウェブトラフィックを通じたデータの奪取
   b. リアルタイムのコマンド＆コントロール接続の維持
8. [防御回避] リフレクティブコードローディング (T1620)
   a. リフレクティブ DLL 注入
   b. メモリ内での検出回避
9. [発見] システム情報の発見 (T1082)
   a. システム情報の収集
   b. 環境プロファイリング
10. [データ流出] ウェブサービスを介したデータ流出 (T1567.002)
    a. ウェブサービスを通じたデータの送信
    b. 秘密裏の情報奪取

12) SectorA05 used Phishing Emails with LNK disguised as PDF Icons (2025-08-18)

https://cti.nshc.net/events/view/17803

攻撃対象産業群: 外交

2025 年初頭、精巧なサイバー諜報キャンペーンが主に韓国の外交使節団を対象に、3 月から 7 月にかけてスピアフィッシングメールを通じて攻撃を実施しました。攻撃者は信頼できる外交連絡先を装い、世界中の大使館職員に巧妙に作成されたメールを送信し、このメールには悪意のある ZIP 添付ファイルが含まれていました。このメールは外交官や官僚を装い、信頼できる会議の招待や公式文書を提供しました。ZIP ファイルには悪意のある Windows ショートカット（.lnk）ファイルが含まれており、開くと PowerShell コマンドを実行し、持続性を設定しました。攻撃者は GitHub をコマンド＆コントロールチャネルとして活用し、Dropbox をマルウェア配布に使用して XenoRAT というリモートアクセス型トロイの木馬の亜種を配布しました。このマルウェアは GitHub API を通じたデータ窃取を含む、諜報のための完全なシステム制御を可能にしました。インフラ分析は以前の北朝鮮

の諜報作戦と関連しており、以前に識別された C2 サーバーを活用しました。キャンペーンの感染チェーンは、暗号化された PowerShell コマンドの実行、偵察処理、および GitHub トラフィックに偽装したデータ窃取を含んでいました。GitHub リポジトリの迅速な更新は動的ペイロード配布を可能にし、マルウェアの隠蔽性を向上させました。攻撃者は専用の仮想マシンを使用し、韓国のインフラを活用して活動を隠蔽し、高度な運用セキュリティと持続性を示しました。技術的証拠は北朝鮮関連の行為者と関連する歴史的諜報作戦と一致し、外交的標的を欺くための高度な侵入技術と社会工学的戦術を示しています。

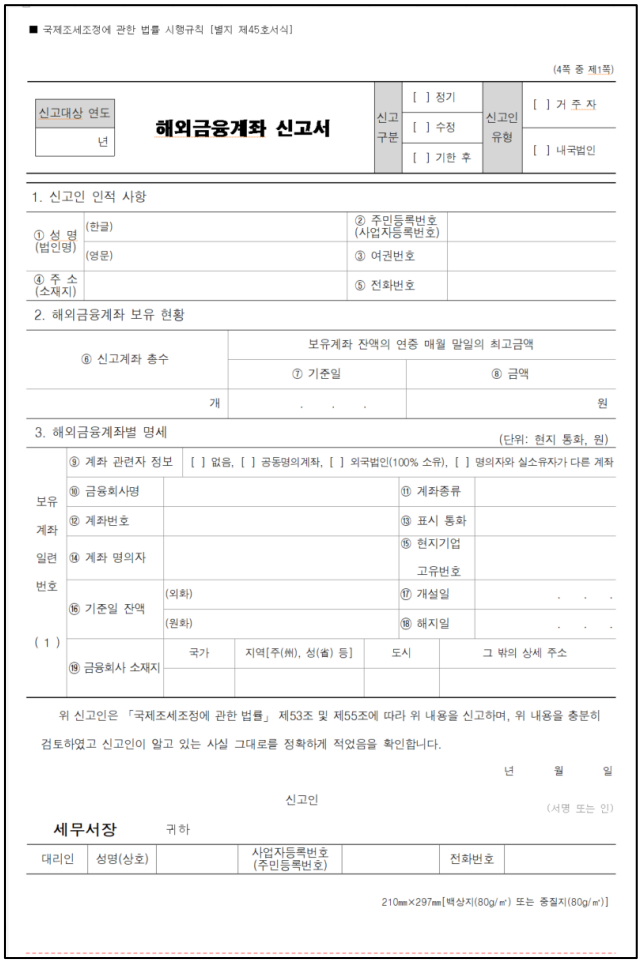
[Attack Flow]

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. 信頼できる外交連絡先を装ったスピアフィッシングメールの使用
   b. マルウェア ZIP ファイルの添付および会議招待や公式文書の提供
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. ZIP ファイル内の.lnk ファイルを開く
   b. PowerShell コマンドの実行
3. [持続性] スケジュールされたタスク/ジョブ (T1053.005)
   a. 持続性のためのスケジュールされたタスクの設定
   b. PowerShell スクリプトを通じた自動実行の維持
4. [コマンド＆コントロール] Web サービス経由のデータ流出 (クラウド) (T1567.002)
   a. GitHub API を使用したデータの流出
   b. GitHub リポジトリの迅速な更新を通じたペイロードの配布
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 暗号化された PowerShell コマンドの使用
   b. GitHub トラフィックへの偽装
6. [発見] システム情報の発見 (T1082)
   a. システム情報の収集
   b. IP アドレスおよびタイムスタンプを含むデータの収集
7. [データ流出] Web サービス経由のデータ流出 (クラウド) (T1567.002)
   a. GitHub API を通じたデータのアップロード
   b. HTTPS を通じて GitHub のドメインと共にデータを流出

13) SectorA07 used LNK Malware disguised as a Foreign Financial Account Report Form (2025-07-21)

https://cti.nshc.net/events/view/17205

攻撃者は「海外金融口座申告書.hwp.lnk」というファイルを作成し、外国金融口座の報告書に偽装しました。このファイルは国税庁の公式文書のように見せかけ、メールを通じて無作為に配布されました。悪性ファイルは主に Windows PowerShell を利用して実行されました。PowerShell スクリプトは文字列の分割とランダムなコメントの挿入を通じて回避技術を使用し、「rshell.exe」という特定の悪性ファイルを検索して実行しました。主な PowerShell 機能には、ファイル内容の操作、ディレクトリパスの識別、CAB ファイルの抽出が含まれていました。マルウェアはユーザーのダウンロード、ドキュメント、デスクトップディレクトリからデータを収集し、システム情報を追加で収集し、RC4 ベースの暗号化方法を使用してデータを窃取しました。収集されたデータは技術ソリューション会社に偽装したリモートサーバーに送信された後、元のファイルは削除されました。脅威行為者が管理するサーバーは Laravel を使用して収集されたデータを処理し、潜在的に復号化しました。この作戦は、機密性の高い金融およびユーザー情報を抽出するための標的化された努力であり、窃取されたデータを利用した追加攻撃につながる可能性があります。



■ 국제조세조정에 관한 법률 시행규칙 [별지 제45호서식]

(4쪽 중 제1쪽)

신고대상 연도 / 년	해외금융계좌 신고서	신고 구분	[ ] 정기 / [ ] 수정 / [ ] 기한 후	신고인 유형	[ ] 거 주 자 / [ ] 내국법인

1. 신고인 인적 사항

① 성 명 (법인명)	(한글)	② 주민등록번호 (사업자등록번호)	
	(영문)	③ 여권번호	
④ 주 소 (소재지)		⑤ 전화번호	

2. 해외금융계좌 보유 현황

⑥ 신고계좌 총수	보유계좌 잔액의 연중 매월 말일의 최고금액	
	⑦ 기준일	⑧ 금액
개	. . .	원

3. 해외금융계좌별 명세 (단위: 현지 통화, 원)

보유계좌 일련번호	⑨ 계좌 관련자 정보	[ ] 없음, [ ] 공동명의계좌, [ ] 외국법인(100% 소유), [ ] 명의자와 실소유자가 다른 계좌		
	⑩ 금융회사명		⑪ 계좌종류	
	⑫ 계좌번호		⑬ 표시 통화	
	⑭ 계좌 명의자		⑯ 현지기업 고유번호	
	⑮ 기준일 잔액	(외화)	⑰ 개설일	. . .
		(원화)	⑱ 해지일	. . .
(1)	⑲ 금융회사 소재지	국가 / 지역[주(州), 성(省) 등] / 도시 / 그 밖의 상세 주소		

위 신고인은 「국제조세조정에 관한 법률」 제53조 및 제55조에 따라 위 내용을 신고하며, 위 내용을 충분히 검토하였고 신고인이 알고 있는 사실 그대로를 정확하게 적었음을 확인합니다.

년 월 일

신고인 (서명 또는 인)

세무서장 귀하

대리인	성명(상호)		사업자등록번호 (주민등록번호)		전화번호	

210㎜×297㎜[백상지(80g/㎡) 또는 중질지(80g/㎡)]

[図 5: SectorA07 グループが悪用したおとり文書]

[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. メール添付ファイルとして「海外金融口座申告書.hwp.lnk」を配布
   b. 国税庁の公式文書に偽装
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 スクリプトを通じてマルウェアファイルを実行
   b. 文字列分割およびランダムなコメント挿入を使用
3. [防御回避] 偽装 (T1036)
   a. 国税庁の公式文書に偽装
   b. ランダムなコメント挿入による検出回避
4. [発見] ファイルおよびディレクトリの発見 (T1083)
   a. ディレクトリパスの識別
   b. ユーザーのダウンロード、ドキュメント、デスクトップディレクトリからファイルを検索
5. [収集] ローカルシステムからのデータ (T1005)
   a. ユーザーディレクトリからデータを収集
   b. システム情報を収集
6. [流出] C2 チャネルを介したデータ流出 (T1041)
   a. RC4 ベースの暗号化を通じてデータを盗む
   b. リモートサーバーに盗まれたデータを送信
7. [影響] データ破壊 (T1485)
   a. 元のファイルを削除
   b. 盗んだ後にファイルを破壊

14) SectorB01 used DLL Sideloading and Cobalt Strike for Government Attacks (2025-07-21)

https://cti.nshc.net/events/view/17097

攻撃対象産業群: 健康、IT、政府・行政、通信、教育、エネルギー

攻撃者はアフリカの政府 IT サービスを対象に精巧なサイバー攻撃を実行しました。内部サービス名、IP アドレス、プロキシサーバーなどのハードコーディングされた詳細情報を Malware に組み込んで使用しました。複数のワークステーションで Impacket ツールキットモジュール（WmiExec と Atexec）を利用したコマンド実行を通じて疑わしい活動が検出されました。攻撃者は監視されていないホストを悪用し、侵害された SharePoint サーバーを C2 として使用し、レジストリハイブからの資格情報収集を通じて権限昇格を行いました。悪意のあるツールは SMB プロトコルを介して対象ホストのさまざまなディレクトリに転送され、Cobalt Strike の実行には DLL サイドローディングが

利用されました。攻撃者は暗号化されたペイロードをディレクトリに配置し、合法的なアプリケーションを通じて実行しました。GitHub を装ったドメインから JavaScript スクリプトを使用してリバースシェルを生成しました。データ漏洩はウェブシェルとトロイの木馬を通じて行われ、偵察にはホストから資格情報や機密データを盗むための修正されたユーティリティが使用されました。検出を回避するための適応にもかかわらず、初期のアーティファクトは IIS ウェブサーバーで発見され、これは精巧な技術と継続的な努力を示しています。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1203)
   a. 内部サービス名および IP アドレスのハードコーディング
   b. プロキシサーバー情報の内蔵
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. Impacket WmiExec モジュールの使用
   b. Impacket Atexec モジュールの使用
3. [持続性] システムプロセスの作成または変更 (T1543)
   a. 合法的なアプリケーションを通じた DLL サイドローディング
   b. Cobalt Strike ペイロードの暗号化および実行
4. [権限昇格] アクセストークン操作: トークン偽装/盗用 (T1134.001)
   a. レジストリハイブからの資格情報収集
   b. ドメイン管理者権限アカウントの使用
5. [防御回避] 偽装 (T1036)
   a. GitHub を装ったドメインの使用
   b. 合法的な DLL ファイル名の使用
6. [資格情報アクセス] OS 資格情報ダンピング: レジストリ (T1003.002)
   a. レジストリハイブのダンプ
   b. SYSTEM および SAM ハイブの活用
7. [探索] システム情報探索 (T1082)
   a. 実行中のプロセスおよびポートの確認
   b. セキュリティソリューションの検出回避の確認
8. [横移動] リモートサービス: SMB/Windows 管理共有 (T1021.002)
   a. SMB プロトコルを通じたツールの転送
   b. C$ネットワーク共有の使用
9. [収集] ローカルシステムからのデータ (T1005)
   a. 敏感なデータおよび資格情報の収集
   b. 修正された Pillager ユーティリティの使用
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: Web プロトコル (T1071.001)

a. SharePoint サーバーを通じた C2 通信
b. Web シェル(CommandHandler.aspx)の活用
11. [データ流出] Web サービスを通じたデータ流出 (T1567.002)
a. Web シェルを通じたデータ流出
b. SharePoint サーバーへのデータアップロード
12. [影響] システム回復の抑制 (T1490)
a. マルウェアファイルおよび痕跡の削除
b. 検出回避のためのコーディング修正および DLL コンパイル

15) SectorB01 used GodRAT disguised as financial docs via Skype (2025-08-19)

https://cti.nshc.net/events/view/17826

攻撃対象産業群: 金融

2024 年 9 月、攻撃者は金融機関を対象に Skype メッセンジャーを通じて金融文書に偽装した.scr ファイルを配布し、攻撃を開始しました。彼らは Gh0st RAT から派生した GodRAT というリモートアクセス型トロイの木馬（RAT）を配布しました。攻撃者は画像内にシェルコードを隠すステガノグラフィ技法を使用して、Command-and-Control（C2）サーバーから GodRAT をダウンロードしました。GodRAT はプラグインを通じて攻撃者が FileManager を使用してシステムを探索し、ブラウザのクレデンシャルを盗む機能を実行しました。また、持続的なアクセスのために AsyncRAT を補助的に活用しました。Malware は.scr および.pif ファイルが文書に偽装されてユーザーを欺き、合法的なプロセス内で実行されるようにするシェルコード注入技法を悪用しました。署名スプーフィングは、有効期限切れの証明書で署名された実行ファイルを含んでいました。GodRAT とそのインフラは、既知の脅威フレームワークと起源を共有する過去の RAT の進化に繋がっています。この攻撃は 2025 年にも依然として活発であり、金融機関内への侵入とアクセス維持のために継続的に悪用方法を使用しています。

[Attack Flow]

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
a. Skype メッセンジャーを通じた悪性.scr ファイルの配布
b. 金融文書に偽装されたファイル送信
2. [実行] ユーザー実行 (T1204.002)
a. ユーザーが.scr ファイルを実行
b. ユーザーが.pif ファイルを実行
3. [防御回避] 偽装 (T1036)
a. 文書に偽装された.scr および.pif ファイルの使用
b. 期限切れの証明書で署名された実行ファイルの使用

4. [防御回避] ステガノグラフィー (T1027.003)
   a. 画像ファイル内にシェルコードを隠匿
   b. ステガノグラフィーを通じた検出回避
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. シェルコードを通じて C2 サーバーに接続
   b. GodRAT のダウンロードおよび実行
6. [持続性] RAT のインプラント (T1219)
   a. GodRAT および AsyncRAT のインストール
   b. 持続的なアクセスのための補助 RAT の使用
7. [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. ブラウザ資格情報の窃取
   b. 資格情報収集のためのパスワードスティーラーの配布
8. [探索] システム情報探索 (T1082)
   a. FileManager を通じたシステム探索
   b. プラグインを通じた情報収集
9. [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 TCP 接続
   b. コマンドおよびデータ送受信のための暗号化通信の使用

16) SectorB22 used FireWood Backdoor for Linux Espionage Operations (2025-08-13)

https://cti.nshc.net/events/view/17678

FireWood バックドアの新しい亜種は、核心機能を維持しつつ、実装と構成に変化を見せています。このバックドアはリモートアクセス型トロイの木馬として機能し、侵害された Linux デスクトップにウェブシェルを通じて侵入します。コマンド実行と機密データの漏洩を通じて、カーネルレベルのルートキットと TEA ベースの暗号化を使用し、隠密な作戦を支援します。更新されたバージョンは、初期権限チェックを削除し、起動順序を修正して隠蔽性を強化しました。ネットワーキングプロトコルの変化は、接続プロセスを簡素化し、時間的難読化を取引し、コマンド制御の到達可能性を高めました。構成ベースのタイムアウトを削除し、デーモン化およびカーネルモジュールの相互作用に新しいロジックを導入しました。ファイルパスとコマンド構造が更新され、「自動終了」機能の追加、プロセスの隠蔽およびファイル転送コマンドが修正されました。イランとフィリピンで検出されたサンプルは、世界的な配布を示し、広範な使用を示しています。以前の脅威アクターとの関連は推測に過ぎません。

[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. 侵害されたウェブシェルを通じた初期侵入
   b. Linux デスクトップのターゲティング
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. リモートコマンドの実行
   b. システム情報の収集とコマンドの実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. 起動順序の修正と PID の保存
   b. デーモン化プロセスでのカーネルモジュールのロード
4. [防御回避] ルートキット (T1014)
   a. カーネルレベルのルートキットの使用
   b. プロセスおよびファイルパスの隠蔽
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. システム資格情報の窃取
   b. 機密情報の収集
6. [発見] システム情報の発見 (T1082)
   a. ユーザーおよびシステム情報の収集
   b. OS 検出と情報収集経路の変更
7. [収集] ローカルシステムからのデータ (T1005)
   a. ファイルおよびデータの収集
   b. ファイル転送およびアップロードコマンド
8. [流出] 代替プロトコルを介した流出 (T1048)
   a. TEA ベースの暗号化を通じたデータ流出
   b. 拡張子ベースのファイル流出
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. ネットワークプロトコルの変更と接続の簡素化
   b. 継続的な C2 接続とコマンドの受信

17) SectorB106 Targets Telecoms with Stealthy Intrusion Tactics (2025-07-29)

https://cti.nshc.net/events/view/17388

攻撃対象産業群: 通信

2024 年の間、南西アジア地域の通信プロバイダーを対象とした脅威クラスターは、非常に巧妙な侵入キャンペーンを実行しました。攻撃者は、SSH ブルートフォース攻撃を開始点として、通信環境に合わせた資格情報辞書を使用して初期アクセスを確保しました。内部に侵入した後、攻撃者は DirtyCoW や PwnKit のような既知の権限昇格の脆弱性を悪用して、ルートレベルのアクセス権を取

得しました。カスタムバックドアを展開して持続性を維持し、GTP、ICMP、DNS トンネリング、SSH リバースポートフォワーディングなどのプロトコルを使用して、隠密なコマンド＆コントロール（C2）チャネルを構築しました。これらのチャネルは、従来のセキュリティモニタリングツールを回避しながら、外部サーバーとの通信を可能にしました。フォレンジック分析をさらに回避するために、攻撃者はログ削除、プロセス改ざん、ファイルのタイムスタンプ変更、SELinux のようなセキュリティメカニズムの無効化といった手法を使用しました。これらの侵入技術と回避技術の組み合わせは、通信インフラに対する深い理解を示しており、即時のデータ窃取よりも長期的な偵察および戦略的制御を目的としていました。

[Attack Flow]

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. 通信環境に特化した資格情報辞書の使用
2. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. DirtyCoW 脆弱性の悪用
   b. PwnKit 脆弱性の悪用
3. [持続性] カスタムバックドアのインプラント (特定の TID なし)
   a. カスタムバックドアの配布
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. GTP、ICMP、DNS トンネリングの使用
   b. SSH リバースポートフォワーディングの使用
5. [防御回避] ホスト上のインジケーター削除 (T1070)
   a. ログ削除
   b. ファイルのタイムスタンプ変更
6. [防御回避] 偽装 (T1036)
   a. プロセスの改ざん
7. [防御回避] ツールの無効化または変更 (T1562)
   a. SELinux の無効化

18) SectorB117 Phishing Campaign Targeting Tibetan and Taiwanese Political Entities (2025-08-13)

https://cti.nshc.net/events/view/17782

攻撃対象産業群: 非政府組織(NGO)、報道・メディア

2025 年 7 月末、フィッシングキャンペーンがチベットのメディアおよび擁護団体を標的にしました。メールはヨーロッパの人権研究者を装い、Netlify にホスティングされたマルウェア RAR アーカイ

ブを配信しました。埋め込まれたペイロードの実行は、DLL サイドローディングチェーンを通じて Golang ベースのバックドア CuVn をインストールしました。チベットの政治圏内の組織は高い警戒を維持する必要があります。また、類似の技術が台湾の被害者を対象としていることが判明しました。

[Attack Flow]

1. [偵察] 情報を得るためのフィッシング (T1598)
   a. チベットのメディアおよび擁護団体を対象としたフィッシングメールの送信
   b. ヨーロッパの人権研究者を装う
2. [リソース開発] インフラの取得 (T1583)
   a. Netlify にマルウェア RAR アーカイブをホスティング
3. [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 RAR アーカイブを添付
   b. メールを通じて対象に送信
4. [実行] ユーザー実行 (T1204)
   a. 埋め込みペイロードの実行
5. [持続性] DLL サイドローディング (T1574.002)
   a. DLL サイドローディングチェーンの実行
   b. Golang ベースのバックドア CuVn のインストール
6. [防御回避] 偽装 (T1036)
   a. ヨーロッパの人権研究者を装って検知を回避
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. バックドアを通じて C2 サーバーとの通信

19) SectorB118 exploited SharePoint vulnerabilities (2025-07-22)

https://cti.nshc.net/events/view/17140

攻撃対象産業群: 金融、健康、政府・行政、防衛、非政府組織(NGO)、シンクタンク、高等教育

攻撃者は 2025 年 7 月 19 日に、CVE-2025-49706 および CVE-2025-49704 の脆弱性を悪用してオンプレミスの SharePoint サーバーを標的にしました。中国の国家主導の攻撃グループ 2 つと別の中国拠点のグループが、インターネットに露出した SharePoint サーバーを狙い、細工された POST リクエストを通じて spinstall0.aspx というマルウェアスクリプトをアップロードしました。このスクリプトは MachineKey データを抽出し、GET リクエストを通じて攻撃者に返送しました。ウェブシェルは後続の攻撃ペイロードとして使用され、システムのさらなる侵害を可能にしました。攻撃者は探索と認証回避を試み、リモートコード実行を行いました。Microsoft は、CVE-2025-53770 および CVE-2025-53771 のような追加の関連脆弱性を解決するためのセキュリティアップデートを発

表し、さらなる悪用を防ぐためにパッチの緊急性を強調しました。悪意のある行為者は、知的財産の盗用、システム侵入、ランサムウェアの配布の過去のパターンを持っています。

[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. インターネットに公開された SharePoint サーバーの脆弱性攻撃
   b. 改ざんされた POST リクエストを通じた悪性スクリプトのアップロード
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ペイロードの実行
   b. リモートコード実行のための認証バイパスの試み
3. [持続性] Web シェル (T1505.003)
   a. 悪性 Web シェルのインストール
   b. Web シェルを通じた持続的なシステムアクセス
4. [収集] 設定リポジトリからのデータ (T1602)
   a. MachineKey データの抽出
   b. GET リクエストを通じたデータの返却
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. ファイル名の変更を通じた検出回避
   b. 様々なファイル名の変形使用 (spinstall1.aspx など)
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 (T1071)
   a. HTTP GET リクエストを通じたコマンドとコントロール
   b. 攻撃者サーバーへのデータ送信

20) SectorB118 used LockBit Black and Warlock ransomware (2025-07-31)

https://cti.nshc.net/events/view/17421

サイバー攻撃者は 2025 年初頭に Microsoft SharePoint サーバーを対象に「ToolShell」脆弱性を利用した大規模な作戦を実施しました。この攻撃はラテンアメリカと APAC 地域をまたいで行われました。攻撃者は「ak47c2」というカスタム C2 フレームワークを使用し、HTTP および DNS ベースのクライアントと共に動作しました。彼らの活動には、LockBit Black や Warlock/X2anylock を含む様々なランサムウェアの亜種の配布が含まれ、主に DLL ハイジャック技術がベクターとして使用されました。また、攻撃者は PsExec や WinPcap といったオープンソースツールを使用し、BYOVD 技術を活用したカスタムツールでエンドポイント保護機能を無効化しました。特に DNS トンネリングバックドアと dnsclient.exe という危険なファイルを通信に使用しました。対象インフラは 2025 年 3 月から update.updatemicfosoft[.]com ドメインを悪意のある活動に継続的に使用しました。

[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. ToolShell 脆弱性の活用
   b. Microsoft SharePoint サーバーのターゲティング
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. PsExec の使用
   b. DNS ベースの C2 クライアントの実行
3. [持続性] DLL 検索順序ハイジャック (T1574.001)
   a. DLL ハイジャックによる持続性の確保
   b. ランサムウェアの変種の維持
4. [防御回避] ツールの無効化または変更 (T1562)
   a. BYOVD 手法でエンドポイント保護を無効化
   b. WinPcap の活用
5. [コマンドと制御] アプリケーション層プロトコル (T1071)
   a. ak47c2 フレームワークで HTTP 通信
   b. DNS トンネリングバックドアの使用
6. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. dnsclient.exe ファイルでデータ流出
   b. update.updatemicfosoft[.]com ドメインの活用

21) SectorB120 used SoundBill Shellcode Loader for Long-Term Access (2025-08-15)

https://cti.nshc.net/events/view/17735

攻撃者は 2022 年以降活動している高度持続的脅威グループであり、台湾のウェブインフラエンティティを対象にオープンソースツールを活用して検出を回避し、長期的な持続性を確立しました。このグループは VPN およびクラウドインフラへのアクセスに集中し、Cobalt Strike のようなシェルコードをデコードしてロードする「SoundBill」というカスタムシェルコードローダーを含む様々なツールを使用しました。攻撃者はパッチが適用されていないサーバーの既知の脆弱性を悪用して初期アクセスを取得した後、ターゲットの価値を評価するために偵察を行いました。持続性を維持するために SoftEther VPN クライアントと直接 RDP アクセスを使用し、関連グループがウェブシェルを使用するのとは異なります。脅威グループは持続的な運用のためにカスタムのマルウェアとバックドアを展開しました。侵害後には、Mimikatz や JuicyPotato のようなツールを使用して資格情報の抽出と権限昇格を行いました。ネットワークの拡散は、FScan と SharpWMI を使用してネットワークスキャンおよび WMI クエリを実行することで達成されました。セキュリティ機能を無効化し、平文パスワードを抽出するための設定変更が試みられました。

[Attack Flow]

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. パッチが適用されていないサーバーの既知の脆弱性を悪用
   b. インターネットに公開されたウェブインフラエンティティをターゲット
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. cmd.exe を使用したシステム情報の収集
   b. PowerShell を使用したファイルのダウンロードと実行
3. [持続性] 外部リモートサービス (T1133)
   a. SoftEther VPN クライアントを使用した持続性の維持
   b. RDP を使用したシステムへの直接アクセス
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. JuicyPotato を使用した権限昇格
   b. レジストリの変更を通じた UAC の無効化
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. カスタムシェルコードローダー「SoundBill」の使用
   b. オープンソースツールのカスタマイズ
6. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. Mimikatz を使用した資格情報の抽出
   b. レジストリおよびディスクからの VNC 資格情報の検索
7. [探索] リモートシステム探索 (T1018)
   a. SharpWMI を使用した WMI クエリの実行
   b. ネットワークスキャンのための FScan の使用
8. [横移動] リモートサービス (T1021)
   a. SMB を使用したリモートシステムへのアクセス
   b. 資格情報を使用したシステムのピボット
9. [収集] 情報リポジトリからのデータ (T1213)
   a. システムの情報リポジトリからのデータ収集
   b. コマンドを使用した追加情報の収集
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)
    a. Cobalt Strike を使用した HTTPS による C2 通信
    b. リモートサーバーとの持続的な接続の維持

22) SectorC02 used AiTM to deploy ApolloShadow in cyberespionage (2025-07-31)

https://cti.nshc.net/events/view/17405

攻撃対象産業群: 外交、政府・行政

攻撃者はモスクワに位置する外国大使館を対象にサイバー諜報キャンペーンを実施しました。彼らは中間者攻撃（AiTM）手法を利用して、ApolloShadow というカスタムマルウェアを配布しました。攻撃者はロシアの ISP ネットワークを活用してインターネットトラフィックを傍受し操作し、対象デバイスにルート証明書をインストールして持続的な情報収集の足場を築きました。このキャンペーンは少なくとも 2024 年から活動しており、現地 ISP に依存する外交機関やその他の敏感な組織に深刻なリスクをもたらしています。初期アクセスはキャプティブポータルを通じて対象デバイスをリダイレクトすることで行われ、ApolloShadow は権限を悪用して既知のアンチウイルスソフトウェアに偽装し、証明書をインストールすることでネットワークトラフィックを操作しました。このマルウェアはデータ漏洩のためにエンコーディング手法を活用し、感染したデバイスに管理者ユーザーアカウントを作成して持続性を維持しました。

[Attack Flow]

1. [実行] コマンドとスクリプトインタープリター (T1059)
    a. ApolloShadow のダウンロードと実行
    b. 証明書インストールのためのユーザーアクセス制御の回避
2. [持続性] アカウント操作 (T1098)
    a. 管理者ユーザーアカウントの作成
    b. 証明書インストールによる持続性の確保
3. [防御回避] 偽装 (T1036)
    a. Kaspersky インストーラーの偽装
    b. ルート証明書インストールによる権限昇格
4. [資格情報アクセス] 入力キャプチャ (T1056)、中間者攻撃 (AiTM) (T1557)
    a. ネットワークトラフィックの操作
    b. 認証情報とトークンの収集
    c. ISP ネットワークを通じたトラフィックの傍受
    d. キャプティブポータルを利用したデバイスのリダイレクト
5. [収集] ローカルシステムからのデータ収集 (T1005)
    a. ホスト情報の収集
    b. IP 情報をエンコードして C2 へ送信
6. [データ流出] C2 チャネルを介したデータ流出 (T1041)
    a. Base64 エンコードされたデータの送信
    b. C2 サーバーへの継続的なデータ流出
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. DNS 操作を通じた C2 通信
    b. 暗号化された VBScript ペイロードの受信と実行

23) SectorC05 used Phishing Emails Disguised as Court Subpoenas (2025-08-04)

https://cti.nshc.net/events/view/17493

攻撃対象産業群: 政府・行政、国防

攻撃者はウクライナの政府機関、防衛軍および防衛産業企業を対象にサイバー攻撃を実行しました。初期段階では、UKR.NET を通じて「裁判所召喚状」をテーマにしたメールを送信しました。このメールには URL 短縮サービスを使用して短縮されたリンクが含まれており、合法的なファイルサービスに接続され、二重に圧縮された HTA ファイルをダウンロードさせました。HTA ファイルには難読化された VBScript が含まれており、これは HEX コード化されたデータを含むテキストファイルと PowerShell コードを生成し、それを実行してデータを変換し実行ファイルを生成する作業を開始しました。キャンペーンはペイロード配布のためのローダーとレジストリ持続性を維持する様々なマルウェアを活用しました。バックドアは PowerShell コマンドの実行、データの窃取、ブラウザーデータとシステム情報の収集を目的としていました。コマンドサーバーとの通信は HTTP/HTTPS を通じてエンコードされたペイロードで行われ、持続性はスケジュールされたタスクとレジストリキーを通じて維持されました。これらの手法は、持続的なアクセスとデータ窃取能力を目的とした高度な脅威の複雑性を示しています。

[Attack Flow]

1. [初期アクセス] フィッシング: スピアフィッシング添付ファイル (T1566.001)
   a. UKR.NET を通じた裁判所召喚状テーマのメール送信
   b. URL 短縮サービスを使用したリンクの含有
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. 正当なファイルサービスからの HTA ファイルダウンロード
   b. HTA ファイル内の VBScript 実行
3. [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. VBScript が PowerShell コードを生成および実行
   b. データ変換を通じて実行ファイルを生成
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. レジストリキーを通じた持続性の維持
   b. 予約されたタスクを通じた持続性の維持
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 VBScript の使用
   b. HEX コード化されたデータの生成
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: Web プロトコル (T1071.001)

a. HTTP/HTTPS を通じたコマンドサーバーとの通信
b. エンコードされたペイロードの送信
7. [データ流出] 自動化されたデータ流出 (T1020)
a. データの窃取および送信
b. ブラウザデータとシステム情報の収集

24) SectorC32 used Spear Phishing with Lookalike Domains (2025-07-25)

https://cti.nshc.net/events/view/17285

攻撃対象産業群: 航空宇宙、非政府組織(NGO)、警察・法執行機関

ロシア政府が支援する APT グループは、2024 年 4 月から NATO 加盟国とウクライナを対象に情報収集を目的として活動していました。彼らは盗用された資格情報やセッションクッキーを初期アクセスに利用し、micsrosoftonline[.]com のようなドメインのタイプミスを利用して標的を欺くスピアフィッシング手法を使用しました。主な標的には、オランダ警察、ウクライナ航空機関、ヨーロッパおよびアメリカの複数の NGO が含まれていました。グループのインフラには、ebsummit の正規ドメインを模倣した ebsumrnit[.]eu のようなドメインが含まれ、Mailgun DNS で設定され、PDR Solutions に登録されていました。Validin のピボット機能を使用して、キャンペーンに関連する追加のドメインを発見しました。これらのドメインは PDR Ltd.に登録され、onionmail のメールおよび Cloudflare DNS を使用する類似の戦術を使用していました。フィッシング戦術には、合法的なコンテンツにリダイレクトする方法が含まれていました。ドメインはしばしば合法的なサービスを偽装するために CNAME として構成されていました。分析は、彼らの活動が公開された後も迅速に適応する洗練されたインフラと技術を強調しました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング (T1566.002)
a. タイポスクワッティングされたドメインの使用
b. スピアフィッシングメールの送信
2. [資格情報アクセス] ウェブセッションクッキーの盗難 (T1539)
a. セッションクッキーの盗用
b. 資格情報の窃取
3. [コマンド＆コントロール] 有効なドメインの使用 (T1071.004)
a. 合法的なサービスの CNAME 設定
b. Cloudflare を通じたトラフィックの偽装
4. [防御回避] ドメインフロント (T1172)
a. 合法的なコンテンツへのリダイレクト
b. onionmail メールの使用

5. [探索] ネットワークサービススキャン (T1046)
   a. DNS 記録の探索
   b. ドメインピボットと検出
6. [収集] 情報リポジトリからのデータ (T1213)
   a. ターゲット情報の収集
   b. フィッシングを通じたデータ収集
7. [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. 流出データの暗号化と送信

25) SectorC34 exploited Cisco IOS vulnerability CVE-2018-0171 (2025-08-20)

https://cti.nshc.net/events/view/17836

攻撃対象産業群: 製造、通信、高等教育

サイバー諜報グループは 10 年以上にわたり活動しており、Cisco IOS ソフトウェアの Smart Install 機能の脆弱性（CVE-2018-0171）を悪用してネットワークデバイスを標的にしています。主なターゲットは、北米、アジア、アフリカ、ヨーロッパの通信、高等教育、製造業部門です。攻撃者は構成データを盗み出し、持続的なアクセスを維持し、戦略的利益に合わせた長期的な運用を支援します。このグループは SYNful Knock ファームウェアインプラントとカスタム SNMP ツールを使用して検出を回避し、公開スキャンデータを利用して対象を特定します。攻撃チェーンは、脆弱性を悪用してデバイスの構成を変更し、TFTP を通じてデータを流出させることで構成されています。このグループは、アクセス制御リストおよび TACACS+構成を変更してログ機能を妨害し、GRE トンネルを通じてネットワークトラフィックをキャプチャすることが知られています。彼らのキャンペーンは、類似の国家支援攻撃から保護するために、パッチおよびセキュリティ強化措置の重要性を強調しています。

[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. Cisco IOS Smart Install 機能の脆弱性(CVE-2018-0171)を悪用
   b. 非公開および老朽化したネットワークデバイスを対象に攻撃を実行
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
   a. SNMP を通じてリモートサーバーからテキストファイルをダウンロードおよび実行
   b. SNMP コミュニティ文字列を使用して実行コマンドを伝達
3. [持続性] 内部ネットワークへのインプラント (T1505)
   a. SYNful Knock ファームウェアインプラントを使用
   b. ローカルユーザーアカウントおよび SNMP コミュニティ文字列を作成

4. [防御回避] 認証プロセスの変更 (T1556)
   a. TACACS+構成の修正でログ機能を妨害
   b. アクセス制御リストを修正して特定の IP アドレスへのアクセスを許可
5. [収集] ネットワークスニッフィング (T1040)
   a. GRE トンネルを通じてネットワークトラフィックをキャプチャ
   b. NetFlow データの収集および流出
6. [データ流出] 代替プロトコルを介したデータ流出 (T1048)
   a. TFTP および FTP を通じて構成ファイルを流出
   b. SNMP を利用して構成データを外部に送信
7. [探索] ネットワークサービススキャン (T1046)
   a. 公開スキャンデータを活用してターゲットシステムを識別
   b. 'show cdp neighbors'コマンドで追加のターゲットを識別

26) SectorD02 used Android Malware DCHSpy disguised as VPN Apps (2025-07-21)

https://cti.nshc.net/events/view/17154

攻撃対象産業群: 防衛、石油

イスラエルとイランの対立の中で、新しい Android 監視ツールのサンプルが登場しました。これはイランの情報機関と関連があると推定されるサイバー諜報グループによって継続的に開発されています。このツールは、WhatsApp メッセージ、連絡先情報、SMS、ファイル、位置データを収集し、デバイスのマイクとカメラを有効にしてオーディオと写真を記録することができます。最近、このツールはイラン政府が課したインターネット遮断中に StarLink インターネットアクセスに関連する誘引策を使用して拡散されています。Telegram のようなメッセージングアプリを通じて悪意のある URL で配布され、VPN サービスのような合法的なアプリケーションに偽装されています。このツールは 2022 年に初めて報告された別の Android マルウェアとコマンド＆コントロールインフラを共有しています。収集されたデータは暗号化され、指定されたサーバーに送信されます。これらの活動は、グループがさまざまな地域の政府および民間部門を対象とした諜報活動に集中していることを反映しています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. StarLink インターネットアクセス誘引策
   b. メッセージングアプリを通じた悪性 URL 配布
2. [実行] コマンドとスクリプトインタープリター (T1059)
   a. VPN アプリケーションに偽装したマルウェア実行
   b. 政治的誘引策を活用した実行

3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. デバイス起動時の自動実行設定
   b. 持続的なモジュール更新
4. [防御回避] 偽装 (T1036)
   a. 合法的なアプリに偽装
   b. VPN サービスに偽装
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. デバイス内のログインアカウント情報収集
   b. 連絡先および SMS データアクセス
6. [収集] 自動収集 (T1119)
   a. WhatsApp メッセージおよびファイル収集
   b. オーディオおよび写真記録
7. [コマンドと制御] 暗号化チャネル (T1573)
   a. 暗号化されたチャネルを通じたコマンド受信
   b. C2 サーバーからの追加コマンド受信
8. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. データの圧縮および暗号化
   b. SFTP サーバーへのデータアップロード

27) SectorD02 used PowerShell Malware disguised as Teams Invitation (2025-08-11)

https://cti.nshc.net/events/view/17650

攻撃対象産業群: 社会基盤施設

攻撃者はイスラエルのビジネスおよびインフラ部門を標的にし、内部メールシステムを悪用してフィッシングメールを配布しました。このメールは「戦時状況の処理および医薬品使用に関するメンタリングセッション」の招待状に偽装されており、偽の Microsoft Teams ページに接続するリンクが含まれていました。受信者が Windows + R およびクリップボード活動を含む特定のユーザー指示に従うと、PowerShell ベースのシーケンスがリモートアクセス型トロイの木馬（RAT）のダウンロードと実行を開始しました。全体の感染チェーンは外部実行ファイルを使用せず、難読化された PowerShell スクリプトを使用して実行され、攻撃者はこれを通じてリモートアクセスを取得し、データ漏洩および監視を行いました。被害者の追跡は、特定のドメインにホスティングされたサーバーとのエンコードされたコマンド＆コントロール通信を通じて行われました。運用戦術は既知の脅威キャンペーンと一部重複していますが、明確な帰属は不確実です。このキャンペーンは、検出を回避するために生活基盤技術（living-off-the-land）と階層化された難読化を組み合わせた複雑なケースとして機能しています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 内部メールシステムの悪用
   b. メンタリングセッション招待状の偽装
2. [実行] ユーザー実行 (T1204)
   a. Windows + R およびクリップボード指示
   b. PowerShell コマンドの実行
3. [実行] PowerShell (T1059.001)
   a. Base64 エンコードされた PowerShell コマンド
   b. Invoke-WebRequest で追加ペイロードをダウンロード
4. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. スクリプトの持続性維持
   b. システム起動時の自動実行
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. GZip 圧縮および Base64 エンコード
   b. 文字列の逆順および難読化
6. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
   a. HTTPS を通じて C2 サーバーと通信
   b. コマンド＆コントロール通信のエンコード
7. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. コマンド結果およびデータの流出
   b. サーバーエンドポイントへの送信
8. [収集] 入力キャプチャ (T1056)
   a. ターゲットシステム情報の収集
   b. システムドメインおよびユーザー情報の確認
9. [横移動] リモートサービス (T1021)
   a. 追加の組織をターゲットに
   b. 地域内での拡散および拡張

8) SectorD02 used Spear-Phishing as Rothschild Recruiter for CFOs Attack (2025-08-20)

https://cti.nshc.net/events/view/17877

攻撃者は CFO および財務役員を対象とした巧妙なスピアフィッシングキャンペーンを実施しました。攻撃者は Rothschild & Co のリクルーターを装い、被害者を Firebase にホスティングされたフィッシングページに誘導し、カスタマイズされた CAPTCHA チャレンジを利用しました。悪性 VBS ス

クリプトと多段階ペイロードを配布し、NetBird や OpenSSH のような合法的なリモートアクセスツールをインストールして持続的なシステム制御を維持しました。初期アクセスはソーシャルエンジニアリングを通じて Firebase にホスティングされたページに誘導し、ペイロードの配信は攻撃者インフラからの ZIP アーカイブと VBS ダウンロードを含みました。持続性は RDP の有効化、隠し管理者アカウントの作成、タスクの自動化を含めて維持されました。攻撃者は複数の Firebase およびウェブアプリドメインで同じフィッシングキットを使用し、AES 暗号化されたリダイレクションのような技術を使用しました。キャンペーンの一貫した方法とアーティファクトは、組織的で適応的な性格を強調しました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. スピアフィッシングメール送信
   b. Firebase ホスティングフィッシングページへの誘導
2. [実行] コマンドとスクリプトインタープリタ: Visual Basic (T1059.005)
   a. マルウェア VBS スクリプト実行
   b. 多段階ペイロード配布開始
3. [持続性] アカウント作成 (T1136)
   a. 隠し管理者アカウント作成
   b. RDP 有効化および自動起動設定
4. [権限昇格] ブートまたはログオン自動開始実行 (T1547)
   a. NetBird サービス自動開始設定
   b. タスクスケジューラでサービス再起動設定
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. AES 暗号化されたリダイレクト使用
   b. インフラパス変更による検出回避
6. [コマンドとコントロール] リモートアクセスソフトウェア (T1219)
   a. NetBird および OpenSSH のインストールと活用
   b. リモート管理およびモニタリングチャネル維持
7. [発見] システム情報の発見 (T1082)
   a. システム情報収集
   b. ネットワーク設定および接続状態確認
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のデータ収集
   b. 収集したデータを外部へ送信
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. 継続的なデータ収集および送信

29) SectorE01 used LNK Malware disguised as conference invitations (2025-07-23)

https://cti.nshc.net/events/view/17188

攻撃対象産業群: 防衛、製造

サイバー諜報キャンペーンは、トルコの防衛産業、特に精密誘導ミサイルシステムの製造業者を対象としていました。攻撃は、無人車両システムに関心のある個人に会議の招待状として偽装したマルウェア LNK ファイルを配布することから始まりました。複数の段階からなるこの攻撃は、VLC Media Player や Microsoft Task Scheduler のような合法的なバイナリファイルを利用して、DLL サイドローディングを通じて防御を回避しました。キャンペーンの時期がトルコとパキスタンの防衛協力および地域の緊張と一致しており、地政学的な動機がある可能性を示唆していました。攻撃インフラは、指揮統制活動のために合法的なウェブサイトを模倣し、高度な社会工学的戦術を通じて戦略的情報を取得しました。今回のキャンペーンは、x64 DLL から x86 PE 実行ファイルへと技術的に進化し、改善された命令構造を示しました。キャンペーンは、プロセス注入、デジタル偵察、画面キャプチャを通じて機密情報を収集すると同時に、制御された命令実行およびデータ窃取方法を通じて作戦の安全性を維持しました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング (T1566.001)
   a. 会議招待状に偽装された LNK ファイルの配布
   b. 無人車両システムに関心のある個人を対象とする
2. [実行] コマンドとスクリプトインタープリタ: PowerShell (T1059.001)
   a. PowerShell を通じた Malware の実行
   b. Wget でホスティングサイトからファイルをダウンロード
3. [防御回避] DLL サイドローディング (T1574.002)
   a. VLC Media Player を通じて悪意のある DLL ファイルをロード
   b. 追加の文字を使用して検出を回避し、ファイル拡張子を変更
4. [持続性] スケジュールされたタスク/ジョブ (T1053.005)
   a. Microsoft Task Scheduler を利用した持続性の維持
   b. VLC Player ファイルを実行して持続性を確保
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. システムの資格情報を収集
   b. デジタル偵察およびプロファイリングを実施
6. [収集] スクリーンキャプチャ (T1113)

a. スクリーンショットを撮影し、C2 サーバーにアップロード
b. リモート環境での機密データの収集
7. [コマンドと制御] アプリケーション層プロトコル (T1071)
a. 正当なウェブサイトを模倣して C2 サーバーを運営
b. ROSERVER を通じてコマンドとデータの窃取を実施
8. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. C2 チャネルを通じてデータを窃取
b. コマンドベースの制御されたデータ転送を実施

30) SectorE04 used new Domains (2025-07-23)

https://cti.nshc.net/events/view/17195

攻撃対象産業群: 銀行、政府・行政、軍事機関

攻撃者は 2012 年から活動している高度なサイバー諜報グループで、主に南アジアと中東の政府機関、軍事組織、金融機関を標的にしてきました。攻撃者はソーシャルエンジニアリング、スピアフィッシング、ゼロデイエクスプロイトといった高度な戦術を用いてネットワークに侵入しました。内部に侵入した後、攻撃者はカスタマイズされた Malware とバックドアを使用して持続的なアクセスを確保し、機密データを流出させました。彼らの作戦は主に諜報活動、データ窃盗、情報収集を目的としており、外交および軍事機関を対象とした政治的動機の攻撃が含まれていました。代表的な攻撃事例としては、2013 年のカブールにあるインド大使館侵害、2015 年のパキスタン空軍標的攻撃、2018 年のウクライナ軍事ウェブサイト侵害があります。最近ではパキスタン政府機関に集中しており、この地域で持続的な脅威を示しています。このグループの長年にわたる成功した隠密作戦の歴史は、彼らの高度な手法に対する警戒を強調しています。

[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. 目標組織にカスタマイズされたフィッシングメールを送信
b. マルウェア添付ファイルを含む
2. [実行] クライアント実行のためのエクスプロイト (T1203)
a. ゼロデイエクスプロイトの実行
b. 脆弱性を利用して初期実行
3. [持続性] カスタムマルウェアのインプラント (T1547)
a. バックドアのインストール
b. 持続的なアクセスの維持
4. [権限昇格] 公開アプリケーションのエクスプロイト (T1190)
a. 外部攻撃面を通じた権限昇格

b. 公開アプリケーションの脆弱性を利用
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. コードの難読化
b. 検出回避技術の適用
6. [資格情報アクセス] 資格情報ダンピング (T1003)
a. 資格情報のダンプ
b. 認証情報の収集
7. [探索] システム情報の探索 (T1082)
a. システム情報の収集
b. ネットワーク環境の分析
8. [横移動] リモートサービス (T1021)
a. リモートサービスの利用
b. 内部ネットワークへの拡張
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. 機密情報の収集
10. [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. 外部サーバーへの情報送信
11. [影響] データ操作 (T1565)
a. データの改ざん
b. 情報の完全性の損傷

31) SectorE04 used Phishing Pages disguised as Government Portals (2025-08-08)

https://cti.nshc.net/events/view/17699

攻撃対象産業群: 政府・行政、防衛、軍事機関

攻撃者はネパール、バングラデシュ、トルコの政府および軍事機関を対象に、精巧なフィッシングキャンペーンを実施しました。このキャンペーンは、政府および防衛機関の公式通信を装い、武器化された文書と悪意のあるリンクを使用するスピアフィッシング技法を活用しました。攻撃は、Netlify や Pages.dev のようなプラットフォームを利用して、Zimbra ウェブクライアント、政府のメールポータル、文書アップロードサービスなどを模倣した偽のログインページをホスティングし、ユーザーの資格情報を収集しました。複数のドメイン、特に mailbox-inbox-bd.com のバリエーションが、集中管理された資格情報収集ポイントとして使用されました。このインフラは、個別の URL が発見されてブロックされても持続的な運用を保証するために、余分な経路を特徴としています。さまざまなフィッシングキットで再利用された POST スクリプトは、効率的なターゲティングのためのテン

プレートベースの配布を示しています。フィッシングキャンペーンは、信頼できるドメインテーマとサブドメインスプーフィングを活用して、バングラデシュの防衛購入総局と軍事ウェブメールシステムを侵害することに重点を置いていました。攻撃者が制御するインフラは、匿名性と悪用に優しいホスティングサービスを強調し、既知の Malware や C2 特性とは一貫して差別化を図っていました。

[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. 政府および防衛機関の公式通信を装った攻撃
   b. 武器化された文書添付ファイルの送信
2. [資格情報アクセス] 情報フィッシング (T1566.002)
   a. Zimbra ウェブクライアントおよび政府ポータルを模倣したページのホスティング
   b. ユーザー資格情報収集のための偽ログインパネルの作成
3. [コマンド＆コントロール] ウェブサービス (T1102)
   a. Netlify および Pages.dev を通じたフィッシングページのホスティング
   b. 信頼性のあるドメインテーマおよびサブドメインスプーフィングの活用
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 多数のフィッシングドメインおよびパスを使用して検出を回避
   b. テンプレートベースの配布を通じた攻撃の持続性確保

32) SectorF01 used C2 Domain in a lure campaign themed around cooperation (2025-07-28)

https://cti.nshc.net/events/view/17317

攻撃対象産業群: 外交

2025 年初頭、サイバー諜報キャンペーンは中国の第 15 次 5 カ年計画の一環として、中国-アフリカ協力を目標としていた。これは、米中間の関税戦争が再開され、東南アジア経済に影響を与える状況で発生した。サイバー敵対勢力は、先進的なサプライチェーン攻撃を通じて国内生産システムを対象にし、中国の対外貿易戦略に関する情報を収集した。別の関連する動きとして、7 月初めには中国-アフリカ協力ユニットを狙ったスピアフィッシングメールが配布された。このメールには、敏感なデータを抽出し、さらなる諜報活動を可能にする実行ファイルにリンクする悪性 LNK ファイルが含まれていた。このキャンペーンは、中国-アフリカ開発計画をテーマにした悪性添付ファイルを利用して、外交および貿易戦略を監視することを目的としていた。攻撃者は、政治的変化と経済的再編を事前に把握するために、精巧な方法を用いて情報を収集した。これは特に中国とアフリカの外交の焦点内で顕著であった。

[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 ファイルが含まれたスピアフィッシングメールの配布
   b. 中国-アフリカ協力ユニットを対象とした攻撃の実行
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. LNK ファイル実行時に悪意のある実行ファイル kyxiang.exe を呼び出す
   b. ユーザー実行を通じたマルウェアの活性化
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. システム再起動時の持続性のためにレジストリキーを作成
   b. スタートアップフォルダに悪意のあるファイルを配置
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. ファイルの難読化および暗号化技術の使用
   b. 検出を避けるためのコード難読化の適用
5. [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機密データの収集
   b. 外交および貿易戦略に関する情報の収集
6. [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. 外部サーバーとの通信を通じた情報流出

33) SectorH03 used .desktop Files Disguised as PDFs for Malware Delivery (2025-07-31)

https://cti.nshc.net/events/view/17442

攻撃対象産業群: ガス、政府・行政、石油、鉄道

攻撃者は主にインド政府部門を標的にして、精巧で持続的なサイバーキャンペーンを開始しました。鉄道システム、石油・ガスインフラ、外務省を含む主要なターゲットが選定されました。攻撃者は高度なフィッシング技術と PDF 文書に偽装された.desktop ファイルを使用してマルウェアをダウンロードし、クーロンジョブを通じて持続性を確立しました。2 つの感染チェーンが識別されており、1 つは単一のコマンド＆コントロール（C2）サーバーを使用し、もう 1 つは復元力を高めるために冗長 C2 インフラを使用しています。感染後、システムアクセスを維持するための主要なツールは Mythic フレームワークに基づく Poseidon バックドアで、持続性を強化し、資格情報の収集や潜在的な横方向移動を可能にします。フィッシングドメインはインド政府機関を装い、主に AlexHost にインフラがホスティングされており、中央集中的な制御を示しています。このキャンペーンは 2025 年 7 月に開始され、グループの戦術的進化を強調し、隠密性と持続性を重視しています。

[Attack Flow]

1. [偵察] フィッシング (T1566)
   a. インド政府機関を装ったドメインの使用
   b. PDF に偽装された.desktop 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ー (T1059)
   a. スクリプトを通じて Malware をダウンロード
   b. バックグラウンドでスクリプトを実行
3. [持続性] スケジュールされたタスク/ジョブ (T1053)
   a. クロンジョブを通じて持続性を維持
   b. ダウンロードしたペイロードの自動実行設定
4. [防御回避] 偽装 (T1036)
   a. システムファイルに偽装した悪性ファイル名の使用
   b. Google Drive にホスティングされた文書で初期の相互作用を偽装
5. [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 サーバーとの通信経路を Base64 エンコード
   b. 冗長 C2 インフラの使用で復元力を強化
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. 資格情報収集機能を含む
   b. Poseidon バックドアを通じた長期的アクセスの維持
7. [横方向移動] リモートサービス (T1021)
   a. システム情報の収集と横方向移動のサポート
   b. Mythic フレームワークに基づくモジュール設計の活用

34) SectorT01 used XLS malware disguised as Ukrainian public services documents (2025-08-20)

https://cti.nshc.net/events/view/17853

攻撃対象産業群: 政府・行政、軍事機関、反政府勢力

攻撃者は 2025 年 4 月にウクライナとポーランドを対象とした巧妙なサイバー脅威キャンペーンを実施しました。攻撃者は武器化された XLS スプレッドシートを使用し、スピアフィッシングメールを通じて配布しました。これらの XLS ファイルには難読化された VBA マクロが含まれており、マルウェア DLL をドロップおよびロードしてシステムデータを収集し、追加の悪意のあるステップを展開するように設計されています。攻撃者は各国ごとに異なる感染チェーンとツールを使用しましたが、DLL の実行に LNK ファイルを使用することや、マクロの難読化に MacroPack を使用することなどの技法を共有していました。ウクライナでは公共サービスをターゲットにしたアーカイブが配信され、ポーランドでは地方自治体に関連する文書が誘引として使用されました。両キャンペーンは、クラ

ウドベースのコラボレーションツールや合法的なウェブサイトを模倣したドメインを含むハイジャックされた C2 インフラを活用しました。攻撃者のツールセットには C#および C++のダウンローダーが含まれており、特定のキャンペーンでは Slack を通信チャネルとして活用しました。これらのインフラはウクライナとポーランドに集中したアプローチを示しており、技法の一貫性と共有されたアーティファクトの特性が国家支援のサイバー諜報活動を示唆しています。

[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を通じた XLS ファイル添付
   b. 誘引策として偽装された文書を含む
2. [実行] コマンドおよびスクリプトインタープリタ: Windows コマンドシェル (T1059.003)
   a. VBA マクロ実行後 DLL ドロップ
   b. regsvr32 を使用した DLL ロード
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 Run キー/スタートアップフォルダ (T1547.001)
   a. レジストリ Run キーを使用した持続性確保
   b. スケジュールされたタスク登録を通じた持続性確保
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. MacroPack を使用したマクロ難読化
   b. ConfuserEx を使用した DLL 難読化
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. システムデータ収集および C2 サーバーへの送信
   b. 外部 IP アドレス情報収集
6. [収集] ローカルシステムからのデータ (T1005)
   a. システム情報収集 (OS、ホスト名、ユーザー名など)
   b. WMI クエリを通じた詳細システム情報抽出
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: Web プロトコル (T1071.001)
   a. HTTP POST リクエストを通じた C2 サーバーとの通信
   b. JPEG 拡張子に偽装されたペイロードダウンロード
8. [流出] C2 チャネルを介した流出 (T1041)
   a. Base64 でエンコードされたデータ送信
   b. C2 サーバーへの定期的な情報送信
9. [影響] データ操作 (T1565)
   a. システム内ファイル操作およびレジストリ修正
   b. マルウェアペイロード実行およびシステム影響

2. サイバー犯罪（Cyber Crime）ハッキンググループの活動

1) SectorJ39 used WinRAR Vulnerability in Targeted Attacks (2025-08-11)

https://cti.nshc.net/events/view/17651

攻撃対象産業群: 金融、製造、物流、防衛

攻撃者は、WinRAR の新しいゼロデイ脆弱性である CVE-2025-8088 を利用して、2025 年 7 月 18 日から標的型攻撃を実行しました。このパス横断脆弱性は、WinRAR 7.12 以下のすべての Windows バージョンに影響を及ぼし、攻撃者はソフトウェアを欺いて意図されたディレクトリ外にファイルを抽出させることができました。この欠陥により、悪意のある DLL や実行ファイルを Windows のスタートフォルダなどの敏感な場所に配置し、ログイン時に自動的に実行されるようにします。特に、このエクスプロイトは、歴史的にゼロデイ脆弱性を悪用してきた諜報および金融活動で悪名高いハッキンググループによって実行されました。この攻撃は主にヨーロッパとカナダの金融、防衛、製造、物流部門の企業を対象に、悪意のある RAR ファイルを含むスピアフィッシングメールを通じて行われました。主要な 3 つの実行チェーンには、Mythic Agent、SnipBot Variant、そして RustyClaw の使用が含まれていました。

[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 RAR ファイル添付メール送信
   b. 特定の産業および地域をターゲット
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 RAR ファイルを抽出
   b. マルウェア DLL および実行ファイルをインストール
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. Windows スタートフォルダにマルウェア .lnk ファイルを配置
   b. 自動実行を保証
4. [防御回避] 偽装: 正当な名前または場所に一致 (T1036.005)
   a. 無害なファイルに偽装して検出を回避
   b. 長い抽出メッセージリストにエラーを含む
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: Web プロトコル (T1071.001)
   a. C2 サーバーと通信
   b. ドメイン特定ロジックを実行

6. [収集] 入力キャプチャ: キーロギング (T1056.001)
   a. キー入力を記録
   b. 機密情報を収集
7. [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送信
   b. C2 インフラを活用
8. [影響] データ操作 (T1565)
   a. システム設定を修正
   b. ファイルパスを操作

2) SectorJ72 used Raspberry Robin with Enhanced Obfuscation Tactics (2025-08-04)
https://cti.nshc.net/events/view/17535

攻撃者は、マルウェアに追加の初期化ループを導入し、平坦化された制御フローの関数でブルートフォース攻撃による復号を妨害しました。スタックポインタの難読化により IDA の逆コンパイルが妨げられ、条件文の難読化によりコード分析がさらに複雑になりました。ネットワーク通信は AES-CTR から ChaCha-20 アルゴリズムに切り替えられ、32 バイトのハードコーディングされたキーとリクエストごとにランダムに生成されたカウンターとノンスが使用されました。RC4 暗号化では、8 バイトのランダムシードをキーの末尾に追加し、サンプルおよびキャンペーンごとにハードコーディングされたキーが変わります。CRC-64 アルゴリズムの初期値はキャンペーンごとにランダムに設定されます。コマンド＆コントロール通信のために、TOR オニオンドメインの意図的に損傷された部分を動的に修正する技術を改善し、キャンペーンごとに変更されるハードコーディングされたアルゴリズムを使用しました。

[Attack Flow]
1. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 初期化ループの追加
   b. 条件文の難読化
   c. スタックポインタの難読化
   d. IDA デコンパイルの妨害
2. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
   a. ChaCha-20 でネットワークデータを暗号化
   b. RC4 暗号化にランダムシードを追加
3. [コマンド＆コントロール] ドメイン生成アルゴリズム (T1568)
   a. TOR オニオンドメイン修正アルゴリズムの使用
   b. キャンペーンごとのアルゴリズム変更

3) SectorJ93 used fake browser updates for malware distribution (2025-08-06)

https://cti.nshc.net/events/view/17536

攻撃者は、SocGholish という名前の Malware-as-a-Service（MaaS）プラットフォームを通じて、巧妙なサイバー脅威作戦を実行しました。このプラットフォームは、合法的なソフトウェアアップデートに偽装してシステムを損傷させました。攻撃グループは、初期アクセスブローカー（IAB）として、JavaScript インジェクションを通じて損傷したウェブサイトで偽のブラウザアップデートの誘引策を使用し、世界中のユーザーを対象にしました。これは、ドライブバイダウンロードを通じてマルウェアをインストールさせました。キャンペーンは、Parrot や Keitaro のような高度なトラフィック配分システム（TDS）を活用し、被害者を悪意のあるコンテンツにリダイレクトして、従来のセキュリティ対策を回避しました。SocGholish は、主にランサムウェア活動やその他の悪意のある行為に関与する財政的に動機付けられたサイバー犯罪者に、損傷したシステムへのアクセスを販売しました。この設定は、ドメインを頻繁に回転させ、ドメインシャドウイングを活用して検出を回避しました。インフラは、複数の層の C2 サーバーと動的に生成されたペイロードを含み、しばしばユーザーが信頼するソフトウェアアップデート形式を悪用して配信されました。この脅威は、特にロシアのサイバー犯罪団体と関連しており、合法的な広告技術を悪意を持って利用しました。

[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での JavaScript インジェクション
   b. 偽のブラウザ更新誘引の使用
2. [実行] ユーザー実行 (T1204)
   a. ユーザーに偽の更新ページを表示
   b. ダウンロードボタンをクリックするとマルウェアペイロードが実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. システム起動時に自動実行設定
   b. ソフトウェア更新に偽装した持続性維持
4. [防御回避] ドメインシャドウイング (T1071.001)
   a. ドメインシャドウイングを使用して検出回避
   b. 頻繁にドメインを回転
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. 複数の層の C2 サーバーを使用
   b. Tor プロキシを通じた C2 パネルのホスティング
6. [データ抽出] C2 チャネルを介したデータ抽出 (T1041)

a. C2 サーバーを通じたデータ流出
b. 感染したシステムの情報を攻撃者に送信

4) SectorJ146 used Phishing PDFs disguised as financial documents (2025-08-19)

https://cti.nshc.net/events/view/17829

攻撃対象産業群: 工学

攻撃者は 2025 年 5 月にロシアのあるエンジニアリング会社を対象に、金融関連のメッセージを含むフィッシングメールキャンペーンを開始しました。添付された PDF 文書とパスワードで保護された ZIP ファイルは、PDF に偽装された Malware ダウンローダーTrojan.Updatar.1 を実行するように設計されていました。このトロイの木馬は、他のバックドアコンポーネントをダウンロードして機密データを抽出する機能を果たしました。初期感染システムにワクチン保護がなかったため、トロイの木馬は簡単にネットワークを掌握しました。数日後、Trojan.Updatar.2 や Trojan.Updatar.3 といった追加コンポーネントが配布され、Metasploit フレームワークの Meterpreter ツールをダウンロードして深層システム侵入を行いました。複数の感染デバイスを通じて盗まれた資格情報を使用し、ネットワーク内での横方向移動が可能となり、主に Windows ユーザーアカウントデータを活用しました。攻撃者はセキュリティソフトウェアを無効化し、リモート管理、トラフィックトンネリングプロジェクト、RDP セッションを通じた持続的アクセスを確立する高度な方法を使用しました。攻撃者は主に updatingservices[.]com のようなドメインや 77[.]105.161[.]30 のような IP を使用した C2 インフラを通じて通信し、検出を困難にしました。また、トロイの木馬の機能は RockYou パスワードリストを活用した手法で難読化され、分析を複雑にしました。このキャンペーンは諜報を目的とし、データ収集とシステム制御に重点を置いています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 金融関連のフィッシングメール送信
   b. PDF および ZIP ファイルを通じて Malware を配布
2. [実行] ユーザー実行 (T1204)
   a. ユーザーによって PDF に偽装されたファイルを実行
   b. Trojan.Updatar.1 のダウンロードおよび実行
3. [持続性] BITS ジョブ (T1197)
   a. BITS サービスを通じた持続的な Malware ダウンロード
   b. ダウンロードされたバックドアコンポーネントのインストール
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. 盗まれた資格情報で管理者権限を取得
   b. RDP Wrapper のインストールを通じたリモートシステムアクセス

5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. RockYou リストを利用したトロイの木馬の難読化
   b. セキュリティソフトウェア無効化技法の使用
6. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. LSASS プロセスを通じた資格情報の窃取
   b. 盗まれたアカウントでネットワーク内に拡散
7. [探索] システム情報探索 (T1082)
   a. システム情報収集のための WMI クエリ使用
   b. 外部 IP アドレスの取得
8. [横移動] リモートサービス (T1021)
   a. RDP およびリモートサービスでネットワーク移動
   b. 様々なツールを使用したリモートコマンド実行
9. [収集] ローカルシステムからのデータ (T1005)
   a. ファイルマネージャーモジュールを通じたファイル窃取
   b. システムから収集されたデータのアップロード
10. [コマンド＆コントロール] ウェブプロトコル (T1071)
   a. C2 サーバーとウェブプロトコルを通じた通信
   b. 暗号化されたチャネルでのコマンド伝達および結果受信

5) SectorJ149 used Remcos RAT with LNK files targeting Ukrainian military (2025-07-23)

https://cti.nshc.net/events/view/17244

攻撃対象産業群: 政府・行政、軍事機関

攻撃者は 2025 年 7 月初旬を基準に、ウクライナ政府および軍事関係者を標的として Remcos RAT を積極的に配布しました。攻撃者は武器化された Microsoft LNK ファイルと PowerShell スクリプトを利用し、ウクライナ軍に関連するテーマの文書に偽装して Remcos RAT を配信しました。2024 年から進行しているこのキャンペーンは、最初の段階で LNK または PowerShell ファイルがコマンド・コントロールインフラに接続し、マルウェアペイロードをダウンロードする複雑な感染チェーンを含んでいます。ペイロードは ZIP ファイル内の複数のコンポーネントを含む HijackLoader を通じて配信され、Remcos RAT の実行に至りました。Remcos は持続的なアクセスを維持し、C2 サーバーと通信し、さまざまな監視、情報窃取およびリモート管理機能を実行しました。攻撃者の誘引策テーマの適応は、被害者の範囲を広げるための戦略の進化を示唆し、戦略的標的のための接続性を維持しつつ、休眠アクセスを優先しました。

[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. 武器化された Microsoft LNK ファイルの使用
   b. PowerShell スクリプトを通じた初期感染の試み
2. [実行] ユーザー実行 (T1204.001)
   a. LNK ファイルの実行による第一ステージの実行
   b. PowerShell スクリプトの実行による第一ステージの実行
3. [コマンドと制御] アプリケーション層プロトコル (T1071)
   a. C2 インフラとの最初の接続試行
   b. 地理的フィルタリングとユーザーエージェントの確認
4. [配信] メールによるアーカイブ (T1566.003)
   a. ZIP ファイルに含まれる HijackLoader の使用
   b. ZIP ファイル内のコンポーネントとして Remcos RAT を配信
5. [防御回避] 偽装 (T1036)
   a. 誘引文書として偽装
   b. ジャンクデータファイルとして偽装
6. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. Remcos の持続的アクセス維持
7. [収集] 入力キャプチャ (T1056)
   a. キーロギング機能の有効化
8. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. C2 サーバーへの定期的なデータ送信
9. [影響] データ操作 (T1565)
   a. PE ヘッダーの上書き
   b. システムサービス管理

6) SectorJ153 used Bulletproof Hosting Disguised as VPS for RaaS Ops (2025-08-04)

https://cti.nshc.net/events/view/17514

攻撃者は 2022 年 7 月から多数のランサムウェア・アズ・ア・サービス（RaaS）運営に関与しており、主要なランサムウェアブランド間の重複を悪用し、ロシアのサイバー諜報活動者と戦術を共有しました。攻撃インフラは LockBit や BlackCat などの主要なランサムウェアエコシステムとのつながりを示し、Citrix Bleed のような特定の脆弱性を利用しました。インフラの支援は、ロシアおよび海外法人と関連する違法ホスティングプロバイダーネットワークから来ていました。このグループは国家支援活動の仲介者として、北朝鮮や中国の高度持続的脅威（APT）作戦に関与しました。インフォスティーラーを通じた広範なサイバー犯罪ネットワークに参加し、ゼロデイ脆弱性を悪用しました。彼らの洗練された戦術は、地政学的なサイバー紛争において弾力的なインフラを可能にしました。

[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. Citrix Bleed 脆弱性 (CVE-2023-4966) の活用
   b. MOVEit 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: PowerShell (T1059.001)
   a. Cobalt Strike ビーコンの使用
   b. Powershell スクリプトの実行
3. [持続性] アカウントの作成 (T1136)
   a. 新しいユーザーアカウントの作成
   b. SSH フィンガープリントを通じた持続性の確保
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. ScreenConnect 欠陥の活用 (CVE-2024-1708/1709)
   b. システム権限の昇格試行
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. ファイル難読化技術の使用
   b. 検出を避けるためのコード難読化
6. [資格情報アクセス] ブルートフォース (T1110)
   a. Brutus ボットネットの活用
   b. 無差別攻撃の実行
7. [探索] ネットワークサービススキャン (T1046)
   a. Shodan および Fofa を通じたネットワークサービスのスキャン
   b. 脆弱なサービスの識別
8. [収集] ローカルシステムからのデータ (T1005)
   a. システムからのデータ収集
   b. 特定のファイルおよび情報の検索
9. [流出] C2 チャネルを通じたデータ流出 (T1041)
   a. ToneShell バックドアの使用
   b. コマンド＆コントロール (C2) チャネルを通じたデータ流出
10. [影響] 影響を与えるためのデータ暗号化 (T1486)
    a. LockBit および BlackCat ランサムウェアの配布
    b. データ暗号化による被害の誘発

7) SectorJ170 used CrossC2 and Cobalt Strike in global malware attacks (2025-08-14)

https://cti.nshc.net/events/view/17708

攻撃者は 2024 年 9 月から 12 月の間に CrossC2 ツールを使用して Linux システムを標的にしました。CrossC2 は Cobalt Strike Beacons の非公式な拡張で、バージョン 4.1 以上と互換性があります。攻撃者は PsExec、Plink、Cobalt Strike などの複数のツールを活用して Active Directory 環境への侵入を試みました。攻撃者は Nim 言語で書かれた ReadNimeLoader というカスタムの Malware を使用し、DLL サイドローディングを通じてペイロードの配信を促進しました。java.exe をハイジャックして jli.dll として ReadNimeLoader をロードしました。ローダーはエンコードされたファイル「readme.txt」を読み込み、メモリ上で実行し、OdinLdr シェルコードローダーを統合して Cobalt Strike Beacon ペイロードをシステムメモリ上でデコードおよび実行しました。ReadNimeLoader には BeingDebugged フラグを通じたデバッグの有無の確認や CONTEXT_DEBUG_REGISTER を活用した戦略など、高度な解析防止技術が統合されています。このキャンペーンは複数の国で観察され、ドメインの使用やツールの重複を通じて以前の既知の脅威活動と関連付けられました。CrossC2 ツールは Linux、macOS、Windows でのクロスプラットフォーム作戦を実行でき、GitHub のようなリポジトリを通じて配布された Beacons を生成できます。攻撃者は持続的な C2 通信のために SystemBC RAT の Linux 変種も配布しました。XOR エンコーディングやコード難読化などの検出回避技術を含む技術的な洗練と配布方法は脅威の高度性を強調し、一部の標的システムの限定的な防御により攻撃面が拡大する可能性を示しています。

[Attack Flow]

1. [初期アクセス] 有効なアカウント (T1078)
   a. 有効なアカウント情報の使用
   b. AD 環境への侵入試行
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. PsExec の使用
   b. Plink の使用
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. java.exe ハイジャックを通じた DLL サイドローディング
   b. ReadNimeLoader を jli.dll としてロード
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. XOR エンコーディングの使用
   b. コード難読化技術の適用
5. [防御回避] 実行ガードレール (T1480)
   a. PEB の BeingDebugged フラグを通じたデバッグ確認
   b. CONTEXT_DEBUG_REGISTER の活用
6. [防御回避] 偽装 (T1036)
   a. 正規ファイル java.exe のハイジャック

b. jli.dll に偽装された ReadNimeLoader
7. [コマンドとコントロール] 暗号化されたチャネル (T1573)
   a. SystemBC RAT を通じた持続的な C2 通信
   b. CrossC2 を通じたクロスプラットフォーム作戦の実行
8. [目的の行動] 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. エンコードされたファイル「readme.txt」のメモリ実行
9. [データ流出] C2 チャネルを通じたデータ流出 (T1041)
   a. C2 チャネルを通じたデータ流出
   b. Cobalt Strike Beacon ペイロードのメモリ内実行

8) SectorJ199 abused Steam Games to distribute Malware (2025-07-25)

https://cti.nshc.net/events/view/17266

攻撃者は 2025 年 7 月 22 日から Steam のオンラインゲームプラットフォームを悪用して情報スティーラーを配布しました。攻撃者は Steam の「Chemia」というアーリーアクセスゲームに悪意のあるファイルを挿入しました。トロイの木馬ダウンローダーがシステムを感染させ、Fickle Stealer、HijackLoader、Vidar を配布しました。Vidar は Malware-as-a-Service として公共プラットフォームを Command & Control 通信に使用しました。HijackLoader は Danabot や RedLine Stealer のような追加のマルウェアを配布するために使用されました。Fickle Stealer は PowerShell スクリプトを使用してユーザーアカウント制御を回避し、システムデータや暗号通貨ウォレット情報を含む機密情報を漏洩しました。これらの攻撃は、金融損失やアイデンティティ盗難につながる可能性のある脆弱性を示しています。1 億人以上のアクティブユーザーを持つ Steam は、侵害された場合、かなりのリスクベクターとなります。

[Attack Flow]

1. [初期アクセス] ソフトウェアサプライチェーンの妥協 (T1195.002)
   a. Chemia ゲームにマルウェアファイルを挿入
   b. Steam プラットフォームの悪用
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. PowerShell スクリプトの実行
   b. ユーザーアカウント制御の回避
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. トロイの木馬ダウンローダーによる持続性の維持
4. [防御回避] 偽装 (T1036)
   a. ゲームファイルと共に実行

b. 正常なゲームコードに偽装
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
a. システムデータの窃取
b. 暗号通貨ウォレット情報の窃取
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 (T1071)
a. 公共プラットフォームを通じた C2 通信
b. Vidar によるコマンドとコントロール
7. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. 機密情報の流出
b. ネットワークを通じたデータ送信

9) SectorJ199 used MSC EvilTwin to exploit CVE-2025-26633 vulnerability (2025-08-14)

https://cti.nshc.net/events/view/17695

EncryptHub キャンペーンは CVE-2025-26633 の脆弱性（MSC EvilTwin）を悪用して、悪性ペイロードを配信しました。攻撃者は IT サポートスタッフを装い、Microsoft Teams を通じてリモートアクセスを確立し、被害者に PowerShell コマンドを実行させました。これは、悪性.msc ファイルをドロップするスクリプトの配布につながり、MMC の脆弱性を悪用して攻撃者制御のペイロードを実行しました。キャンペーンは Web3 開発者を対象としており、Brave Support や Steam のような信頼できるプラットフォームを悪用してマルウェアを拡散しました。EncryptHub は SilentCrystal という Golang でコンパイルされたローダーと SOCKS5 プロキシバックドアを配布し、持続的な C2 サーバー接続を促進し、PowerShell ベースの情報窃取ツールを実行しました。キャンペーンはまた、ビデオ会議用の偽プラットフォームを使用して悪性 DLL を含むインストーラーを配布し、AES 暗号化されたコマンドを使用してネットワーク通信のステルス性と制御を維持しました。脅威アクターは洗練された技術を示し、検出を避けるために適応し、持続的な脅威インテリジェンスと保護措置の重要性を強調しました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング (T1566.002)
a. IT サポートスタッフを装う
b. Microsoft Teams リクエストを送信
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 コマンドを実行
b. Invoke-RestMethod を使用
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. .msc ファイルをドロップ

b. マルウェアファイルを MUIPath に配置

4. [防御回避] 偽装: 正当な名前または場所に一致 (T1036.005)

a. 模擬ディレクトリを作成

b. 正当な MSC ファイルを実行

5. [資格情報アクセス] OS 資格情報ダンピング: LSASS メモリ (T1003.001)

a. 暗号化されたコマンドを受信

b. 情報スティーラーを展開

6. [探索] システム情報探索 (T1082)

a. システム情報を収集

b. C2 サーバーに送信

7. [コマンドとコントロール] 暗号化チャネル (T1573)

a. AES で暗号化されたコマンドを受信

b. コマンドを復号して実行

8. [データ引き出し] C2 チャネルを介したデータ引き出し (T1041)

a. 機密ファイルを盗む

b. 暗号通貨ウォレットデータを盗む

10) SectorJ210 used PipeMagic disguised as ChatGPT Desktop App (2025-08-18)

https://cti.nshc.net/events/view/17785

攻撃対象産業群: 金融、IT

攻撃者は PipeMagic というモジュラー型バックドアを配布しました。このバックドアは合法的なオープンソースの ChatGPT デスクトップアプリケーションに偽装されていました。攻撃者は CVE-2025-29824 の脆弱性を利用して、Windows 共通ログファイルシステム(CLFS)で権限を昇格させました。この攻撃はアメリカ、ヨーロッパ、南アメリカ、中東などの様々な地域の IT、金融、不動産など多様な部門を対象としていました。PipeMagic の高度なアーキテクチャは、動的ペイロードの実行と専用ネットワーキングモジュールを通じた強力な C2（コマンド＆コントロール）通信を可能にしました。攻撃者は RC4 暗号化、SHA-1 検証、名前付きパイプを通じた安全なプロセス間通信技術を活用しました。攻撃ベクターは certutil を使用してトロイの木馬化されたファイルをダウンロードし、それを通じて PipeMagic をメモリ内で実行する方法で進行しました。攻撃の目的は、隠密で持続的な状態を維持しながらランサムウェアの配布を可能にすることでした。

[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. トロイの木馬化された ChatGPT デスクトップアプリケーションの使用
   b. メモリ内でのマルウェアドロッパー実行
2. [実行] コマンドおよびスクリプトインタープリター: Certutil (T1059.003)
   a. certutil を通じてマルウェアファイルをダウンロード
   b. MSBuild ファイルを通じて PipeMagic を実行
3. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. CVE-2025-29824 脆弱性の悪用
   b. Windows CLFS での権限昇格の実行
4. [防御回避] 偽装 (T1036)
   a. 正規のアプリケーションに偽装
   b. モジュラー型バックドアでの検出回避
5. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. 継続的なモジュール更新
   b. メモリ内モジュールの保存および維持
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: HTTP(S) (T1071.001)
   a. C2 サーバーとの TCP 通信
   b. ネットワークモジュールを通じた C2 データの送信および受信
7. [収集] ローカルシステムからのデータ (T1005)
   a. システム情報の収集および送信
   b. ホストの固有識別子の活用
8. [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. モジュールおよびシステム情報の収集後送信
9. [影響] 影響のためのデータ暗号化: ランサムウェア (T1486)
   a. ランサムウェアの配布
   b. ファイルの暗号化およびシステム影響力の拡大

11) SectorJ217 used Interlock RAT Backdoor via KongTuke Site (2025-07-31)

https://cti.nshc.net/events/view/17459

攻撃対象産業群: マネージドサービスプロバイダー

2025 年 7 月、ランサムウェアグループが北米とヨーロッパの複数の組織を対象に PHP ベースのバックドアを使用して「Interlock RAT」を配布しました。攻撃は、被害者が改ざんされたウェブサイトを訪問することから始まり、ClickFix という技術を通じて悪意のある PowerShell コマンドを実行するようリダイレクトされました。この技術はソーシャルエンジニアリングを利用して Windows シ

ョートカットを実行するよう誘導し、「Simple Process Launcher」（c2.exe）というコンポーネントを配布しました。このランチャーは追加の悪意のある PowerShell スクリプトを呼び出し、PHP インタープリターをダウンロードして「config.cfg」という難読化されたバックドアファイルを実行しました。バックドアは追加の偵察やデータ窃取のためのコマンドをサポートし、スケジュールされたタスクを通じて持続性を維持しました。被害者システムのフィンガープリント情報収集は追加の悪意のある活動に先立って行われ、詳細なシステム情報が C2 サーバーに送信されました。グループは NodeJS と PowerShell を活用してペイロードを実行しました。C2 通信は XOR キーを使用してコマンドと応答を復号化する暗号化されたデータ交換を含みました。プロセス注入やユーザーインターフェースを欺くといった高度な技術を使用して検出を回避し、コマンドを秘密裏に実行しました。

[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の訪問
   b. マルウェアの PowerShell コマンドリダイレクト
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. Windows ショートカット実行の誘導
   b. "Simple Process Launcher" (c2.exe) の配布
3. [実行] コマンドとスクリプトインタープリター: PowerShell (T1059.001)
   a. 追加のマルウェア PowerShell スクリプトの呼び出し
   b. PHP インタープリターのダウンロードと実行
4. [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維持
5. [発見] システム情報の発見 (T1082)
   a. システム情報の収集
   b. C2 サーバーへの情報送信
6. [コマンドとコントロール] 暗号化されたチャネル (T1573)
   a. XOR キーを使用したコマンドと応答の復号化
   b. 暗号化されたデータ交換
7. [防御回避] プロセスインジェクション (T1055)
   a. プロセス注入
   b. ユーザーインターフェースの欺瞞

12) SectorJ217 used ClickFix technique with compromised sites for attacks (2025-08-16)

https://cti.nshc.net/events/view/17753

攻撃対象産業群: 健康、政府・行政、教育、技術

インターロックランサムウェアグループは 2024 年 9 月から観察されており、機会主義的なオペレーターとして、損傷したウェブサイトと巧妙な社会工学技術を利用してペイロードを配信しました。このグループは、従来の RaaS モデルとは異なり、自律的に運営され、カスタマイズされた流出サイトを使用していました。2025 年 7 月、彼らはミネソタ州セントポールを攻撃し、過去 11 ヶ月間に北米およびヨーロッパの企業と重要インフラを対象に攻撃を行いました。このグループの戦術には、被害者を損傷したサイトにリダイレクトし、無意識のうちに Malware をダウンロードさせる「ClickFix」が含まれます。この方法は、合法的なプラットフォームのように見える偽のソフトウェアアップデーターを通じて初期アクセスを試みます。ユーザーが実行したバックドア PowerShell スクリプトは、コマンド＆コントロールサーバーと通信し、追加の活動を可能にします。彼らはトラフィックマスキングのために Cloudflare のようなサービスを使用してプロセスを難読化します。二重恐喝を実行し、データを暗号化して奪取し、身代金を支払わない場合は被害を公開すると脅迫します。急速な進化を通じて、攻撃ベクターとプラットフォームの悪用を通じた回避技術を含む戦術を発展させてきました。

[Attack Flow]

1. [初期アクセス] ユーザー実行 (T1204.002)
   a. 偽のソフトウェアアップデーターのダウンロード
   b. 侵害されたウェブサイトを通じた Malware 実行の誘導
2. [実行] PowerShell (T1059.001)
   a. バックグラウンドでの PowerShell スクリプト実行
   b. コマンド＆コントロールサーバーとの継続的な通信
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 文字列マッチング回避のための難読化
   b. Cloudflare サービスを利用したトラフィックマスキング
4. [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. Windows レジストリキーを通じた持続性の確保
   b. スクリプトを通じた任意コマンドの受信と実行
5. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. システム情報、ユーザー権限などのデータ収集
   b. C2 エンドポイントへのデータ圧縮と送信
6. [影響] 影響のためのデータ暗号化 (T1486)
   a. データの暗号化と窃取
   b. 身代金未払い時のデータ流出の脅威
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. HTTP リクエストを通じたリモートホストのポーリング
b. コマンドとペイロード送信のための C2 通信

13) SectorJ224 used Malware and GSocket for Cryptomining (2025-07-21)

https://cti.nshc.net/events/view/17133

攻撃対象産業群: IT

攻撃者は、Magento e コマース CMS プラットフォームの脆弱性を悪用するために戦術を調整しました。以前は Craft CMS を標的としていましたが、現在は未確認の PHP-FPM 脆弱性を利用して Magento を攻撃しています。このマルウェアグループは、巧妙な持続性と回避方法を使用し、合法的な GSocket ツールを使用して持続的な不正アクセスを維持しています。このツールはネットワーク制限を回避し、強力な暗号化を使用します。持続性は SystemD サービスユニット、crontab、およびレガシーrc.local 初期化を通じて維持されます。マルウェアはカーネルスレッド名に偽装し、メモリを通じて運用し、検出を回避するための様々なプロセス難読化技術を使用します。攻撃者は /etc/ld.so.preload を通じて alamdar.so ルートキットを注入し、悪意のある活動を隠す追加の保護層を加えました。CPU および帯域幅の搾取方法を通じてリソースを収益化するために、暗号通貨のマイニングおよびプロキシジャッキングを活用します。また、誤って構成された Docker インスタンスを標的にして攻撃範囲を拡大する追加の攻撃を行います。これらの進化は、向上した技術的能力と金銭的利益を目的とした意図を強調しています。

[Attack Flow]

1. [初期アクセス] 公開向けアプリケーションのエクスプロイト (T1190)
   a. Magento CMS の PHP-FPM 脆弱性の利用
   b. 誤って構成された Docker インスタンスのスキャンおよび悪用
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
   a. GSocket ベースのリバースシェルのダウンロードおよび実行
   b. Base64 エンコードコマンドの実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. SystemD サービスユニットの使用
   b. rc.local 初期化の使用
4. [権限昇格] 権限昇格制御メカニズムの悪用 (T1548)
   a. alamdar.so ルートキットの注入
   b. /etc/ld.so.preload の修正
5. [防御回避] 偽装 (T1036)
   a. カーネルスレッド名でプロセスを偽装
   b. メモリ上での運用による検出回避

6. [資格情報アクセス] 保護されていない資格情報 (T1552)
   a. SSH 設定ファイルから公開鍵を検索
   b. known_hosts ファイルから情報を取得
7. [探索] システムネットワーク接続の探索 (T1049)
   a. Go の net.dial 機能で外部 IP アドレスを確認
   b. ローカルサブネット内のランダムホストに SSH 接続を試行
8. [収集] ローカルシステムからのデータ (T1005)
   a. ファイルシステム I/O 作業の実行
   b. プロセス情報の収集
9. [コマンドと制御] 暗号化されたチャネル (T1573)
   a. GSocket を通じた暗号化された C2 チャネルの設定
   b. 多様な C2 サーバーを通じた通信
10. [影響] リソースのハイジャック (T1496)
    a. XMRig 変種を通じた暗号通貨の採掘
    b. IPRoyal Pawns クライアントを通じた帯域幅の再販売

14) SectorJ224 used RCE Vulnerability to Deploy 4L4MD4R Ransomware (2025-07-30)

https://cti.nshc.net/events/view/17387

攻撃対象産業群: ヘルスケア

攻撃者は 2025 年 7 月に Microsoft SharePoint サーバーの深刻なリモートコード実行（RCE）脆弱性を悪用しました。この攻撃は数千台のサーバーに影響を与えました。[Attack Flow]は w3wp.exe プロセスから始まり、cmd.exe を呼び出し、powershell.exe を実行して実行ポリシーを回避し、感染したイタリアのウェブサイトからペイロードをダウンロードしました。ペイロードは Golang で書かれた新しいランサムウェア 4L4MD4r で、関数名に宗教的な色合いが濃いです。このランサムウェアはメモリ内でペイロードを復号し、システムごとの ID と暗号化キーを生成して.4l4md4r 拡張子でファイルを暗号化しました。暗号化された JSON を攻撃者のサーバーに送信するのに 3 回失敗すると、プロセスは終了しました。暗号化されたファイルの名前は base64 形式に変換され、被害システムにはランサムノートが残されました。報告時点までに身代金の支払いは記録されていませんでした。

[Attack Flow]

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. SharePoint サーバーの RCE 脆弱性を利用
   b. 外部に公開された SharePoint サーバーで悪性 PowerShell コマンドを実行

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. cmd.exe を通じて powershell.exe を呼び出し
   b. 実行ポリシーを回避して悪性ペイロードのダウンロードを試みる
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. PowerShell コマンドをエンコードして検出を回避
   b. メモリ内でペイロードを復号
4. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. メモリに復号された PE ファイルをロード
   b. 新しいスレッドを生成して実行を持続
5. [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. 暗号化された JSON を攻撃者のサーバーに送信しようとする
   b. 通信が失敗した場合、プロセスを終了
6. [影響] 影響のためのデータ暗号化 (T1486)
   a. ファイルを.4l4md4r 拡張子で暗号化
   b. 暗号化されたファイル名を base64 に変換
7. [影響] システム回復の抑制 (T1490)
   a. デスクトップにランサムノート DECRYPTION_INSTRUCTIONS.html を生成
   b. 暗号化されたファイルリスト NCRYPTED_LIST.html を生成

15) SectorJ242 used AMOS Stealer variant (2025-08-20)

https://cti.nshc.net/events/view/17838

攻撃者は 2025 年 6 月から 8 月の間に 300 以上の環境を標的にして、SHAMOS という macOS 情報窃取の亜種を配布しました。この作戦は、ユーザーを詐欺的な macOS ヘルプウェブサイトに誘導する悪意のある広告を使用して、悪意のある一行インストールコマンドの実行を促しました。このコマンドは macOS Gatekeeper の検査を回避し、情報窃取のための Mach-O 実行ファイルをインストールしました。キャンペーンはロシアを除く全世界のユーザーを対象としており、これは CIS 諸国での Malware 配布制限が原因と見られます。攻撃者はオーストラリアの電子商店に偽装した Google 広告プロファイルを使用して、被害者を mac-safer[.]com のようなサイトにリダイレクトしました。インストールコマンドは Base64 文字列をデコードし、悪意のあるサーバーから Bash スクリプトをダウンロードし、セキュリティ対策を回避し、機密資格情報を収集し、データを漏洩する作業を行いました。このグループはまた、合法的なソフトウェアに偽装して GitHub リポジトリを活用し、Malware を配布し、Base64 難読化およびユーザープロンプトを使用して感染を誘導しました。

[Attack Flow]

1. [初期アクセス] ドライブバイ妥協 (T1189)
   a. 悪性広告の使用
   b. 詐欺的な macOS ヘルプウェブサイトへの誘導
2. [実行] ユーザー実行 (T1204)
   a. 悪性の一行インストールコマンドの実行
   b. ユーザープロンプトの使用
3. [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. Base64 でスクリプトダウンロード URL を難読化
   b. Gatekeeper の回避
4. [持続性] Plist 修正 (T1547.011)
   a. com.finder.helper.plist ファイルの作成
   b. LaunchDaemons ディレクトリに保存
5. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. キーチェーンおよび敏感な資格情報ファイルの収集
   b. 暗号通貨ウォレットファイルの検索
6. [収集] ローカルシステムからのデータ (T1005)
   a. AppleScript コマンドでホスト偵察
   b. ブラウザおよび AppleNotes データの収集
7. [流出] C2 チャネル経由の流出 (T1041)
   a. curl を利用したデータ送信
   b. out.zip ファイルでデータを圧縮および送信
8. [コマンドと制御] アプリケーション層プロトコル (T1071)
   a. 追加の悪性ペイロードのダウンロード
   b. スプーフィングされた Ledger Live ウォレットおよびボットネットモジュールの配布

今月のサイバー脅威の特徴

最近のサイバー脅威活動で見られる主な特徴は、攻撃者の技術と戦術がますます高度化している点です。過去にもマルウェアの拡散に一般的に使用されていたメールの添付ファイル、フィッシングメッセージ、マクロ文書といった伝統的なベクターが引き続き登場していますが、これらが単に繰り返し使用されるのではなく、精巧に改善された形で再び現れています。特に LNK ファイルを利用した攻撃が多く観察されており、単純なショートカットアイコンファイルに偽装されたこのファイルは、ユーザーが実行する瞬間に内部に挿入された PowerShell ベースのスクリプトを通じて二次ペイロードをダウンロードします。この過程で文字列難読化、コマンド分割、ランダムなコメント挿入などの技術が適用され、静的分析ツールによる検出を困難にしています。マクロ文書の場合も Excel、Word

、HWP など様々な形式で作成され、正常な文書に見えるように装ったデコイファイルと共に提供され、ユーザーが脅威を認識しにくくなっています。フィッシングメールも単純なソーシャルエンジニアリング技術を超えて、実際の企業や機関の文書形式、ロゴ、署名まで精巧に偽造し、被害者が信頼できるように設計されています。

検出を回避するために攻撃者が選択する手法はますます多様化しています。最近の事例では、ChaCha-20、RC4、AES-CTR などの複数の暗号化アルゴリズムが混合して使用され、CRC-64 の初期値をランダム化する方法も観察されました。これはネットワーク分析および Malware リバースエンジニアリングのプロセスを困難にし、同じ Malware 系列であってもキャンペーンごとに変形された難読化と暗号化パターンを示します。したがって、攻撃者が単純な繰り返しではなく、分析妨害と追跡回避を意図的に設計していることが確認できます。また、PowerShell、WMI、DLL ハイジャックなどの Living-off-the-Land 手法も依然として活発に使用され、正当なプロセス環境内で悪意のある行為を隠蔽します。これは検出を困難にするだけでなく、セキュリティソリューションが正常なオペレーティングシステムプロセスをブロックできないようにする効果を持ちます。

感染後の段階では、攻撃者は情報収集と資格情報の窃取に集中します。ブラウザに保存された資格情報、システム情報、キー入力の記録、ローカルファイルなどが主な収集対象であり、特にキー入力データを特定のパスに保存した後、暗号化して外部の C2 に送信する事例が報告されています。この過程で合法的なクラウドサービスが悪用されることが多いです。GitHub、Dropbox、Netlify、PubNub などがマルウェア通信チャネルとして利用され、正常なトラフィックに偽装することでセキュリティモニタリングを回避します。攻撃者が合法的なプラットフォームを C2 に使用する傾向は、従来のセキュリティ体制に大きな負担を与え、攻撃と正常な活動を区別することを困難にします。

多段階攻撃チェーンの活用も顕著です。初期侵入後、追加モジュールが連続的にダウンロードされ実行され、最終的にはシステムの掌握、情報漏洩、ランサムウェアの配布に至ります。この過程で、Meterpreter、Remcos RAT、Trojan.Updatar などの様々なマルウェアツールが組み合わされて使用されます。このような構造は単一のセキュリティソリューションでブロックするのが難しく、長期的に被害組織内部に留まり、持続的な情報窃取と制御を可能にします。攻撃者は単一のペイロードに依存せず、多層的なモジュール構造を通じてセキュリティシステムを継続的に圧迫しています。

総合すると、今月のサイバー脅威の特徴は、攻撃手法が単純な繰り返しではなく、持続的に進化している点です。攻撃ベクターは同じでも、検出回避技術や難読化手法が高度化し、合法サービスの悪用による隠蔽戦略が強化され、多段階攻撃チェーンによって被害範囲を最大化する事例が増えています。これは、セキュリティ対応が一層困難になったことを示すと同時に、単一のソリューションや特定の防御手法だけでは十分でないことを示唆しています。結局、特徴は技術的多様化、検出回避、隠蔽、多段階構造という 4 つの軸で説明でき、これは今後の防御戦略の策定において必ず考慮すべき要素として位置づけられています。

今月のサイバー脅威の示唆点

最近観察された脅威の動向で最も重要な示唆は、攻撃者の活動が単なる技術的行為に留まらず、戦略的な次元へと発展している点です。国家支援のハッキンググループとサイバー犯罪グループが同時に活発に動いており、特定の産業群や地域を狙ったカスタマイズされた攻撃が続いています。攻撃手法はスピアフィッシング、悪性 LNK、DLL ハイジャック、脆弱性エクスプロイトなど多様化しており、各キャンペーンには被害者が簡単に騙されるように社会工学的手法が組み合わされています。例えば、偽のインタビュー手続きを通じて悪性スクリプトを実行させたり、偽のメールやウェブサイトでユーザーの信頼を得る方法が代表的です。

このような動向は、従来の署名ベース、パターンベースの検出システムが限界に達していることを示しています。攻撃者は正常なサービスと合法的なトラフィックを積極的に利用して、悪意のある行為を隠します。Netlify、Dropbox、GitHub、PubNub のようなプラットフォームが悪性 C2 チャネルとして悪用され、これにより検出と防御の難易度が一層高まります。また、攻撃者は既知の脆弱性と新規の脆弱性を同時に利用します。DirtyCoW、PwnKit のような古い権限昇格脆弱性が依然として使用されている一方で、SharePoint の脆弱性などの新しい問題も迅速に悪用されます。これは最新のセキュリティパッチの適用だけでなく、既存の脆弱性管理がどれほど重要であるかをよく示しています。

産業別では、政府・行政、国防、金融、通信、エネルギー、メディア、NGO、暗号通貨分野が主要な標的となっています。韓国政府機関を狙ったキャンペーンでは、政府の通知を装った LNK ドキュメントが使用され、ロシアのエンジニアリング会社が金融関連のフィッシング PDF キャンペーンのターゲットとなりました。特定の企業や機関を模倣する事例も増えており、クレジットカード会社のセキュリティメール認証画面を装った攻撃も確認されました。これは、攻撃者が対象産業の運用環境や状況を綿密に調査した上で攻撃戦略を立てていることを示しています。

社会工学手法の高度化は、もう一つの示唆点です。Contagious Interview キャンペーンや PyLangGhost RAT の配布事例は、信頼を基盤とした人間心理の操作が技術的防御を超える可能性があることを示しています。偽のインタビュー、偽のアップデート、偽の書類を通じた攻撃は、検出を極めて困難にし、単純な技術的遮断だけでは防ぐことが難しいです。したがって、セキュリティ意識の向上と内部報告体制の強化が不可欠です。

サービス型犯罪エコシステムの拡大も注目すべき点です。ランサムウェアサービス（RaaS）、マルウェアサービス（MaaS）などが拡散することで、攻撃者は直接マルウェアを開発しなくても高度な攻撃を実行できるようになりました。SocGholish のような MaaS プラットフォームや、LockBit Black、Warlock のようなランサムウェアの亜種が代表的な例です。このような構造は、技術力の低いアクターでさえも精巧な攻撃を容易に実行できるようにし、脅威の裾野を広げ、全体的なリスク度を引き上げます。

今月の示唆点は結局 5 つに要約される。第一に、国家支援グループとサイバー犯罪グループの活動が同時に活発化し、脅威レベルが強化されている。第二に、合法的なサービスを利用した隠蔽戦略が増加し、検出の難易度が大幅に上昇している。第三に、産業別のカスタマイズ攻撃が拡散しており、防御戦略も産業特化の観点から設計される必要がある。第四に、既存の脆弱性と新規の脆弱性が同時に悪用されており、パッチ管理とセキュリティチェックの重要性が強調されている。第五に、攻撃サービスのエコシステムの拡散により、脅威へのアクセスが容易になり、攻撃頻度が高まっている。これらの示唆点は、組織レベルで単なる技術的対応を超え、脅威インテリジェンスに基づく事前防御、セキュリティ意識の教育、多層的なセキュリティ戦略の策定、インシデント対応体制の整備が必須であるという結論につながる。

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)

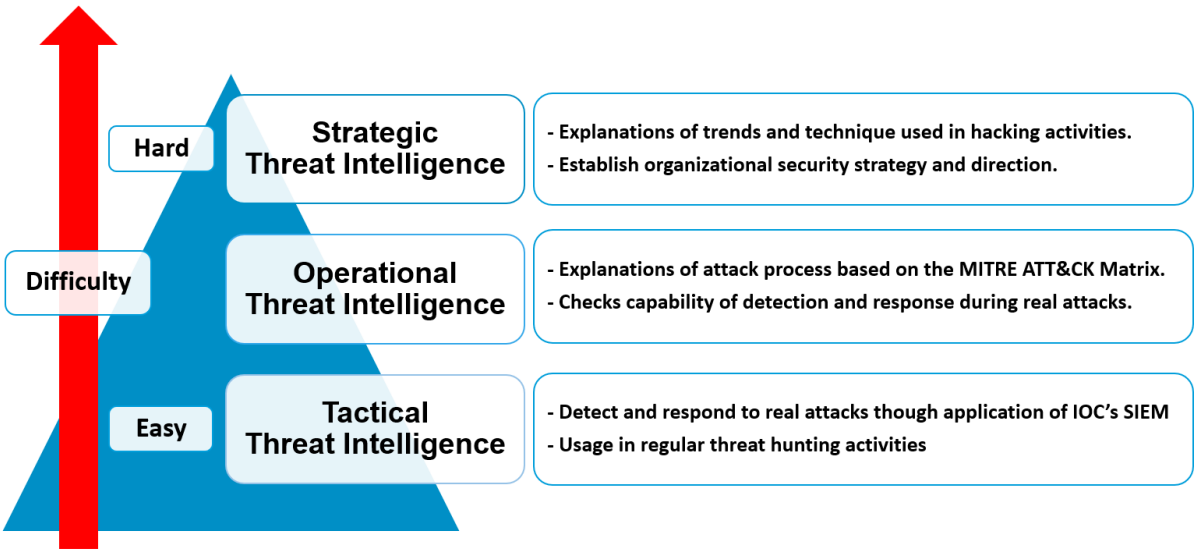
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

- 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

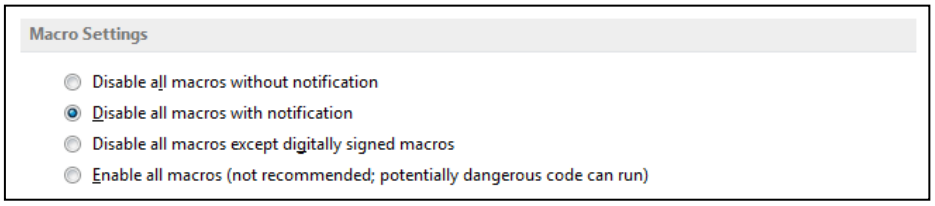
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

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.