NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI2025120202

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

Nov 2025

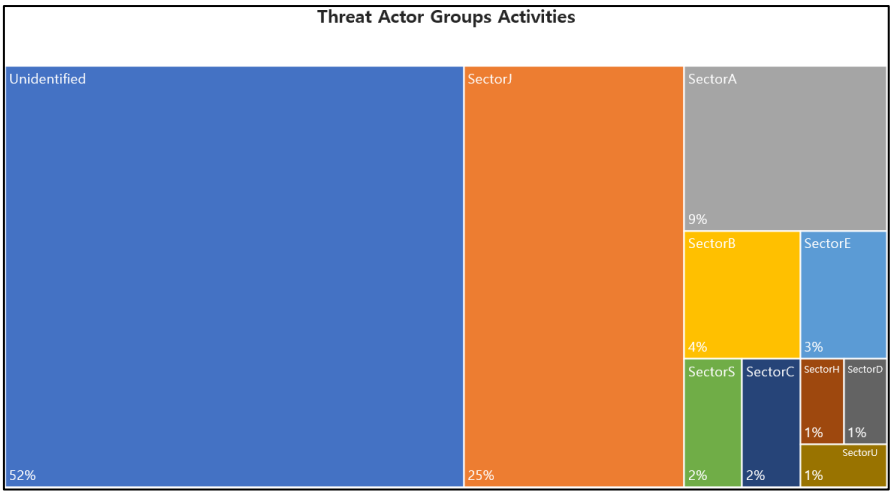
NSHC PTE. LTD.

このレポートは 2025 年 10 月 21 日から 2025 年 11 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

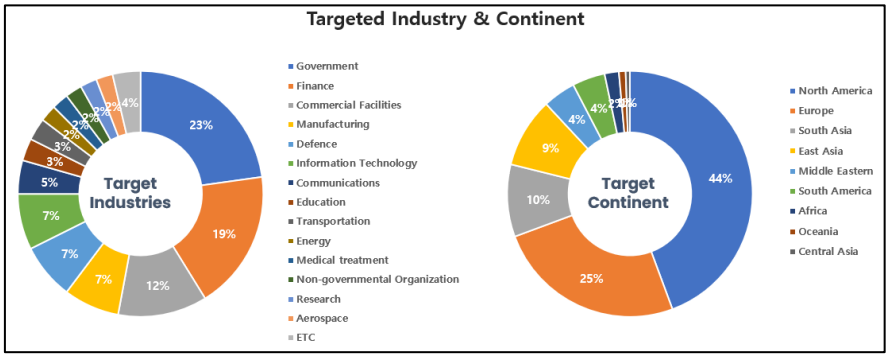
エグゼクティブサマリー

2025 年 10 月 21 日から 2025 年 11 月 20 日まで NSHC 脅威分析研究所(Threat Research Lab)で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)の活動を要約整理した内容である。
今回 11 月には、合計 82 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 52%で最も多く、SectorJ、SectorA グループの活動がそれに続いた。



[図 1: 2025 年 11 月に確認されたハッキンググループ別活動統計]

今回 11 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分野に従事する関係者またはシステムを対象に最も多くの攻撃を行い、地域別では北アメリカ(North America)とヨーロッパ(Europe)に位置する国家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る。



[図 2: 2025 年 11 月攻撃対象となった産業分野と国家統計]

SectorA グループは、採用・業務提案の偽装、開発者対象の社会工学、メッセンジャー基盤のアプローチなど、様々な心理欺瞞技法を活用して技術・防衛産業・航空宇宙・Web3・モバイル生態系を集中的に狙う。初期侵入は主にスピアフィッシング文書、LNK・VHDX 基盤の実行チェーン、トロイの

木馬化された開発プロジェクト、メッセンジャープラットフォームを通じた偽装ファイル送信などを活用して行われる。彼らは GitHub、Bitbucket、Telegram、LinkedIn、WhatsApp など正常プラットフォームを攻撃インフラとして積極的に悪用し、悪性スクリプト・バックドア・情報窃取モジュールを多段階形態で体系的に配布する。Malware は ChaCha20、AES-128、RC4 など様々な暗号化アルゴリズムを混合してペイロード復号化と C2 通信を隠蔽し、DLL サイドローディング、難読化されたスクリプト、正常実行ファイル基盤ローディング(LOLBins)などを使用して検出を回避する。また、macOS・Windows・Android をすべて包含するマルチプラットフォーム感染構造を運営し、ビデオ通話・コーディングテスト偽装・インストール型開発プロジェクトなどを活用して Web3 開発者、暗号通貨トレーダー、航空宇宙エンジニア、IT 人材などを主要ターゲットとする。全般的に SectorA グループは、高度化された社会工学、正常開発・メッセンジャープラットフォーム悪用、マルチステージ攻撃チェーン、暗号化基盤隠蔽、マルチプラットフォームサポートなど複合戦術を結合して長期間の隠密な侵入と技術・財務情報収集を遂行する特徴を示す。

SectorB グループは、高度な脆弱性（ゼロデイを含む）悪用、サプライチェーン・アップデートチャネルハイジャック、ネットワーク機器掌握、ShadowPad 系ツールキット、DLL サイドローディング、BYOVD などの高度な技術を組み合わせた持続型スパイ・ランサムウェア作戦を遂行する。初期侵入には、Atlassian・SharePoint・ActiveMQ・WSUS・WinRAR など広く使用されているエンタープライズソフトウェアの脆弱性を積極的に活用し、一部はルーター・VPN・エンドポイント管理ソリューションを先に侵害して攻撃インフラを外部から内部へ連携する。

これらは、DNS query 回避、Malware アップデート注入、スクリプトベースのローダー、PowerShell・Certutil・Revsocks・PetitPotam などの正常なツールの組み合わせ、msbuild ベースのスケジュールタスク登録を通じて内部ネットワークの拡散と長期潜伏を実行します。また、ShadowPad、Zingdoor、KrustyLoader、様々なネットワーク型バックドアなどの高度なモジュールを使用して、資格情報の窃取、lateral movement、データ窃取、リモート制御を精巧に行います。一部のグループは高度なランサムウェア運用に熟練しており、DLL サイドローディングおよび BYOVD ベースのセキュリティ製品無効化後に暗号化モジュールを配布し、攻撃者別のアクセス権を販売する Access-as-a-Service モデルを運営することもあります。全体として SectorB グループは、最新の脆弱性、サプライチェーン攻撃、高度なバックドア、難易度の高いネットワーク隠蔽技術を組み合わせた戦略的サイバー作戦を駆使し、長期的なスパイ活動と高付加価値ランサムウェア運用を並行する高脅威群です。

SectorC グループは、伝統的な Malware よりも Web シェル、PowerShell、VBScript、HTA ファイル、スクリプトベースのローダーなど Living-off-the-Land 中心の戦術を積極的に活用します。攻撃は主にスピアフィッシングベースのドキュメント・RAR・HTA ファイルを通じて開始され、難読化されたスクリプトで URL・パスを動的に組み合わせて分析を困難にします。また、正常な Web サーバーの脆弱性を悪用して Localolive のような Web シ

エルを配布し、システム診断ツールを偽装して活用し、ネットワーク偵察と資格情報の取得を行います。

このグループは多段階感染チェーンを好み、初期ローダーは PowerShell ベースのペイロードをデコードした後、追加モジュールをダウンロードする。感染インフラは短い有効期間および循環型構造で維持され、ファイル名・サーバーアドレス・暗号化キーが頻繁に変更され追跡が困難である。

一部の作戦では、NGO や政府機関などを対象に、武器化された PDF、偽装された Zoom ページ、WebSocket ベースの RAT などが用いられ、Windows や Android など複数のプラットフォームを横断している。SectorC グループの核心特徴はスクリプト中心攻撃構造、ロー・プロファイル運営、多段階ローダー、頻繁なインフラ交換、長期的な情報収集であり、非常に隠密で分析抵抗的な形態の作戦を展開する。

SectorD グループは政府・軍事・航空宇宙・政策分野など高価値目標を中心に作戦を遂行し、社会工学・供給網侵害・文書ベースのスクリプト攻撃・メッセンジャーベースの関係構築など多様なアプローチを結合します。初期侵入はスピアフィッシングや認証情報の盗用に基づき、PDF・DOC 偽装ファイルのマクロ、偽の会議招待状、健康・採用テーマのウェブサイトなど現実的な餌を活用します。技術的には PowerShell ベースのバックドア、DLL ハイジャック、DCSYNC ベースの AD 侵害、ファイルレス実行、クラウドサービス(WebDAV, Telegram, Discord など)ベースの C2、RMM ツールを通じたリモート制御など多様な高度機能を使用します。一部の活動は WhatsApp などメッセンジャープラットフォームで長期間信頼を構築した後、標的に悪性ペイロードを伝達する関係型社会工学(relationship-based social engineering)方式を使用します。SectorD グループはバックドア、スクリプトローダー、アカウント奪取ツール、リモート制御モジュールなどを組み合わせ、長期的な侵入・情報収集・資格証明確保を目標に戦略的スパイ活動を遂行します。活動全般は高位標的中心、社会工学高度化、クラウドインフラ悪用、AD 侵入、ファイルレス・モジュール型攻撃チェーンが核心特徴です。

SectorE グループは南アジア中心の外交・政府・軍事・教育機関を標的とし、ドキュメント・アップデート・ログインページ偽装ベースのスピアフィッシングと脆弱性悪用を結合した攻撃を実行する。初期感染段階では、悪性 PDF、Word ドキュメント、ClickOnce ベースのインストールチェーン、正常ソフトウェア（例: MagTek プログラム）悪用 DLL サイドローディング、ジオフェンシングベースの URL などを使用して検出を回避する。

また、Zimbra などの正常なウェブメールログインページを精巧に模倣したフィッシングワークフローを構築し、PDF 文書を通じて被害者を誘引した後、アカウント情報を窃取します。

一部の作戦は、WinRAR ディレクトリトラバーサル脆弱性 (CVE-2025-6218) を悪用して Normal.dotm テンプレートを操作し、Word マクロを通じて追加ペイロードのダウンロードとリモートコマンドの実行を行います。

全体として、SectorE グループは正常なソフトウェアの偽装、DLL サイドローディング、ジオフェン

シングインフラ、文書ベースのマクロ、ウェブメールフィッシングを組み合わせて、外交・軍事インフラに深く侵入する長期的なスパイ活動を行います。
SectorH グループは Linux ベースの政府システムを精密に狙い、ZIP・DESKTOP ファイルを活用した多段階スクリプトベースのインストール構造を使用する。フィッシングメールを通じてステージングサーバーから Malware アーカイブをダウンロードさせ、Bash スクリプトを通じてペイロードを/tmp ディレクトリでデコード・実行する。配布されるリモート制御ツールは WebSocket ベースの C2 通信、多数の Linux 特化持続性技法、ネットワーク偽装用の偽データ生成、ファイル操作・クライアント管理など広範な機能を含む。インフラは短い寿命と転換性を基に運営され、特定国家の公共 OS 環境(BOSS など)に特化したカスタム設計が確認される。SectorH グループは Linux 特化攻撃技術、スクリプトベースローダー、WebSocket
C2、政府用 OS ターゲティングを基に長期的なスパイ活動を遂行する。
SectorJ グループは、電子商取引・銀行・リテール・クラウド・IoT・エッジデバイスなど幅広い産業を対象に金銭的利益とインフラ構築を同時に追求する犯罪型脅威群である。攻撃はトロイの木馬化されたインストーラ、悪性 WordPress プラグイン、GitHub ベースの悪性プロジェクト、スミッシング・フィッシングメッセージ、USB ベースの VBS ワームなど多様な形態で開始される。彼らは、決済情報スキミング、アカウント・セッションの奪取、クラウド環境への侵入、Microsoft 365 アカウントの掌握、大規模スミッシングインフラの運用、ランサムウェアの配布、違法賭博・地下金融用ブラウザの配布、IoT ベースのプロキシネットワーク構築など多様な目的に合わせて攻撃を展開する。技術的には DLL サイドローディング、署名されたドライバーの悪用(BYOVD)、XMRig ベースのマイニング、AsyncRAT・PowerShell ローダー、サービスハイジャッキング、難読化・暗号化ベースの隠蔽、Outlook ベースの拡散、多数の短い有効期間を持つドメイン運用など高度化された手法を使用する。SectorJ グループの核心的特徴は金銭目的特化、ウェブスキミング・ランサムウェア・クリプトマイニング・クラウド侵害・大規模フィッシング・IoT プロキシ化など大規模犯罪生態系運営能力であり、これは長期的で組織的なサイバー犯罪運営モデルを形成する。

詳細情報

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

1) SectorA01 used BeaverTail Malware disguised as AI Job Offer (2025-10-21)

https://cti.nshc.net/events/view/19580

Sophisticated なサイバー脅威事件は BeaverTail というキャンペーンを含み、これは LinkedIn メッセージを通じて開発者をターゲットにし、DLMind という偽の会社の採用担当者 Tim Morenc を装い

ました。攻撃は有望なリモート AI エンジニアリング職を提案し、被害者に見た目には合法的なプロジェクトを含む GitHub リポジトリを複製するよう誘導しました。実行時、コードはバックドア実行で始まる多段階攻撃を引き起こしました。この複雑な攻撃チェーンは、資格情報の窃取、暗号通貨のマイニング、持続的なアクセス維持を目的として設計された様々な Malware コンポーネントの順次配布を含んでいました。初期段階では、プロジェクト内に含まれた C2 URL が API キー、ブラウザログイン、クリップボードデータ、システムフィンガープリントを窃取できるペイロードを配信しました。後の段階では、検出を避けるために深く難読化された JavaScript と Python スクリプトを使用し、様々な回避技術を活用し、WebSocket ビーコンを通じてリモート制御を獲得しました。脅威行為者は追加の搾取を可能にするためにリモートアクセス型トロイの木馬(RAT)をインストールし、AnyDesk を使用して持続的な GUI リモートアクセスを実行しました。

[Attack Flow]

1. [Reconnaissance] Gather Victim Information (T1592)
a. LinkedIn プロフィール分析
   b. 知人ネットワーク悪用
2. [Resource Development] Develop Capabilities (T1587.001)
   a. 偽の GitHub リポジトリ構成
   b. Malware 挿入
3. [Initial Access] Phishing: Spearphishing via Service (T1566.003)
   a. LinkedIn メッセージを通じた求職提案の伝達
   b. GitHub リポジトリ クローン(Clone) 誘導
4. [Execution] Command and Scripting Interpreter: JavaScript (T1059.007)
   a. Node.js スクリプト実行
   b. バックドアの活性化
5. [Persistence] Implant Internal Image (T1525)
   a. WebSocket ビーコン配布
6. [Privilege Escalation] Abuse Elevation Control Mechanism (T1548)
   a. UAC 回避手法
   b. 予約タスクの作成
7. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. 多重難読化適用
   b. カスタム Base91 エンコーディング使用
8. [Credential Access] Steal Application Access Token (T1528)
   a. API キー スキャン
   b. ブラウザ資格情報の窃取
9. [Discovery] System Information Discovery (T1082)

a. システムフィンガープリンティング
b. VM 検知
10. [Collection] Input Capture (T1056.001)
a. キーロガー設定
b. クリップボードモニタリング
11. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
a. WebSocket 基盤 C2 通信
b. HTTP POST を通じたデータ送信
12. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. 資格証明およびウォレットデータのアップロード
b. スキャナー結果アップロード

2) SectorA01 used Malware disguised as job description files (2025-10-23)

https://cti.nshc.net/events/view/19622

攻撃対象産業群: 国防

最近のサイバー脅威キャンペーンは主に無人航空機(UAV)分野で活動する複数のヨーロッパ防衛企業を対象としており、これは北朝鮮のドローンプログラム開発と関連がある可能性を示唆する。脅威行為者は過去のキャンペーンと一般的に関連付けられる精巧な社会工学戦術を使用し、標的ネットワークに侵入するためにトロイの木馬化された求人提案を含めた。初期のアプローチは、ユーザーが Malware PDF リーダーを実行するよう要求する餌求人説明書を通じて行われた。実行されると、リモートアクセス型トロイの木馬(RAT)である ScoringMathTea バックドアが配布され、攻撃者に損傷したシステムへの完全な制御権限を与えた。このキャンペーンはトロイの木馬化されたオープンソースプロジェクトを使用し、DLL プロキシを活用して回避能力を向上させた。攻撃の目的は UAV 技術に関連する独占情報および製造ノウハウの奪取であり、これは北朝鮮の戦略的利益と一致すると評価される。攻撃者はコマンドおよびコントロールのために損傷したサーバーを使用し、暗号化された通信と base64 エンコーディングを使用してデータ奪取活動を隠蔽した。この作戦は技術発展のためのサイバースパイ活動の継続的な傾向を反映している。

[Attack Flow]

1. [Resource Development] Develop Capabilities (T1587.001)
a. Malware 開発
b. オープンソースプロジェクト Malware 挿入
2. [Resource Development] Compromise Infrastructure (T1584.004)
a. 侵害されたサーバーを C&C として活用
b. インフラ構築

3. [Initial Access] Spearphishing via Service (T1566.003)
   a. 求職提案を利用した社会工学
   b. マルウェア PDF リーダーの実行誘導
4. [Execution] Native API (T1106)
   a. 動的 API ローディング
   b. DLL サイドローディング
5. [Persistence] Hijack Execution Flow (T1574.002)
   a. DLL プロキシ技術
   b. 正常プログラムサイドローディング
6. [Defense Evasion] Obfuscated Files or Information (T1027.009)
   a. 含まれるペイロードを隠す
   b. ディスク内暗号化されたペイロード保存
7. [Defense Evasion] Reflective Code Loading (T1620)
   a. リフレクティブ DLL インジェクション
   b. プロセスインジェクション
8. [Discovery] System Information Discovery (T1082)
   a. システム情報収集
   b. プロセス一覧の照会
9. [Command and Control] Application Layer Protocol (T1071.001)
   a. HTTP/HTTPS 基盤通信
   b. 暗号化された C&C トラフィック 使用
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. データ流出
    b. Base64 エンコーディングを通じたデータ偽装

3) SectorA01 used DLL Sideloading in DreamJob Campaigns (2025-10-24)

https://cti.nshc.net/events/view/19629

2025 年 8 月、巧妙なマルウェア配布戦略に関連するサイバー脅威が確認された。脅威行為者は、正規のツールやシステムバイナリに偽装したマルウェアを配布し、管理者を標的としたキャンペーンを展開していた。特に、多様なペイロードを展開可能な複数のローダー、いわゆる「dream loaders」が使用されていた。主な要素として、DLL サイドローディングを利用して悪性サービスとして実行されるローダーである TSVIPSrv.dll や、認証情報および機密情報を抽出するための誘導として設計されたトロイの木馬化ツール tnsviewer.exe が含まれる。攻撃者は wkspbroker.exe のような正規実行ファイルをサイドローディングに悪用し、暗号化されたペイロードとコード再利用によって活動を秘匿していた。TSVIPSrv.dll や HideFirstLetter.dll といった解析済みアーティファクトは、高いコ

ード類似性を示し、複数システムに跨る協調的な活動の一環であることを示唆している。これらの手法は高度な回避技術を特徴としており、継続的な脅威に対処するための事前分析の重要性を強調している。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
   a. トロイの木馬化された TightVNC クライアント
   b. パスワードで保護された ZIP ファイル
2. [Execution] User Execution (T1204.002)
   a. 管理者が tnsviewer.exe を実行
   b. マルウェアサービスを通じて TSVIPSrv.dll が実行される
3. [Persistence] Create or Modify System Process (T1543.003)
   a. マルウェアサービス(sessionenv)作成
   b. 正常実行ファイルを使用した DLL サイドローディング
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. DLL 内の暗号化されたペイロード
   b. Base64 および RC4 復号化 適用
5. [Credential Access] Credential Dumping (T1003)
   a. 管理者アカウント資格情報抽出
   b. バイナリに含まれたアクセス トークン
6. [Discovery] System Information Discovery (T1082)
   a. TightVNC が生成したレジストリキー確認
   b. メモリダンプ分析
7. [Command and Control] Application Layer Protocol (T1071)
   a. Microsoft Graph API リクエスト
   b. SharePoint サーバー URL の照会
8. [Collection] Data from Information Repositories (T1213)
   a. SharePoint データアクセス
   b. 機微情報の収集
9. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 攻撃者制御ドメインにデータ送信
   b. 正常な Microsoft URL を活用した通信

4) SectorA01 used New BLINDINGCAN Variant in Phishing Emails (2025-11-03)

https://cti.nshc.net/events/view/19847

Comebacker Malware の新しい変種が発見された。この変種は高級持続脅威と関連しており、最初の侵入はフィッシングを活用したものと推定される。Comebacker Malware は DLL と EXE の二つのバージョンで確認され、ペイロード復号化、レジストリ操作、サービス配布を含む同じ機能を示す。攻撃は複数の段階を経て進行し、動的 API 関数確認及びパラメータ検証を通じて Malware を実行する。Malware は文字列復号化のために HC256 と RC4 を使用し、タイムスタンプは合法的なファイルを模倣するように操作される。第二段階では"Compcat_v1.dll"というサービスバイナリを配布し、主にメモリで最終ペイロードをロードして実行するのに使用される。最終ペイロードは BLINDINGCAN リモートアクセスツールの変種で、ファイル実行、データ流出、システム偵察を含む広範な機能と向上した暗号化機能を特徴とする。コマンド及びコントロール(C2)サーバーとの通信は高級暗号化を通じて難読化され、悪性作業の持続性と隠蔽性を保証する。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
   a. VPN 請求書に偽装した ZIP ファイル
   b. フィッシングメールの配信
2. [Execution] User Execution (T1204)
   a. .scr ファイル実行
   b. PDF 誘い込み画面表示
3. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. XOR および SIMD 難読化
   b. カスタムハッシング技法使用
4. [Persistence] Create or Modify System Process (T1543)
   a. "AhnlabUpdate" 予約タスク作成
   b. 任意の名前のサービス登録
5. [Privilege Escalation] Abuse Elevation Control Mechanism (T1548)
   a. 権限が昇格された状態でコマンドを実行
   b. COM サーバー登録
6. [Credential Access] OS Credential Dumping (T1003)
   a. メモリベースの認証情報ロード
   b. 含まれるペイロード復号化
7. [Discovery] System Information Discovery (T1082)
   a. システム言語および OS バージョン収集
   b. ネットワークアダプタおよび CPU アーキテクチャ列挙
8. [Lateral Movement] Remote Services (T1021)
   a. リバースシェル接続
   b. CreateProcessAsUserW を通じたコマンド実行

9. [Collection] Screen Capture (T1113)
   a. スクリーンショットキャプチャ
   b. COM インターフェース基盤映像キャプチャー
10. [Command and Control] Application Layer Protocol (T1071)
   a. HTTP POST ベースの C2 通信
   b. AES-128-CBC 暗号化を通じたデータ転送
11. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. ファイルアップロードおよびダウンロード
   b. 圧縮を通じたファイル流出
12. [Impact] Data Destruction (T1485)
   a. 安全なファイル削除
   b. 自己終了および痕跡除去

5) SectorA01 used DOCX Malware disguised as Aerospace Documents (2025-11-07)

https://cti.nshc.net/events/view/20101

攻撃対象産業群: 航空宇宙、防衛

Comebacker
として知られるマルウェアの新たに確認された亜種が、航空宇宙など特定分野を標的として発見された。このマルウェアは docx
ファイルに偽装された形で 2019 年 6 月に確認され、バックドア戦略の一環として DLL
ファイルをダウンロードし、システムを侵害するために利用されていた。2021 年に初めて報告されて以降、PyPI
パッケージ挿入などの手法を活用する、より洗練されたバージョンへと進化している。感染は、追加ペイロードを復号して実行する悪性 VBA マクロを含む docx
ファイルから開始される。重要な工程として、カスタム暗号化方式と ChaCha20
アルゴリズムを用いて埋め込まれたコードを復号する処理が挙げられ、C&C サーバーとの通信は HTTPS および AES-128-CBC
によって暗号化される。マルウェア配布にはスピアフィッシング手法が用いられ、航空宇宙関連文書を模倣した誘導文書を通じて当該産業の機微情報取得を目的としているとみられる。攻撃インフラは hiremployee[.]com や birancearea[.]com
を含む複数のドメインで構成されており、継続的な脅威活動を示している。

[Attack Flow]

1. [Initial Access] Phishing: Spear Phishing Attachment (T1566.001)
   a. Malware docx ファイル

b. 航空宇宙 産業 テーマ 餌 文書

2. [Execution] User Execution: Malicious File (T1204.002)
   a. VBA マクロ実行
   b. ペイロードの復号化および実行
3. [Persistence] Boot or Logon Autostart Execution: Shortcut Modification (T1547.009)
   a. LNK ファイル生成
   b. スタートアップフォルダーを基盤とした永続性の確保
4. [Defense Evasion] Obfuscated Files or Information: Encrypted/Encoded File (T1027.013)
   a. ChaCha20 暗号化
   b. カスタム XOR およびビットスワップ復号化
5. [Defense Evasion] System Binary Proxy Execution: Rundll32 (T1218.011)
   a. Rundll32 実行
   b. DLL ローディング
6. [Command and Control] Encrypted Channel: Symmetric Cryptography (T1573.001)
   a. HTTPS 基盤通信
   b. AES-128-CBC 暗号化
7. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. C&C サーバー接続
   b. hiremployee[.]com とのデータ交換
8. [Collection] Data from Local System (T1005)
   a. 情報収集
   b. 航空宇宙産業関連情報収集

6) SectorA01 used JSON Services for Malware in Job Interview Scam (2025-11-13)

https://cti.nshc.net/events/view/20163

最近の Contagious Interview キャンペーンの発展において、サイバー脅威行為者たちはソフトウェア開発者、特に暗号通貨および Web3 プロジェクトに関与する開発者を対象に、トロイの木馬化されたコードプロジェクトを通じて Malware をホスティングするために JSON ストレージサービスを活用する。脅威行為者たちはしばしば LinkedIn のようなプラットフォームで偽のリクルーターアカウントを開始し、偽の面接を通じて対象を誘引し、Malware が含まれたデモプロジェクトを使用する。これらのプロジェクトは API キーに偽装した base64 でエンコードされた変数をホスティングし、これは実際には難読化されたコードが含まれた JSON ストレージサービスの URL である。コードが実行されると、システム情報、ブラウザデータおよび敏感なファイルを窃取するように設計された BeaverTail という情報窃取バリアントが明らかになる。その次の段階では、Pastebin URL から Tsunami コンポーネントを含む追加のペイロードを取得する InvisibleFerret RAT が含まれる。こ

の多段階攻撃チェーンは持続性を維持し、システムの管理者権限を獲得し、さまざまなオペレーティングシステムでデータ窃取および Malware 配布を通じて財政的利益を追求するように設計されている。

[Attack Flow]

1. [Reconnaissance] Gather Victim Information (T1592)
   a. 偽のリクルーター プロフィール生成
   b. ソフトウェア開発者対象識別
2. [Initial Access] Spearphishing via Service (T1566.003)
   a. LinkedIn を通じた社会工学技法
   b. トロイの木馬化されたコードプロジェクトの配信
3. [Execution] User Execution (T1204)
   a. Node.JS 基盤インタビュー課題実行
   b. 難読化された JavaScript 実行
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Base64 でエンコードされた変数使用
   b. 高度難読化された JavaScript コード
5. [Credential Access] Steal Application Access Token (T1528)
   a. ブラウザプロファイル検索
   b. ウォレットデータの窃取
6. [Collection] Data from Local System (T1005)
   a. 機微ファイルの流出
   b. システム情報収集
7. [Command and Control] Web Service (T1102)
   a. JSON ストレージサービスを利用した通信
   b. Pastebin で追加ペイロードをダウンロード
8. [Persistence] Create or Modify System Process (T1543)
   a. 予約タスクの作成
   b. Windows Defender 例外追加
9. [Privilege Escalation] Abuse Elevation Control Mechanism (T1548)
   a. UAC プロンプト使用
   b. Python サイレント(Silent) インストール
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. TOR 基盤データ流出
    b. C2 サーバーと通信

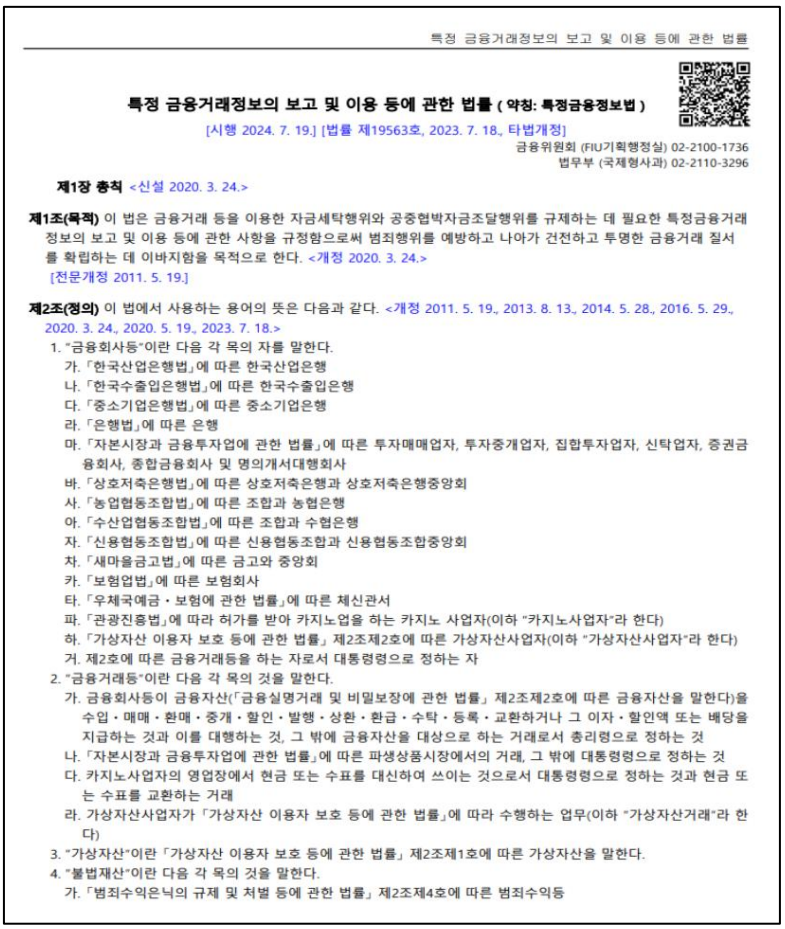
7) SectorA02 distributed Malware disguised as transaction-submission document (2025-11-14)

https://cti.nshc.net/events/view/20239

HWP 文書に偽装された LNK ファイルを含む ZIP アーカイブが、ROKRAT と関連する内蔵ペイロードの実行を開始した。LNK は PowerShell コマンドを実行し、長さが 0 の LNK ファイルを検索した後、固定されたバイナリオフセットからペイロードを抽出し、XOR ルーチンを通じてこれをデコードした上で、生成されたファイルを実行した。スクリプトはその後、元の LNK ファイルを削除し、公用ディレクトリへ移動した後、igamingroundtable[.]com から 2 つのリモートコンポーネントを取得した。最後に、ダウンロードされたペイロードの継続的な動作を可能にし、システム永続性を確立するため、繰り返し実行で構成されたスケジュールタスクを生成した。

[Attack Flow]

1. [Initial Access] Spearphishing Link (T1566.002)
   a. LNK ファイルが含まれた ZIP アーカイブ
   b. HWP ドキュメントに偽装
2. [Execution] User Execution (T1204.002)
   a. LNK ファイル 実行
   b. PowerShell コマンド実行
3. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. XOR ルーチン復号化
   b. 元の LNK ファイル削除
4. [Persistence] Scheduled Task/Job (T1053.005)
   a. 予約タスクの作成
   b. 繰り返し実行構成
5. [Command and Control] Application Layer Protocol (T1071)
   a. リモート構成要素ダウンロード
   b. igamingroundtable[.]com と C2 通信



특정 금융거래정보의 보고 및 이용 등에 관한 법률

특정 금융거래정보의 보고 및 이용 등에 관한 법률 (약칭: 특정금융정보법)

[시행 2024. 7. 19.] [법률 제19563호, 2023. 7. 18., 타법개정]

금융위원회 (FIU기획행정실) 02-2100-1736
법무부 (국제형사과) 02-2110-3296

제1장 총칙 <신설 2020. 3. 24.>

제1조(목적) 이 법은 금융거래 등을 이용한 자금세탁행위와 공중협박자금조달행위를 규제하는 데 필요한 특정금융거래정보의 보고 및 이용 등에 관한 사항을 규정함으로써 범죄행위를 예방하고 나아가 건전하고 투명한 금융거래 질서를 확립하는 데 이바지함을 목적으로 한다. <개정 2020. 3. 24.>
[전문개정 2011. 5. 19.]

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2011. 5. 19., 2013. 8. 13., 2014. 5. 28., 2016. 5. 29., 2020. 3. 24., 2020. 5. 19., 2023. 7. 18.>

1. "금융회사등"이란 다음 각 목의 자를 말한다.
   가. 「한국산업은행법」에 따른 한국산업은행
   나. 「한국수출입은행법」에 따른 한국수출입은행
   다. 「중소기업은행법」에 따른 중소기업은행
   라. 「은행법」에 따른 은행
   마. 「자본시장과 금융투자업에 관한 법률」에 따른 투자매매업자, 투자중개업자, 집합투자업자, 신탁업자, 증권금융회사, 종합금융회사 및 명의개서대행회사
   바. 「상호저축은행법」에 따른 상호저축은행과 상호저축은행중앙회
   사. 「농업협동조합법」에 따른 조합과 농협은행
   아. 「수산업협동조합법」에 따른 조합과 수협은행
   자. 「신용협동조합법」에 따른 신용협동조합과 신용협동조합중앙회
   차. 「새마을금고법」에 따른 금고와 중앙회
   카. 「보험업법」에 따른 보험회사
   타. 「우체국예금·보험에 관한 법률」에 따른 체신관서
   파. 「관광진흥법」에 따라 허가를 받아 카지노업을 하는 카지노 사업자(이하 "카지노사업자"라 한다)
   하. 「가상자산 이용자 보호 등에 관한 법률」 제2조제2호에 따른 가상자산사업자(이하 "가상자산사업자"라 한다)
   거. 제2호에 따른 금융거래등을 하는 자로서 대통령령으로 정하는 자
2. "금융거래등"이란 다음 각 목의 것을 말한다.
   가. 금융회사등이 금융자산(「금융실명거래 및 비밀보장에 관한 법률」 제2조제2호에 따른 금융자산을 말한다)을 수입·매매·환매·중개·할인·발행·상환·환급·수탁·등록·교환하거나 그 이자·할인액 또는 배당을 지급하는 것과 이를 대행하는 것, 그 밖에 금융자산을 대상으로 하는 거래로서 총리령으로 정하는 것
   나. 「자본시장과 금융투자업에 관한 법률」에 따른 파생상품시장에서의 거래, 그 밖에 대통령령으로 정하는 것
   다. 카지노사업자의 영업장에서 현금 또는 수표를 대신하여 쓰이는 것으로서 대통령령으로 정하는 것과 현금 또는 수표를 교환하는 거래
   라. 가상자산사업자가 「가상자산 이용자 보호 등에 관한 법률」에 따라 수행하는 업무(이하 "가상자산거래"라 한다)
3. "가상자산"이란 「가상자산 이용자 보호 등에 관한 법률」 제2조제1호에 따른 가상자산을 말한다.
4. "불법재산"이란 다음 각 목의 것을 말한다.
   가. 「범죄수익은닉의 규제 및 처벌 등에 관한 법률」 제2조제4호에 따른 범죄수익등

[図 3: SectorA02 グループが活用した文書]

8) SectorA03 used LNK Malware disguised as resume to target HR (2025-10-27)

https://cti.nshc.net/events/view/19671

2025 年 6 月から 8 月にかけて、先進的なマルウェアアップデートを配布するサイバー脅威キャンペーンが、求職申請書に偽装したスピアフィッシングメールを用いて組織を標的にした。攻撃者は Malware LNK ファイルが含まれた VHDX 添付ファイルを直接メールで送信した。受信者がこれを開くと、Git を通じて合法的なファイルがスクリプトを実行し、追加の Malware をダウンロードした。この持続性メカニズムは、ダウンロードされたスクリプトを使用した COM ハイジャックを活用してペイロードを取得するために GitHub に接続した。キャンペーンは二つの Downloader バージョンを使用してコンピュータおよびボリュームシリアル番号を通じて Statcounter と通信し、デバイスを識別し、時間の経過とともに方法を適応させた。Downloader2 は SpyGlace Malware とそのローダーのダウンロードおよび実行を容易にし、ADD および XOR でエンコードされた動的 API 解決を活用した。これは最新バージョンで洗練された技術である。SpyGlace 3.1.12 から 3.1.14 までは C2 サーバーとの通信がカスタム RC4 難読化を通じて向上し、コマンド機能の更新およびさまざまな持続性パスなどの顕著な運用の変化を示した。攻撃者はペイロード保存のために GitHub を頻繁に

使用し、削除されない限り過去のペイロードへの持続的なアクセスを悪用してコミットログを通じたバリアント追跡を可能にした。この作戦は主に東アジアの標的に影響を与えた。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
   a. Malware VHDX 添付ファイル
   b. LNK ファイル実行
2. [Execution] User Execution (T1204.002)
   a. LNK ファイルクリック
   b. Git を通じたスクリプト実行
3. [Persistence] Hijack Execution Flow (T1574)
   a. COM ハイジャック
   b. レジストリ修正
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. ADD および XOR エンコーディング
   b. カスタム RC4 難読化
5. [Discovery] System Information Discovery (T1082)
   a. ボリュームシリアル番号収集
   b. コンピュータ名収集
6. [Command and Control] Application Layer Protocol (T1071)
   a. Statcounter 通信
   b. GitHub ペイロード ダウンロード
7. [Collection] Screen Capture (T1113)
   a. スクリーンショットモジュール(Clouds.db)
   b. Export 関数(mssc1)
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. BASE64 および RC4 ベースの通信
   b. AES128-CBC 復号化

9) SectorA03 used GitHub for Payload Delivery (2025-10-31)

https://cti.nshc.net/events/view/19797

攻撃対象産業群: 政府・行政、コンサルティング、文化

2014 年から始まったと推定される高度化されたサイバー脅威作戦が、韓国政府および事業部門と関連する機関を対象にモニタリングおよび情報脱取を目標としている。攻撃者は一時的な Malware ペイロードホスティングのために GitHub を活用し、ダウンロード後に迅速なコード削除を通じて探知

を回避し、動的ロード分散技術を統合した点が含まれる。また、暗号キーを頻繁に交換し、コード難読化を適用して Malware の探知および分析に対する回避能力を強化した。データおよび関数ポインタ技術を導入して静的分析を困難にした。Bitbucket から GitHub へのバックドアホスティングの移動は、攻撃インフラの戦略的統合を示している。これらの措置は攻撃戦術を強化し、セキュリティ分析に迅速に適応できる能力を強調する。

[Attack Flow]

1. [Reconnaissance] Gather Victim Information (T1592)
   a. 韓国政府および企業部門対象識別
   b. 韓国文化および労働コンサルティング関連機関の把握
2. [Resource Development] Develop Capabilities (T1587)
   a. ペイロード配布用 GitHub アカウント生成
   b. 暗号化・難読化機能を備えたマルウェア開発
3. [Initial Access] Spearphishing Attachment (T1566.001)
   a. メールを介したマルウェアペイロードの配信
   b. ユーザーの相互作用を通じた初期侵害誘導
4. [Execution] User Execution (T1204)
   a. ユーザー実行時にペイロード動作
   b. バックドアのダウンロードおよび実行トリガー
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. コード難読化および暗号化適用
   b. データおよび関数ポインタ技法の使用
6. [Defense Evasion] Indicator Removal on Host (T1070)
   a. GitHub でダウンロード痕跡削除
   b. git push --force でコミット履歴を削除
7. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. 継続的アクセスのためのバックドア設置
   b. Backdoor Install 構成要素 活用
8. [Command and Control] Application Layer Protocol (T1071)
   a. GitHub を通じた C2 通信の活用
   b. 動的ロード分配方式で命令伝達
9. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 侵害された機関での敏感情報の窃取
   b. 取得したデータを C2 チャネルへ送信

10) SectorA03 used LNK Malware disguised as researcher resumes (2025-11-06)

https://cti.nshc.net/events/view/19900

2025 年 6 月から 8 月にかけて、日本の採用スタッフを対象とした一連のサイバー攻撃が観察された。この攻撃は、求職申請書に偽装したスピアフィッシングメールを使用していた。攻撃者はメールに悪性な VHDX ファイルを直接添付していた。ファイルを開くと、LNK ファイルが合法的な Git コマンドを使用してスクリプトを実行し、餌文書を表示し、追加のペイロードを活性化した。このキャンペーンには Downloader1 が含まれており、これはボリュームシリアル番号を使用して感染したデバイスを識別し、合法的なサービスである Statcounter と通信した。その後、この Malware は GitHub に接続して Downloader2 のような追加コンポーネントをダウンロードした。SpyGlace Malware はバージョン 3.1.12 から 3.1.14 に進化し、コマンドセット、エンコーディング、通信プロトコルに変化を見せ、安全な通信のために修正された RC4 を含んでいた。GitHub はペイロードを保存および管理するために使用され、バージョン履歴が追跡された。3 つのバージョンが識別され、それぞれが固有の Mutex 値とエンコーディング方式を持っていた。履歴書形式の餌文書は採用担当者をターゲットにしており、攻撃に社会工学的戦術をさらに統合していた。

[Attack Flow]

1. [Reconnaissance] Phishing for Information (T1598)
   a. スピアフィッシングメール送信
   b. 入社志願書で偽装したメッセージ使用
2. [Resource Development] Acquire Infrastructure (T1583)
   a. GitHub インフラ活用
   b. Statcounter サービス活用
3. [Initial Access] Spear Phishing Attachment (T1566.001)
   a. Malware VHDX ファイル使用
   b. 改ざんされた履歴書の餌の活用
4. [Execution] User Execution (T1204)
   a. LNK ファイル実行誘導
   b. Git コマンドを通じたスクリプト実行
5. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. LNK ファイルを基盤とした永続性の確保
   b. Downloader1 自動実行
6. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. 修正された RC4 エンコーディング手法の活用
   b. 固有の Mutex 値生成
7. [Discovery] System Information Discovery (T1082)
   a. ボリュームシリアル番号識別

8. [Command and Control] Application Layer Protocol (T1071)
    a. Statcounter との通信の実行
    b. ペイロード管理のための GitHub 活用
9. [Collection] Data from Local System (T1005)
    a. SpyGlace を通じたデータ収集
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. セキュア通信チャネルの使用
    b. GitHub でバージョン管理を実行

11) SectorA04 used WhatsApp job-themed lure for BURNBOOK loader (2025-11-20)

https://cti.nshc.net/events/view/20367

攻撃対象産業群: 製造、IT

2025 年 8 月、ヨーロッパ製造組織のアジア子会社を対象とした事件が WhatsApp Web を通じて開始された社会工学攻撃を使用して発生する。この攻撃はプロジェクトエンジニアに送信された求職関連の誘引を含み、悪性 ZIP アーカイブのダウンロードにつながる。アーカイブには合法的なドキュメントビューアである SumatraPDF.exe と悪性 DLL である libmupdf.dll が含まれており、PDF を開くとバックドアを実行する。攻撃は BURNBOOK ローダーと MISTPEN バックドア変種を使用し、コマンド＆コントロール(C2)インフラとして損傷した WordPress リソースを活用する。攻撃者は LDAP クエリを活用してドメインユーザーおよびコンピュータリストを抽出する手動活動を行う。'パス・ザ・ハッシュ(Pass-the-Hash)'技法を使用してネットワーク内でアクセスし、レターラルムーブメント(Lateral Movement)を実行する。TSVIPsrv.dll、MISTPEN 変種が SharePoint サーバーを通じて追加の C2 接続を設定するために配布される。このキャンペーンは DLL サイドローディングのような高度な戦術を使用し、初期アクセスのためにインスタントメッセージングプラットフォームの脆弱性を悪用する。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
    a. WhatsApp Web メッセージ使用
    b. 求職関連のミキを活用
2. [Execution] User Execution: Malicious File (T1204.002)
    a. ZIP 圧縮ファイルダウンロード誘導
    b. PDF ファイル閲覧誘導
3. [Execution] DLL Side-Loading (T1574.002)
    a. SumatraPDF.exe 実行

b. libmupdf.dll サイドローディング

4. [Persistence] Boot or Logon Autostart Execution: DLL Search Order Hijacking (T1547.001)
   a. BURNBOOK ローダー 実行
   b. MISTPEN バックドア配布
5. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. 侵害された WordPress サイトの活用
   b. SharePoint 基盤 C2 通信
6. [Discovery] Account Discovery: Domain Account (T1087.002)
   a. LDAP クエリの実行
   b. ユーザーおよびコンピューターリストの抽出
7. [Credential Access] OS Credential Dumping: Pass-the-Hash (T1550.002)
   a. バックアップアカウントの奪取
   b. 管理者アカウントの奪取
8. [Lateral Movement] Lateral Tool Transfer (T1570)
   a. TSVIPsrv.dll 配布
   b. ネットワーク接続試行
9. [Collection] Data from Local System (T1005)
   a. Release_PvPlugin_x64.dll 実行
   b. 情報脱取モジュール実行
10. [Defense Evasion] Masquerading: Match Legitimate Name or Location (T1036.005)
    a. 正規実行ファイルへの偽装
    b. 非標準ディレクトリでの DLL ローディング

12) SectorA05 used Malware disguised as MMC to Execute Remote Payload (2025-10-27)

https://cti.nshc.net/events/view/19673

Sophisticated Malware 事件は Microsoft Management Console(MMC)の悪用を含む悪意のある活動を実行するために使用された。この Malware は"internview.msc"という標準 MMC ファイルに偽装し、システムを対象にコンソールモードの視覚を変更し、被害者を合法的なコンテンツに見せかけたブロックされた Google Drive 文書にリダイレクトした。実行時に、WScript.Shell、Scripting.FileSystemObject、msxml2.xmlhttp を活用してファイル操作および HTTP リクエストを実行した。具体的には、スクリプトはリモートサーバーからペイロードを取得し、%APPDATA%ディレクトリに.gif ファイルとして保存した。このファイルが存在する場合、.bat スクリプトに変換されバックグラウンドで実行され、"OneDriveUpdate"というタスクを予約して 41 分ごとに

VBScript を実行することで持続性を保証した。このスクリプトは mshta を使用してリモート HTML アプリケーション(HTA)を実行し、追加のペイロード配信を容易にした。この攻撃は韓国人を潜在的な対象とし、リモートペイロードの実行と複雑なスケジューリングメカニズムを活用したデータ窃取を目的としていた。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 悪性 .msc(MMC) ファイル配信
2. [Execution] User Execution: Malicious File (T1204.002)
   a. ユーザーが .msc ファイルを手動で実行
   b. 悪性スクリプトが含まれたコンソールロジック動作
3. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.003)
   a. cmd.exe コマンド実行
   b. mshta 呼び出しを通じた HTA 実行準備
4. [Defense Evasion] Masquerading (T1036)
   a. 正常な MMC ファイルに偽装
   b. ペイロード保存のための .gif 拡張子悪用
5. [Persistence] Scheduled Task/Job: Scheduled Task (T1053.005)

a. OneDriveUpdate 予約タスク作成
   b. temp.vbs を 41 分間隔で自動実行するように設定
6. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. リモートサーバーに HTTP リクエストを送信
   b. リモートペイロードダウンロードの実行
7. [Execution] Command and Scripting Interpreter: VBScript (T1059.005)
   a. VBScript 実行
   b. バックグラウンドスクリプト実行
8. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. エンコードされたコマンドの使用
   b. ペイロードを .gif ファイルとして隠す
9. [Execution] User Execution: Malicious File (T1204.002)
   a. mshta を通じたリモート HTA 実行
   b. 追加ペイロードローディング

13) SectorA05 abused MMC to execute VBS-based malware (2025-10-31)

https://cti.nshc.net/events/view/19783

最近の分析によると、Microsoft Management Console (MMC) フレームワークを悪用する精巧な Malware 攻撃が強調されている。この Malware は.msc ファイルを通じて配信され、VBS スクリプトを統合して攻撃を実行する。これはユーザーを Google Docs を開くように誘導し、正常な作業であるかのように偽装する。攻撃はリモートサーバーから悪性ペイロードを取得するダウンローダーを通じて開始され、これを%APPDATA%¥Microsoft ディレクトリに「sus.gif」として保存し、実行のために「sus.bat」に名前を変更する。「temp.vbs」という 2 番目の VBS スクリプトが生成され、Windows タスクスケジューラ項目「OneDriveUpdate」を通じて 41 分ごとに実行される。さらに、Malware は mshta を使用して HTML アプリケーション（「ttt.hta」）を実行し、リモートスクリプトの実行をさらに容易にする。この攻撃ベクターは msxml2.xmlhttp を通じた HTTP リクエストを活用してデータ転送を行い、過去の戦術を思い起こさせる社会工学と持続性メカニズムの混合を示しているが、最近のキャンペーンで継続的に観察されている。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 悪意のある .msc ファイルの配信
2. [Execution] User Execution: Malicious File (T1204.002)
   a. ユーザーが .msc ファイルを実行
   b. 初期 VBS ベース ロジック 実行
3. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.003)
   a. cmd.exe コマンド実行
   b. VBS スクリプト生成および実行
4. [Execution] Command and Scripting Interpreter: VBScript (T1059.005)
   a. temp.vbs スクリプト生成
   b. VBS 実行のための予約タスク設定
5. [Execution] Signed Binary Proxy Execution: Mshta (T1218.005)
   a. mshta で ttt.hta 実行
   b. リモートスクリプトのローディング
6. [Persistence] Scheduled Task/Job: Scheduled Task (T1053.005)
   a. OneDriveUpdate 予約タスクの作成
   b. 41 分間隔で繰り返し実行
7. [Defense Evasion] Masquerading (T1036)
   a. sus.gif に偽装して保存
   b. 実行目的で sus.bat に名称変更
8. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. msxml2.xmlhttp を利用した HTTP リクエスト
   b. リモートサーバーにデータおよびリクエストを送信

9. [Collection] Data from Local System (T1005)
   a. orientedworld.com でリモートペイロードをダウンロード
   b. %APPDATA% パスに一時保存

14) SectorA05 used VPN Invoice Lure with HttpTroy Backdoor Attack (2025-11-03)
https://cti.nshc.net/events/view/19865

HttpTroy という新種のバックドアを含む多段階標的侵入攻撃が発見された。このキャンペーンは VPN 請求書に偽装した ZIP アーカイブを含むフィッシングメールで始まる。このアーカイブは韓国の特定の高価値個人を対象としており、Windows SCR ファイルを活用して小さな Go バイナリを実行し、餌の PDF を表示し、追加の悪性コンポーネントをドロップする。このコンポーネントはローダーである MemLoad と暗号化された HttpTroy DLL バックドアである。MemLoad はローカルセキュリティベンダーを模倣した予約タスクを設定して持続性を確保し、HttpTroy バックドアを解読および実行する。HttpTroy はファイル転送、スクリーンショットキャプチャ、コマンド実行、コマンド＆コントロールサーバーとの難読化された HTTP 通信などリモート制御機能を可能にする。特に、この攻撃は検出を避けるために API ハッシュ技法、文字列難読化、メモリ内実行などの高度な技術を活用する。このキャンペーンの地域化、戦術、方法論は以前に類似した脅威作戦に帰属されたパターンと一致する。

[Attack Flow]
1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. ZIP 圧縮ファイルベースの餌使用
   b. VPN 請求書 偽装 ドキュメント 活用
2. [Execution] User Execution: Malicious File (T1204.002)
   a. Malware SCR ファイル実行
   b. Go バイナリ実行
3. [Execution] Command and Scripting Interpreter (T1059)
   a. コマンド実行
   b. リバースシェル機能サポート
4. [Persistence] Scheduled Task/Job: Scheduled Task (T1053.005)
   a. AhnlabUpdate タスク作成
   b. regsvr32 を通じた DLL 登録
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. String 文字列難読化
   b. API ハッシュ技法使用
6. [Defense Evasion] Masquerading (T1036)

a. 供給業者名と類似したタスク名の使用
b. 誘い込み PDF ファイル表示
7. [Defense Evasion] In-Memory Execution (T1620)
a. メモリ上での DLL ローディング
b. ディスクベースのアーティファクト回避
8. [Collection] Screen Capture (T1113)
a. 画面キャプチャ実行
b. 資格証明書収集
9. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
a. HTTP POST 方式 通信
b. 難読化された C2 ペイロード使用
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. ファイルアップロードおよびダウンロード
b. データ脱取

15) SectorA05 used JavaScript Malware disguised as Windows Themes (2025-11-05)

https://cti.nshc.net/events/view/19929

攻撃対象産業群: 政府・行政、シンクタンク

最近のサイバー脅威事件は、政府機関、シンクタンク、主題専門家を対象とした諜報作戦を含む。攻撃は Themes.js という名前の JavaScript ファイルで始まり、これは攻撃者が制御する URL へネットワークリクエストを開始し、追加ペイロードをダウンロードする。この初期 JavaScript は難読化されておらず、指定された URI からコンテンツを実行する機能を持つ。このリクエストで使用された主要なパラメータは、侵害されたデバイスのコンピュータ名である。第二段階では、システムおよびファイル情報を収集し、コマンド＆コントロールサーバーにアップロードする体系的な偵察を行う追加の JavaScript コードが含まれる。ここには、システム詳細、実行中のプロセス、ディレクトリコンテンツのリストが含まれ、各結果は POST リクエストを通じて送信される。第三段階では、「Windows Themes Manager」という予約タスクを通じて毎分 JavaScript ファイルを実行し、持続性を生成する。追加として、空の Word 文書は潜在的な餌として使用される。様々な技術的要素には、エンコード目的のためのレジストリ項目の修正、データのキャビネットファイルへのエンコード、certutil LOLBIN を使用したエンコード/デコードシーケンスが含まれる。これらの段階は、検出を避け、長期的なアクセスを維持するためのものである。Themes.js ファイルの正確な初期配信方法は知られていない。

[Attack Flow]

1. [Execution] Command and Scripting Interpreter: JavaScript (T1059.007)

a. ダウンロードされた JavaScript 実行

b. 追加ペイロード実行

2. [Persistence] Scheduled Task/Job: Scheduled Task (T1053.003)
   a. "Windows Themes Manager" タスク作成
   b. Themes.js を 1 分間隔で実行
3. [Defense Evasion] Modify Registry (T1112)
   a. HKCU¥Console¥CodePage 値の変更
   b. UTF-8 エンコードに設定
4. [Defense Evasion] Indicator Removal: File Deletion (T1070.004)
   a. 一時ファイルの削除
   b. 痕跡除去
5. [Discovery] System Information Discovery (T1082)
   a. システム情報収集
   b. 実行中のプロセス一覧
6. [Discovery] File and Directory Discovery (T1083)
   a. C:¥Users 内ファイル一覧の閲覧
   b. ディレクトリ属性収集
7. [Collection] Data from Local System (T1005)
   a. 流出のためのデータ準備
   b. データを Cabinet ファイルにエンコード
8. [Command and Control] Ingress Tool Transfer (T1105)
   a. Themes.js ダウンロード
9. [Exfiltration] Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)
   a. C2 サーバーに POST リクエストを送信
   b. システムおよびプロセスデータの流出

16) SectorA05 used RAT Malware disguised as 'StressClear' MSI targeting HRDs (2025-11-05)

https://cti.nshc.net/events/view/19904

攻撃対象産業群: 市民

9 月にサイバー脅威行為者が "EndClient RAT" というリモートアクセス型トロイの木馬 (RAT) を配布し、北朝鮮の人権擁護者を標的にしました。攻撃はある人権活動家の Google アカウントが侵害されることで始まり、これを通じて行為者は被害者のモバイルデバイスをリモートで初期化することができました。悪性 RAT は "StressClear.msi" という名前の AutoIT ベースの Microsoft インストールパッケージを通じて配布され、39 人に影響が及んだと識別されています。この Malware は中国の

ある採掘会社から奪取した署名キーを通じて配布されたと見られ、大韓民国の銀行ソフトウェアと共にバンドルされることで合法的に見せかけ、セキュリティ検出を回避しました。攻撃ベクターはカカオトークを通じた社会工学を利用し、被害者が悪性パッケージをインストールするよう誘導しました。RAT は Windows 予約タスクを通じて持続性を確保し、TCP ソケットを使用してコマンド＆コントロールサーバーと通信し、攻撃者がコマンドを実行しファイルを転送できるようにします。主要な技術要素には、低いアンチウイルス検出のための AutoIT 使用と、C2 プロトコル処理のためのメモリ内モジュール使用が含まれます。この洗練された攻撃は、人権コミュニティに対する脅威行為者の継続的な脅威を強調しています。

[Attack Flow]

1. [Initial Access] Spearphishing via Service (T1566.003)
   a. Google アカウントの窃取
   b. KakaoTalk を基盤としたソーシャルエンジニアリング手法の使用
2. [Execution] User Execution (T1204)
   a. "StressClear.msi" インストール
   b. AutoIT スクリプト実行
3. [Persistence] Scheduled Task/Job (T1053)
   a. "IoKlTr" 予約タスク作成
   b. スタートアップディレクトリに LNK ファイルを生成
4. [Defense Evasion] Code Signing (T1553.002)
   a. 盗まれた署名キーの使用
   b. 正常なソフトウェアとのバンドリング
5. [Credential Access] OS Credential Dumping (T1003)
   a. 名前付きパイプを介したリモートシェルの取得
   b. cmd.exe を利用したコマンド実行
6. [Discovery] System Information Discovery (T1082)
   a. システム情報収集(コンピュータ名, OS, ユーザーなど)
   b. 収集された情報を C2 に送信
7. [Command and Control] Application Layer Protocol (T1071)

a. C2 サーバーへの TCP 接続
   b. JSON ベースの C2 通信
8. [Collection] Data from Local System (T1005)
   a. ファイルダウンロード命令実行
   b. ファイルアップロードコマンド実行
9. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. データを C2 に送信

b. Base64 エンコーディング 使用

17) SectorA05 used JScript Malware disguised as Wedding Photos (2025-11-06)

https://cti.nshc.net/events/view/19938

攻撃対象産業群: 市民

サイバー攻撃が偽の結婚写真を通じて個別ユーザーを損傷させようとしているように見えます。攻撃は難読化された JavaScript ファイルを使用して複数の感染段階を誘導しました。初期には Base64 でエンコードされた文字列が JPG ファイルとしてデコードされ、実行時にユーザーには写真として見えましたが、Malware を含んでいました。Malware は certutil.exe と regsvr32.exe を通じた LotL(Living-off-the-Land)技法を使用して追加ペイロードをデコードおよび実行し、従来のアンチウイルス検出を回避しました。最終ペイロードには DLL またはスクリプトレット(scriptlet)が含まれており、regsvr32.exe を使用して静かに実行されました。ファイルは%ALLUSERSPROFILE%¥ディレクトリに戦略的に配置されました。この事件は結婚写真会社からユーザーデータが流出した可能性を示唆しており、メールで送信された悪意のあるファイルが編集された結婚写真として偽装されていました。さらに、Sony カメラモデルの EXIF データが操作され、写真が 2024 年 11 月 17 日に撮影されたように見えると推定されています。

[Attack Flow]

1. [Execution] User Execution: Malicious File (T1204.002)
   a. Obfuscated JavaScript 実行
   b. Base64 デコードを通じた JPG 変換
2. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Base64 エンコーディング
   b. EXIF データの改ざん
3. [Defense Evasion] Living off the Land (T1218)
   a. Certutil.exe 使用
   b. Regsvr32.exe 実行
4. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. DLL 実行
   b. スクリプトレット実行
5. [Defense Evasion] Masquerading (T1036)
   a. %ALLUSERSPROFILE% パスにファイル配置
   b. 正規のように見せるためのファイル名変更
6. [Collection] Data from Local System (T1005)
   a. ユーザーデータ流出

b. ファイルアクセスおよび流出

[図 4: SectorA05 グループが活用した偽の結婚写真]

18) SectorA05 used JSE Malware Disguised as Health Checkup Document (2025-11-06)

https://cti.nshc.net/events/view/19952

2025 年 10 月末、高度持続的脅威が健康チェック通知文書に偽装した悪性 JSE ファイルと関連付けられました。これは北朝鮮グループと連携していると疑われる攻撃者によって使用されました。攻撃は PDF 文書に偽装した JSE ファイルを含む圧縮ファイルで始まり、ユーザーを騙してこれを実行させました。実行時、難読化された JavaScript コードが WScript.exe を通じて実行され、ユーザーが気付かないように正常に見える PDF が表示されました。同時に、rundll32.exe を使用してバックグラウンドで悪性 PE データがロードされました。このプロセスは特定の条件が満たされると追加の悪性行動を準備するために毎分コマンド＆コントロール(C2)サーバーとの通信を試みました。通信プロセスは複数のチャネルを含み、収集されたシステム情報は AES-128 および Base64 でエンコードされて C2 サーバーに送信されました。最終段階では追加のペイロードを要求し、これを RC4 で復号化した後、定義された'hello'関数を実行しましたが、分析当時 C2 サーバーの非活性により正確な行動は不明でした。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)

a. JSE ファイルが含まれた圧縮ファイル

b. PDF ドキュメントに偽装

2. [Execution] Command and Scripting Interpreter: JavaScript (T1059.007)

a. WScript.exe 実行

b. Obfuscated JavaScript コード

3. [Defense Evasion] Obfuscated Files or Information (T1027)

a. Obfuscated JavaScript 使用

b. Base64 デコードを通じて実行される certutil.exe

4. [Persistence] DLL Side-Loading (T1574.002)

a. Rundll32.exe ローディング

b. Malware PE データ使用

5. [Command and Control] Application Layer Protocol (T1071.001)

a. C2 サーバーと通信

b. 多重チャネルプロトコル使用

6. [Collection] Data from Local System (T1005)

a. システム情報収集

b. AES-128 + Base64 エンコーディング

7. [Exfiltration] Exfiltration Over C2 Channel (T1041)

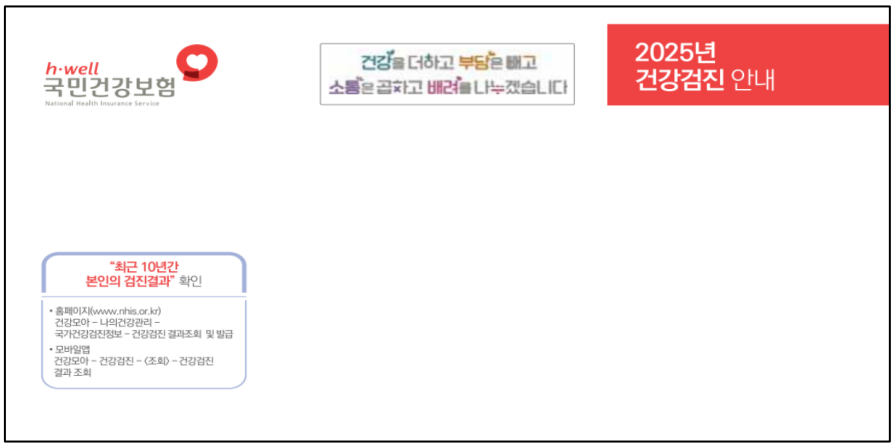
a. 暗号化されたデータアップロード

b. C2 サーバーとの相互作用

8. [Execution] Command and Scripting Interpreter (T1059.001)

a. RC4 復号化

b. 'Hello' 関数 実行



[図 5: SectorA05 グループが活用した PDF 文書]

19) SectorA05 used Phishing Email Disguised as Government Notice (2025-11-06)

https://cti.nshc.net/events/view/19933

Phishing キャンペーンが政府部門を装い、新しい電子文書の到着を主張するメールで個人を対象に攻撃を行いました。メールは公式の出所から来たように見えましたが、実際には Phishing 試みでした。メッセージは受信者に個人情報を含む文書を見るために身元を確認するよう要求し、アクセスのための期限を提供しました。主要な技術的詳細には、発信者のメールインフラがあります。Phishing メールは moise-service(.)dynv6(.)net を使用して Zoho ZeptoMail API を通じて送信され、ARC や DKIM のような認証検査を通過しました。このキャンペーンは特定の URL 形式のリンクを通じてユーザーを Phishing サイトにリダイレクトしました。ユーザーがリンクをクリックしてパスワードを入力すると、これらの資格情報が攻撃者に送信されました。Phishing ページはよく知られたサービスを模倣して合法的に見えるようにし、メール発信者アドレスは公式メール形式に類似するように操作されました。この事件は、発信者アドレスの不一致や異常な文書要求といった微妙な Phishing の兆候を認識することの重要性を強調しています。

[Attack Flow]

1. [Reconnaissance] Phishing for Information (T1598)
   a. 政府機関を詐称
   b. 公式文書の形式に見えるようにメールを作成
2. [Resource Development] Acquire Infrastructure (T1583)
   a. Zoho ZeptoMail API 使用
   b. moise-service(.)dynv6(.)net 設定
3. [Initial Access] Spearphishing Link (T1566.002)
   a. フィッシングメール送信
   b. フィッシングサイトリンク含む
4. [Credential Access] Input Capture (T1056)
   a. フィッシングサイトへのリダイレクト
   b. 入力されたパスワード収集
5. [Command and Control] Web Service (T1102)
   a. 脱取した資格情報を攻撃者に転送
   b. AS 20473 インフラ活用

20) SectorA05 used Golang Malware disguised as Hepatitis A Vaccination Advisory (2025-11-07)

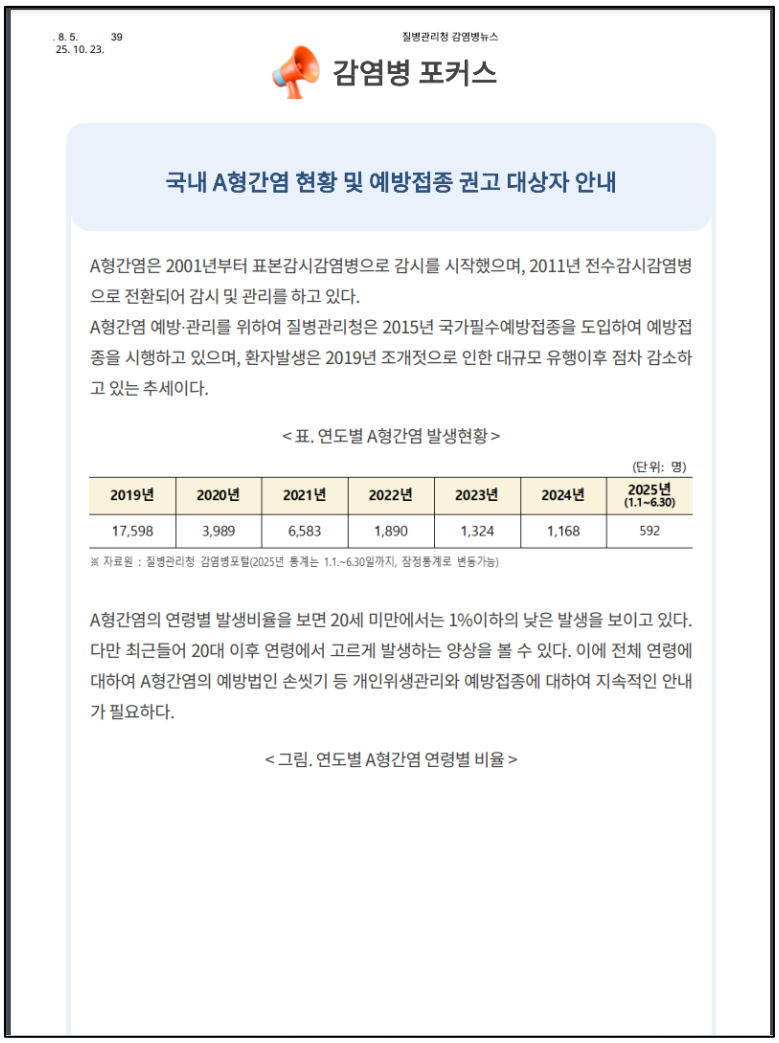
https://cti.nshc.net/events/view/19942

攻撃者は大韓民国光州の市民を対象に「Domestic Hepatitis A Status and Vaccination Guide.pdf.scr.exe」というタイトルの PDF ファイルに偽装した Malware を利用した攻撃を実行しました。Malware が実行されると、ログファイルを生成し、元の実行ファイルを削除します。持続性を確保するために、Windows レジストリに「HancomAgent」として登録し、システム起動時に実行されるようにします。その後、Malware はループに入り、継続的にコマンド＆コントロール(C2)サーバーに接続してペイロードをダウンロードし、これを実行するために復号化および解凍を行います。この Malware は、WinHTTP ライブラリを使用してリモートサーバーに接続するために操作された URL を使用し、ウェブブラウザを偽装するために User-Agent 文字列を使用して隠蔽性を維持します。主な目的は、感染したシステムで持続的な潜伏状態を維持し、データの窃取または不正アクセスを試みることのようです。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
   a. PDF ファイルに偽装
   b. 実行ファイル偽装技法使用
2. [Execution] User Execution (T1204.002)
   a. .scr ファイル実行
   b. 元の実行ファイル削除
3. [Persistence] Registry Run Keys / Startup Folder (T1547.001)
   a. Windows レジストリに登録
   b. HancomAgent のスタートアップ項目を生成
4. [Defense Evasion] Masquerading (T1036.005)
   a. ウェブブラウザへの偽装
   b. User-Agent 文字列操作
5. [Command and Control] Application Layer Protocol (T1071.001)
   a. C2 サーバーへの接続
   b. WinHTTP ライブラリ使用
6. [Command and Control] Web Service (T1102.001)
   a. 改ざんされた URL への接続
   b. 持続的な C2 接続維持
7. [Exfiltration] Exfiltration Over C2 Channel (T1041)

a. データ脱取
   b. 不正なアクセスの維持



. 8. 5. 39
25. 10. 23.

질병관리청 감염병뉴스

감염병 포커스

국내 A형간염 현황 및 예방접종 권고 대상자 안내

A형간염은 2001년부터 표본감시감염병으로 감시를 시작했으며, 2011년 전수감시감염병으로 전환되어 감시 및 관리를 하고 있다.
A형간염 예방·관리를 위하여 질병관리청은 2015년 국가필수예방접종을 도입하여 예방접종을 시행하고 있으며, 환자발생은 2019년 조개젓으로 인한 대규모 유행이후 점차 감소하고 있는 추세이다.

<표. 연도별 A형간염 발생현황>

(단위: 명)

2019년	2020년	2021년	2022년	2023년	2024년	2025년 (1.1~6.30)
17,598	3,989	6,583	1,890	1,324	1,168	592

※ 자료원 : 질병관리청 감염병포털(2025년 통계는 1.1.~6.30일까지, 잠정통계로 변동가능)

A형간염의 연령별 발생비율을 보면 20세 미만에서는 1%이하의 낮은 발생을 보이고 있다. 다만 최근들어 20대 이후 연령에서 고르게 발생하는 양상을 볼 수 있다. 이에 전체 연령에 대하여 A형간염의 예방법인 손씻기 등 개인위생관리와 예방접종에 대하여 지속적인 안내가 필요하다.

<그림. 연도별 A형간염 연령별 비율>

[図 6: SectorA05 グループが活用した文書]

21) SectorA05 used Phishing Domains Disguised as Naver (2025-11-09)

https://cti.nshc.net/events/view/20114

主要企業を対象としたサイバー脅威活動に関する総合分析では、脅威主体が 2021 年と 2022 年にかけてよく知られた企業の正体を偽装し、広範囲なタイポスクワッティングフィッシングドメインを使用したことが明らかになった。2022 年末、彼らは NFT および暗号通貨保有者を対象とする暗号通貨テーマのドメインを設立し、活動を拡張した。合計 1,983 個のユニークホスト名と 19 個のメールアドレスがこれらのキャンペーンと関連付けられており、これは運用の精巧なインフラを明らかにする。この手法は複数のメールエイリアスを通じたドメイン登録を含み、「Tony Smith」のような名前の繰り返しやメールアカウントの複数の繰り返しを通じて作戦の複雑性を示唆する命名規則のパターンを提案する。攻撃はまた、被害者が敏感なウォレット情報を共有するよう誘導し、金融資産を脅かす段階も含んでいた。発見されたドメインは過去および最近の IP 記録とクロスリファレンスされ、知られている敵対的主体と関連する可能性のある複雑なネットワークを明らかにした。特に、ドメインはより広範囲での調整を示唆し、暗号通貨関連インフラとかなりの重複を示した。いくつかのケ

ースでは、フィッシングサイトは運用中であり、疑わないユーザーからデジタル資産資格情報を密かに取得するよう設計されていた。インフラを明らかにするためには集中的なデータ抽出と WHOIS 分析が必要であり、これは進行中と推定されるキャンペーン内で新たに浮上するパターンと相互に関連する脅威ベクターを特定するのに不可欠であった。

[Attack Flow]

1. [Reconnaissance] Gather Victim Identity Information (T1589)
   a. タイポスクワッティングドメイン活用
   b. WHOIS データ分析
2. [Resource Development] Acquire Infrastructure (T1583)
   a. ドメイン登録
   b. IP アドレスの取得
3. [Initial Access] Spearphishing Link (T1566.002)
   a. メールキャンペーンの実施
   b. 暗号通貨関連のミキを活用
4. [Credential Access] Steal Application Access Token (T1528)

a. ウォレットシードフレーズ収集
   b. 暗号通貨ウォレットフィッシングサイト運営
5. [Command and Control] Ingress Tool Transfer (T1105)

a. 難読化された JavaScript 使用
   b. PHP ファイル配布
6. [Exfiltration] Exfiltration Over Alternative Protocol (T1048)
   a. 盗まれた資格情報の転送
   b. 暗号通貨アドレス活用

22) SectorA06 used Malware Disguised as Zoom Update on macOS (2025-10-28)

https://cti.nshc.net/events/view/19717

攻撃対象産業群: IT

サイバー脅威行為者が Web3/ブロックチェーン産業のブロックチェーン開発者と役員を対象に高級侵入戦略を活用することが確認された。彼らの作戦である GhostCall と GhostHire は、主に社会工学、フィッシング、そして AI を使用した向上した攻撃実行を通じて精巧な攻撃を調整する。
GhostCall は macOS デバイスを対象とし、偽のビデオ通話を使用して被害者にソフトウェアアップデートに偽装した悪性スクリプトをダウンロードさせる。感染チェーンは AppleScript とコマンドライン操作を含み、暗号通貨ウォレットや資格情報のような敏感な情報を収集する Malware を配布する。GhostHire は Telegram と GitHub を通じて採用プロセスに偽装し、Web3 開発者を対象とし、

彼らを騙して有害なプロジェクトを実行させる。このアプローチはプログラミングプロジェクト内に隠された Malware を使用して被害者のオペレーティングシステムに特定のペイロードをダウンロードするよう設計されている。両キャンペーンは異なるプログラミング言語を使用し、検出を避けるために複数のコンポーネントに機能を分散させるモジュール式攻撃チェーンを使用して 2023 年以降の行為者の戦略進化を示している。行為者の AI 使用は技術的実行を向上させただけでなく、社会工学戦術を精巧にし、目標との相互作用をさらにカスタマイズし説得力を持たせた。このようなキャンペーンは日本、オーストラリアおよびその他の地域で被害者を発生させ、主に APAC 地域の技術役員とベンチャーキャピタル機関に影響を与えた。この脅威行為者は多様なオペレーティングシステムの弱点を活用した歴史を持ち、検出を減らすためにツールと方法を調整しながら継続的に新しい Malware セットを開発し、個人および企業のサイバーセキュリティ環境全般にわたって脅威を強化している。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. 投資機会に偽装した Telegram メッセージの使用
   b. Calendly を通じた偽の Zoom ミーティングリンク提供
2. [Execution] User Execution: Malicious File (T1204.002)
   a. Zoom アップデート用に偽装した AppleScript のダウンロードおよび実行
   b. 採用プロセスでの悪性 GitHub プロジェクト実行
3. [Persistence] Boot or Logon Autostart Execution: Launch Agent (T1547.013)
   a. 自動実行のための plist ファイル生成
   b. 永続性確保のための Launch Daemons の活用
4. [Privilege Escalation] Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
   a. RPC ベースの UAC 回避
   b. 権限が昇格された状態で実行
5. [Defense Evasion] Masquerading (T1036)
   a. Zoom／Microsoft Teams に偽装したアプリケーションの使用
   b. 正規アプリケーション名を利用したマルウェア偽装
6. [Credential Access] OS Credential Dumping: LSASS Memory (T1003.001)
   a. 偽のダイアログボックスを利用した macOS パスワードの窃取
   b. ブラウザおよび Keychain 資格情報収集
7. [Discovery] System Information Discovery (T1082)
   a. OS およびハードウェア情報収集
   b. 実行中のプロセスおよびボリュームの列挙
8. [Collection] Input Capture: Keylogging (T1056.001)

a. 資格証明書収集のための keylogger 配布
b. ブラウザおよびアプリケーションデータ収集
9. [Command and Control] Application Layer Protocol: WebSocket (T1071.001)
a. WSS を利用した C2 通信
b. 収集したデータを C2 サーバーへ送信
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. HTTP POST 方式で脱取データをアップロード
b. curl を利用したデータ流出

23) SectorA07 used Android Malware disguised as stress-relief programs (2025-11-10)

https://cti.nshc.net/events/view/20039

サイバー脅威事件が識別されており、これは Android デバイスを対象とする悪性キャンペーンで、Google の Find Hub 機能を悪用します。この攻撃はより広範なキャンペーンと連携しており、脅威行為者たちは北朝鮮人権活動家と心理カウンセラーを装っています。彼らは大韓民国のカカオトークメッセンジャーを通じてストレス解消プログラムに偽装した Malware を配布し、知人との信頼関係を利用して社会工学的攻撃を行います。このキャンペーンの戦術には、Find Hub を通じたリモートデータ削除のために Google アカウントを悪用することが含まれており、これは新しい国家支援攻撃方法として評価されます。この脅威は他の認識されたサイバー脅威グループと関連する重複インフラに関連した持続的作戦の一環として識別されました。このキャンペーンは MSI パッケージと AutoIt スクリプトを含むファイルベースの持続性メカニズムを含む洗練された技術を示しています。これはリモートで破壊的な活動を実行するために合法的な管理機能を悪用する事例を強調し、損傷したメッセンジャーアカウントを追加で悪用して Malware を拡散させます。これは国家支援作戦で使用される脅威行為者の能力と戦術の重要な進化を示しています。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
a. 国税庁詐称
b. Malware メール添付ファイル実行
2. [Execution] User Execution (T1204)
a. MSI パッケージ実行
b. AutoIt スクリプト実行
3. [Persistence] Scheduled Task/Job (T1053.005)
a. AutoIt スクリプト用予約タスク生成
b. MSI パッケージ基盤の持続性維持

4. [Privilege Escalation] Abuse Elevation Control Mechanism (T1548)
   a. 権限が昇格された状態で MSI を実行
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. 暗号化された AutoIt スクリプト使用
   b. 正常なコード署名の悪用
6. [Credential Access] Credential Dumping (T1003)
   a. Google アカウント資格情報の窃取
   b. Naver アカウントアクセス
7. [Discovery] System Information Discovery (T1082)
   a. 内部偵察の実行
   b. システム状態モニタリング
8. [Collection] Input Capture (T1056)
   a. RAT ベースのキー ロギング
   b. ウェブカメラ監視
9. [Command and Control] Application Layer Protocol (T1071)
   a. WordPress を基盤とした C2 通信
   b. C2 サーバーとの持続的な接続維持
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. AutoIt スクリプトを通じたデータ流出
    b. RAT を利用した情報脱取
11. [Impact] Data Destruction (T1485)
    a. Find Hub を通じたリモートデータ削除
    b. 反復的なデバイス初期化コマンド

24) SectorB01 used ShadowPad Backdoor disguised as Common Software (2025-10-22)

https://cti.nshc.net/events/view/19559

攻撃対象産業群: 政府・行政, 通信, 軍事機関, 小売, 技術, 高等教育

複数の中国連携 APT グループ間の高度な協力戦術の新しい傾向が「PaaS(Premier Pass-as-a-Service)」モデルで確認された。この協力には二つの脅威行為者が含まれ、彼らは 2023 年末から 2025 年中頃まで APAC およびその他のグローバル地域の政府機関や通信プロバイダーといった重要な部門を対象に攻撃を行った。最初の行為者は二番目の行為者のためのアクセスブローカーとしての役割を果たし、侵害された資産をスムーズに引き渡すことで、検出および帰属の努力を複雑にする。主要な発見事項には、2025 年 1 月に脆弱なサーバーが侵害された後、CrowDoor や ShadowPad のような様々な Malware ツールキットが配布されたことが含まれる。この協力攻撃は共有アクセスイ

ンフラを使用し、複雑な侵入キャンペーンに参加して伝統的な帰属方法に挑戦する洗練された方法である。このような運用モデルの登場は、サイバースパイ戦術の変化を強調し、サイバーセキュリティ分析における向上した帰属戦略の必要性を浮き彫りにする。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. 脆弱なウェブサーバー侵害
   b. CrowDoor バックドア 配布
2. [Execution] Command and Scripting Interpreter (T1059)
   a. Draculoader シェルコード ローダー 配布
   b. CrowDoor ペイロード実行
3. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. DLL サイドローディング
   b. ShadowPad を通じた持続的アクセス維持
4. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
   a. CVE-2025-5777 悪用
   b. 権限昇格の取得
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. 異なる DLL ファイル名の使用
   b. 多重ベクターを通じた ShadowPad 配布
6. [Credential Access] OS Credential Dumping (T1003)
   a. LSASS メモリ ダンプ
   b. カスタムメモリダンピングツール使用
7. [Lateral Movement] Remote Services (T1021)
   a. SSH 接続確立
   b. Checkpoint メールサーバー使用
8. [Collection] Data from Local System (T1005)
   a. 機微データの収集
   b. 流出準備
9. [Command and Control] Application Layer Protocol (T1071)
   a. C&C インフラと通信
   b. CrowDoor および ShadowPad C&C サーバー使用
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. C&C を通じたデータ流出
    b. 共有アクセスインフラ活用

25) SectorB01 used DLL Side-Loading via vetysafe.exe for persistence (2025-11-06)

https://cti.nshc.net/events/view/19908

攻撃対象産業群: 通信

2025 年 4 月、サイバー脅威行為者が特定されていない機関を対象に、そのネットワークに隠密で持続的な存在感を確保しようとする攻撃を敢行する。この攻撃は中国と連携した基地で実行され、複数の精巧な技術が使用された。初期アクセスは 4 月 5 日の大量スキャンを通じて試みられ、Atlassian OGNL Injection、Log4j、Apache Struts のようなエクスプロイトが活用された。しばらく中断後、4 月 16 日に攻撃者は疑わしい curl コマンドを実行して接続性をテストし、その後 netstat を使用してネットワーク詳細情報を収集した。持続性は msbuild.exe を使用した予約タスクを通じて保証され、これは不明な XML ファイルを実行してコマンド＆コントロール通信に繋がった。カスタムローダーが不明なペイロードを復号化して実行し、これはリモートアクセスツールに関連しているように見える。攻撃者は vetysafe.exe を通じた DLL サイドローディングを実装して悪性 DLL を配布した。Active Directory 資格情報を抽出するための Dcsync 攻撃が試みられたようだ。これらの行動はドメインコントローラーを対象とした長期的な諜報キャンペーンを示し、より広範なネットワーク侵入を目指している。運用戦術は中国諜報グループの知られた活動と一致する。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. 脆弱性検出のための大規模スキャンの実施
   b. Atlassian OGNL Injection, Log4j, Apache Struts 脆弱性悪用
2. [Discovery] Network Service Scanning (T1046)
   a. 疑わしい curl コマンドの実行
   b. 内部システム接続の有無テスト
3. [Discovery] System Network Connections Discovery (T1049)
   a. netstat コマンド実行
   b. アクティブネットワーク接続の収集
4. [Persistence] Scheduled Task/Job (T1053)
   a. schtasks を利用した予約タスクの作成
   b. outbound.xml を使用して msbuild.exe を実行
5. [Execution] Command and Scripting Interpreter (T1059)
   a. msbuild.exe 実行
   b. csc.exe によるコードロードおよびインジェクション
6. [Command and Control] Application Layer Protocol (T1071)
   a. C&C サーバー接続
   b. ペイロード実行のためのカスタムローダー使用

7. [Persistence] DLL Side-Loading (T1574.002)
   a. vetysafe.exe を利用した DLL サイドローディング
   b. sbamres.dll 配布
8. [Credential Access] DCSync (T1003.006)
   a. Dcsync ツール使用
   b. Active Directory 資格情報 抽出

26) SectorB10 exploited Motex LANSCOPE zero-day with Gokcpdoor malware (2025-10-30)

https://cti.nshc.net/events/view/19775

2025 年中盤、精巧なサイバー攻撃が Motex LANSCOPE Endpoint Manager のゼロデイ脆弱性である CVE-2025-61932 を悪用して敏感なデータを抽出しました。この事件には国家支援を受けた脅威行為者が関与しており、彼らは最初にリモートコマンド実行を SYSTEM 権限で許可するこの脆弱性を利用してシステムを侵害しました。脆弱なデバイスの数は少なかったものの、侵害されたネットワーク内での悪用は権限昇格とレターラルムーブメント（Lateral Movement）を可能にしました。脅威行為者は Gokcpdoor Malware を使用し、これはマルチプレクシング通信を活用するコマンド＆コントロール（C2）サーバーを通じてバックドアを設定しました。Gokcpdoor の変種はそれぞれ異なる役割を果たし、サーバータイプは接続を待機し、クライアントタイプはハードコーディングされた C2 サーバーに接続しました。特定のホストでは Gokcpdoor の代わりに Havoc C2 フレームワークが使用され、OAED Loader Malware を使用して合法的な実行ファイルにペイロードを注入することで実行フローを操作しました。リモートデスクトップアプリケーションや io、LimeWire、Piping Server のようなクラウドサービスといった合法的なツールが横方向の移動とデータ窃取に悪用されました。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. CVE-2025-61932 脆弱性 悪用
   b. SYSTEM 権限でリモートコマンド実行
2. [Execution] Command and Scripting Interpreter (T1059)
   a. 任意コマンド実行
3. [Persistence] Implant Internal Proxy (T1090.002)
   a. Gokcpdoor サーバー タイプ 設定
   b. バックドア接続生成
4. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
   a. SYSTEM 権限 悪用

5. [Defense Evasion] Masquerading (T1036)
   a. OAED Loader を利用したペイロードインジェクション
6. [Credential Access] OS Credential Dumping (T1003)
   a. goddi ツール使用
7. [Discovery] System Network Connections Discovery (T1049)
   a. ネットワーク接続の列挙
8. [Lateral Movement] Remote Services (T1021)
   a. リモートデスクトップアプリケーション使用
9. [Command and Control] Application Layer Protocol (T1071)
   a. C2 とのマルチプレクシング通信
   b. Havoc C2 フレームワーク活用
10. [Exfiltration] Exfiltration Over Web Service (T1567)
    a. クラウドストレージサービスアクセス
    b. io, LimeWire, Piping Server を通じたデータ流出の試み

27) SectorB22 used LNK Files Exploiting Windows Vulnerability for Attacks (2025-10-30)

https://cti.nshc.net/events/view/19784

攻撃対象産業群: 外交、政府・行政

2025 年 9 月と 10 月にヨーロッパの外交機関を対象とした精巧なサイバー諜報キャンペーンが識別され、これは 2025 年 3 月に公開された Windows ショートカット脆弱性 ZDI-CAN-25373 を悪用したものである。ハンガリー、ベルギーおよびその他のヨーロッパ諸国の外交関係者に、欧州連合執行委員会と NATO イベントに関連するテーマの Malware LNK ファイルにリンクする URL を含むスピアフィッシングメールが送信された。これらのファイルは PowerShell コマンドを実行し、合法的に署名されたキャノンプリンターユーティリティを使用した DLL サイドローディングを通じて PlugX リモートアクセス型トロイの木馬（RAT）に至る多段階 Malware チェーンを配布した。このキャンペーンは、隠密な情報収集のための精巧な技術を展開し、迅速な脆弱性採用を示し、進化した社会工学戦略を実証する。PlugX Malware の亜種配布は難読化および分析防止技術を強調し、広範なリモート制御機能を提供して情報収集を容易にする。この作戦はまた、ポータルハイジャックおよび直接スピアフィッシングを含む複数の攻撃チェーンを通じて迅速に切り替える能力を示した。

[Attack Flow]

1. [Reconnaissance] Gather Victim Information (T1592)
   a. 外交会議関連テーマの識別
   b. ヨーロッパ外交日程収集

2. [Resource Development] Develop Capabilities (T1587.001)
   a. CanonStager ローダー 機能 改善
   b. PlugX Malware 変種 開発
3. [Initial Access] Spearphishing Attachment (T1566.001)
   a. URL が含まれたスピアフィッシングメール
   b. イベントテーマのマルウェア LNK ファイル
4. [Execution] Command and Scripting Interpreter (T1059.001)
   a. PowerShell コマンド実行
   b. TAR アーカイブ抽出
5. [Execution] User Execution (T1204.002)
   a. LNK ファイル実行
   b. 誘餌用 PDF 文書 表示
6. [Defense Evasion] Hijack Execution Flow (T1574.002)
   a. Canon ユーティリティを通じた DLL サイドローディング
   b. Malware DLL 実行
7. [Defense Evasion] Obfuscated Files or Information (T1027.009)
   a. 暗号化された PlugX ペイロード
   b. RC4 復号化
8. [Persistence] Boot or Logon Autostart Execution (T1547.001)
   a. レジストリ Run キー修正
   b. CanonPrinter 基盤持続性メカニズム
9. [Discovery] System Information Discovery (T1082)
   a. プロセス列挙
   b. レジストリクエリ
10. [Command and Control] Application Layer Protocol (T1071.001)
    a. 443 ポート 基盤 HTTPS 通信
    b. C2 ドメイン接続
11. [Collection] Input Capture (T1056)
    a. キーロギング
    b. ファイルアップロード/ダウンロード作業
12. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. C2 を通じたデータ流出
    b. C2 との暗号化された通信

28) SectorB22 used Pubload Malware in East Asia Manufacturing Attack (2025-10-30)

https://cti.nshc.net/events/view/19786
攻撃対象産業群: 政府・行政、製造

2025 年 3 月初、東アジアの製造環境で疑わしい DLL ファイルが分析され、中国と連携した脅威行為者の精巧な諜報キャンペーンとのつながりが明らかになる。この敵対勢力は、世界中の公共および民間部門の組織を対象とした持続的で精巧なキャンペーンでよく知られている。今回の事件では Pubload Malware が使用され、これは脅威グループが検出を避けるために定期的にアップデートするコンポーネントである。攻撃者は複数の同時作戦を管理できる能力を持っており、かなりのリソースと専門性を示している。Malware は主に脆弱性の悪用を通じて不正アクセスを設定し、情報を収集する方法で配信される。この作戦は、製造業者が彼らの部門を特定的に悪用する持続的なサイバー脅威に対して警戒を維持することが重要であることを強調している。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. 脆弱性の悪用
   b. 不正アクセスの実行
2. [Execution] Shared Modules (T1129)
a. DLL ファイル分析
   b. Pubload Malware 実行
3. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. 定期的なアップデートの実施
   b. 探知回避技法適用
4. [Command and Control] Application Layer Protocol (T1071)
   a. スパイ活動キャンペーン運営
   b. 多重作戦管理
5. [Collection] Data from Information Repositories (T1213)
   a. 製造業産業群対象情報収集

29) SectorB22 used Espionage Campaign via Fake Microsoft Domains (2025-11-10)
https://cti.nshc.net/events/view/19946

Sophisticated cyber threats are being carried out by actors engaged in espionage activities globally. これらは、複数の国家にまたがるシグニチャーサイバー作戦を通じて識別された。 これらのキャンペーンは、well-known brands や services を模倣することといった合法的なサービスに混じるように設計された多数のドメインの登録および活用を含む。 過去 90 日間にアクティブ化されたこれらのドメインには、famous tech conglomerates や他の信頼できる機関を模倣する名前が含ま

れている。 また、特定の IP アドレスがこれらの活動と関連付けられており、これらの作戦を調整および実行するために使用されるインフラを示している。 脅威行為者はこれらのデジタル資産を活用してスパイ活動を行い、国家間のセンシティブな情報を標的にして政府および企業部門に影響を与える可能性がある。 このキャンペーンは、特定の技法を通じて重要なデータを窃取する可能性を示しており、これらの侵入を検出するためのネットワークモニタリングの警戒が必要であることを強調している。

[Attack Flow]

1. [Reconnaissance] Gather Victim Network Information (T1590)
   a. ドメイン登録
   b. IP アドレスの取得
2. [Resource Development] Acquire Infrastructure (T1583)
   a. ドメイン設定
   b. サーバーホスティング
3. [Initial Access] Spearphishing Link (T1566.002)
   a. 悪性ドメイン活用
   b. フィッシングメール配布
4. [Execution] User Execution (T1204)
   a. 悪性リンククリック
   b. ペイロード実行
5. [Command and Control] Application Layer Protocol (T1071)
   a. HTTP/HTTPS 基盤 C2 通信
   b. データ漏洩
6. [Collection] Data from Information Repositories (T1213)
   a. 機微情報を対象
   b. 情報抽出
7. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. C2 へのデータ送信
   b. 暗号化されたチャネルの使用

30) SectorB109 used Network Implant to Hijack Software Updates (2025-11-19)

https://cti.nshc.net/events/view/20351

攻撃対象産業群: 製造、 自動車

サイバー脅威キャンペーンが中国、台湾、香港、カンボジア、韓国、アメリカ、ニュージーランドを含む複数の地域を対象として識別された。脅威行為者たちは"EdgeStepper"というネットワークイン

プラントを使用して中間者攻撃を実行している。このツールは DNS クエリを悪性ノードにリダイレクトし、合法的なソフトウェアアップデートトラフィックを攻撃者が制御するインフラに再ルーティングすることで、悪性アップデートを配布する。初期の対象はルーターのようなネットワークデバイスで、脆弱性や弱い資格情報を通じて損傷され、EdgeStepper を配布できるようになる。このシステムは DNS クエリをリダイレクトしてソフトウェアアップデートをハイジャックすることを容易にし、特に Sogou Pinyin のような人気のあるソフトウェアで観察された。このキャンペーンは "LittleDaemon"と"DaemonicLogistics"のような追加ツールを使用し、これは Windows デバイスに"SlowStepper"というバックドアを配布するダウンローダーの役割を果たす。LittleDaemon はハイジャックノードと通信して SlowStepper がすでにアクティブかどうかを評価し、そうでなければ DaemonicLogistics をダウンロードしてバックドアを取得し配布する。攻撃ベクターにはソフトウェアアップデートメカニズムを悪用し、サプライチェーン攻撃を実行する可能性が含まれており、悪性ペイロードの配布および実行において精巧な技術を示している。

[Attack Flow]

1. [Resource Development] Acquire Infrastructure (T1583)
   a. ドメイン登録
   b. DNS ノードホスティング
2. [Initial Access] Exploit Public-Facing Application (T1190)
   a. ネットワークデバイス侵害
   b. EdgeStepper 配布
3. [Execution] Command and Scripting Interpreter (T1059)
   a. LittleDaemon 実行
   b. DaemonicLogistics 実行
4. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. SlowStepper 配布
   b. 持続性確保
5. [Defense Evasion] Masquerading (T1036)
   a. 正常なドメイン名使用
   b. ファイルタイプ偽装
6. [Discovery] System Network Configuration Discovery (T1016)
   a. 360tray.exe の存在確認
   b. MAC アドレス収集
7. [Command and Control] Application Layer Protocol (T1071)
   a. HTTP 基盤通信
   b. 暗号化されたチャネル使用
8. [Collection] Data from Local System (T1005)

a. システム情報収集
b. セキュリティソフトウェア情報収集
9. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. ハイジャックノードにデータ転送
b. HTTP リクエスト 使用

31) SectorB118 used Warlock ransomware exploiting SharePoint vuln (2025-10-22)
https://cti.nshc.net/events/view/19558

2025 年 6 月、Warlock ランサムウェアが登場し、2025 年 7 月 19 日に Microsoft SharePoint のゼロデイ脆弱性(CVE-2025-53770)を悪用します。このランサムウェアは中国に基づくと推定されるグループと関連しており、一般的にロシアと関連する他のランサムウェアと区別されます。攻撃は DLL サイドローディングと"ak47c2"というカスタムコマンド＆コントロールフレームワークを使用する戦術で組織されました。攻撃者は 7zip のような合法的なソフトウェアを使用してサイバー作戦を遂行し、以前のペイロード Anylock を Warlock にリブランディングして暗号化されたファイルに.x2anylock 拡張子を追加します。複数のサイバーセキュリティ企業の調査によると、Malware に署名するために盗まれたデジタル証明書を使用し、防御を回避するために脆弱なドライバーBYOVD 技術を活用したことが明らかになります。歴史的なつながりは、この行為者がスパイ活動、サービス拒否攻撃、ランサムウェア攻撃に関与していたことを示唆し、中国のサイバー犯罪およびスパイ活動との潜在的な関連性を持つ多才な脅威環境を示しています。

[Attack Flow]
1. [Initial Access] Exploit Public-Facing Application (T1190)
a. ToolShell ゼロデイ脆弱性悪用
b. Microsoft SharePoint 対象攻撃
2. [Execution] Command and Scripting Interpreter (T1059)
a. DLL サイドローディング 使用
b. ランサムウェアペイロード配布
3. [Persistence] Boot or Logon Autostart Execution (T1547)
a. 7zip を利用した 7z.dll サイドローディング
b. ローダーを活用した持続性確保
4. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
a. 脆弱なドライバー悪用
b. BYOVD 手法 使用
5. [Defense Evasion] Signed Binary Proxy Execution (T1218)
a. 盗まれたデジタル証明書の使用

b. ドライバー名を googleapiutil64.sys に変更
6. [Credential Access] OS Credential Dumping (T1003)
a. カスタム C&C フレームワーク 活用
b. 資格証明アクセスのためのバックドア配布
7. [Discovery] System Information Discovery (T1082)
a. システム情報収集
b. セキュリティソフトウェア識別
8. [Command and Control] Application Layer Protocol (T1071)
a. ak47c2 フレームワーク 使用
b. C&C 通信構築
9. [Impact] Data Encrypted for Impact (T1486)
a. .x2anylock 拡張子でファイルを暗号化
b. Warlock および LockBit ペイロード配布

32) SectorB118 used Velociraptor for C2 via WSUS vulnerability exploitation (2025-11-20)

https://cti.nshc.net/events/view/20373

2025 年 11 月、複数の脅威行為者が Windows Server Update Services (WSUS)の新たにパッチが適用された脆弱性 (CVE-2025-59287) を利用して無断アクセスを試みた。攻撃者はこのリモートコード実行脆弱性を悪用し、Velociraptor というデジタルフォレンジックおよび事故対応ツールをコマンド＆コントロール (C2) 作業に展開した。これらの活動は 2024 年 11 月に初めて観察され、2025 年の過去三ヶ月間でかなりの増加が確認された。攻撃者は s3[.]wasabisys[.]com ドメインから取得した悪性 MSI パッケージを使用して Velociraptor をインストールした。インストール後、Velociraptor はエンドポイント更新のために構成された Velociraptor サービスを通じて C2 と通信を開始した。攻撃者はさらに base64 でエンコードされた PowerShell コマンドを使用して偵察を行い、侵害されたネットワーク内のユーザー、サービス、および構成に関するデータを収集した。これらの悪用は、Cobalt Strike や他の侵入テストフレームワークのような二重用途のツールが悪意のある目的で展開される継続的な傾向を強調している。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
a. WSUS 脆弱性 悪用
b. CVE-2025-59287 悪用
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
a. Base64 でエンコードされた PowerShell コマンドの実行

b. 偵察スクリプト実行

3. [Persistence] Create or Modify System Process: Windows Service (T1543.003)
   a. Velociraptor サービスインストール
   b. 自動開始構成
4. [Privilege Escalation] Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
   a. MSI パッケージインストール
   b. サービス制御マネージャー(SCM) 操作
5. [Defense Evasion] Masquerading: Match Legitimate Name or Location (T1036.005)
   a. 正常なツールの悪用
   b. DFIR ツールである Velociraptor 偽装活用
6. [Credential Access] OS Credential Dumping (T1003)
   a. ユーザー情報収集
   b. サービスアカウント識別
7. [Discovery] System Information Discovery (T1082)
   a. ネットワーク構成の照会
   b. ドメインコンピュータ列挙
8. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. Velociraptor を基盤とした C2 通信
   b. エンドポイントアップデート構成

33) SectorB122 exploited ToolShell vulnerability in cyber campaign (2025-10-22)

https://cti.nshc.net/events/view/19585

攻撃対象産業群: 通信、学界 - 大学、政府・行政

2025 年 7 月、中国を拠点とする脅威行為者が新たに公開された ToolShell の脆弱性（CVE-2025-53770）を悪用し、中東の通信企業およびアフリカ諸国の政府機関 2 部門を侵害した。彼らはオンプレミスの SharePoint サーバーに影響を与える ToolShell の脆弱性を利用し、非認可のリモートコード実行を可能にしていた。侵害後、Zingdoor と ShadowPad のバックドアが DLL サイドローディング手法を用いて展開された。追加の攻撃は南米の政府機関と米国の大学を標的とし、SQL や Adobe ColdFusion を実行する Apache
HTTP サーバーの脆弱性を悪用して KrustyLoader などのマルウェアを配布し、正規ソフトウェアを模倣したファイル名を使用して検知を回避した。Certutil、Revsocks、PetitPotam エクスプロイトといったツールの使用は、ネットワーク永続性および認証情報窃取を目的とした高度な戦術を示している。このキャンペーンは、地域全体の重要ネットワークへの持続的かつ秘匿的なアクセスを目指す戦略的なスパイ活動を示している。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. ToolShell 脆弱性 悪用
   b. SQL および Apache 脆弱性 悪用
2. [Execution] Command and Scripting Interpreter (T1059)
   a. SharePoint でのリモートコード実行
   b. KrustyLoader マルウェア配布
3. [Persistence] Event Triggered Execution (T1546)
   a. Zingdoor 用 DLL サイドローディング
   b. ShadowPad 用 DLL サイドローディング
4. [Defense Evasion] Masquerading (T1036)
   a. 正常なソフトウェアのように見えるファイル名の使用
   b. Certutil 使用による難読化
5. [Credential Access] Unsecured Credentials (T1552)
   a. PetitPotam を通じた資格情報の窃取
   b. Revsocks を通じた資格情報アクセス
6. [Collection] Automated Collection (T1119)
   a. 重要ネットワーク対象スパイ活動
   b. 戦略的データ流出
7. [Command and Control] Application Layer Protocol (T1071)
   a. Revsocks を基盤としたネットワーク永続性の維持
   b. 秘密の通信チャネル使用

34) SectorC05 used Localolive Webshell and Living-off-the-Land Tactics (2025-10-29)

https://cti.nshc.net/events/view/19734

攻撃対象産業群: 政府・行政

最近のサイバー脅威事件で、ロシアと関連があると推定される攻撃者たちがウクライナの組織を標的にしました。二ヶ月にわたり、大型ビジネスサービス組織と地域政府機関が侵害され、これは攻撃者たちが敏感な情報を抽出し、持続的なネットワーク存在を確保しようとする意図を明らかにしました。攻撃は 2025 年 6 月末に始まり、Localolive のようなウェブシェルをインストールするために外部に露出したサーバーの脆弱性を悪用しました。これはロシア起源の以前のキャンペーンと関連があると見られます。攻撃者たちは検出を避け、高い権限でネットワークを探索するために Living-off-the-Land 戦術と PowerShell スクリプトのような二重使用ツールを広範囲に活用しました。悪意の

ある活動には、セキュリティスキャンを回避するための構成変更、偵察コマンドの実行、資格情報を収集する可能性を考慮したメモリダンプの頻繁な実行が含まれていました。攻撃パターンは複数のコンピュータで続き、Microsoft Windows Resource Leak Diagnostic ツールのような非伝統的な方法を密かに使用し、合法的な実行ファイルに偽装されたウェブシェルを配布しました。伝統的な Malware の使用は最小限に抑えられましたが、攻撃者たちは Windows システムに対する高度な理解に基づき、低い可視性を維持しつつも高価値データを収集しました。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. Localolive web shell 配布
   b. パッチされていない脆弱性の悪用
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. PowerShell を基盤としたバックドア実行
   b. エンコードされた PowerShell コマンドの実行
3. [Persistence] Scheduled Task/Job (T1053.005)
   a. メモリダンプ実行のための予約タスク作成
   b. PowerShell バックドア 実行 予約
4. [Privilege Escalation] Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
   a. Windows Defender 設定再構成
   b. 管理者権限なしで Windows 機能インストール
5. [Defense Evasion] Masquerading (T1036)
   a. 正常のように見える実行ファイル名使用
   b. WebShell を正常実行ファイルに偽装
6. [Credential Access] OS Credential Dumping (T1003)
   a. メモリダンプ実行
   b. レジストリハイブのコピー保存
7. [Discovery] System Information Discovery (T1082)
   a. システム情報収集
   b. 実行中のプロセス列挙
8. [Lateral Movement] Remote Services: Remote Desktop Protocol (T1021.001)
   a. RDP 接続の有効化
   b. RDP アクセスのためのファイアウォールルールの修正
9. [Collection] Data from Local System (T1005)
   a. ユーザーディレクトリ内ファイル列挙
   b. メモリから敏感情報抽出

10. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
    a. Web シェルを利用した C2 通信およびコマンド実行

35) SectorC08 used information-request phishing email to deliver malware (2025-11-10)

https://cti.nshc.net/events/view/20145

攻撃対象産業群: 政府・行政

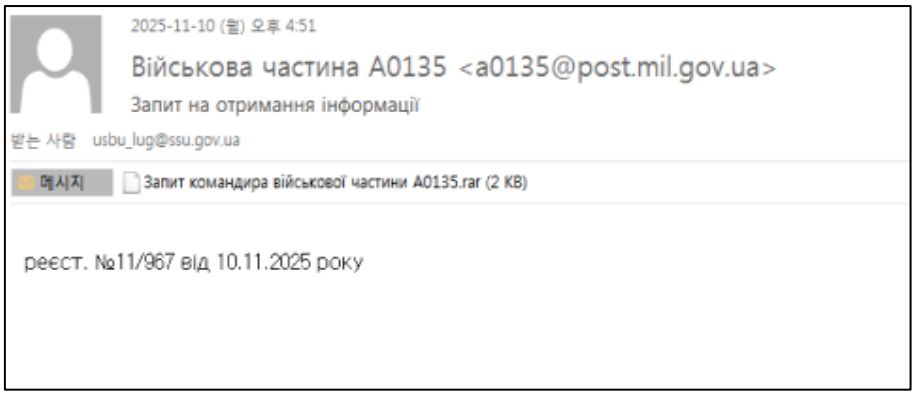
2025 年 11 月 10 日、ウクライナ政府機関に送信されたフィッシングメールは、情報要求に関連する内容に偽装して"Запит командира військової частини A0135.rar"という名前の RAR アーカイブを配布しました。該当アーカイブには、強力に難読化された VBScript を使用して Windows Script Host 機能を実行し、目に見えるウィンドウなしでコマンドを実行する HTA ファイルが含まれていました。このスクリプトは、分析を妨害するためにシステムディレクトリ下のファイルパスを動的に再構成し、断片化された文字列結合を通じて外部 URL を組み立てました。その後、upqdp[.]ax ドメインから追加コンテンツを取得しようと試み、これは段階的な配信プロセスを示しています。最小化された実行、隠された UI 要素、エンコードされたネットワークパラメータの使用は、ユーザーの認識を回避し、基本的なセキュリティ制御を迂回し、追加のペイロード検索を開始しようとする努力を示唆しています。

[Attack Flow]

1. [Reconnaissance] Phishing for Information (T1598)
    a. 公式リクエストを詐称
    b. ウクライナ政府機関住所対象指定
2. [Resource Development] Malicious Domain (T1583.001)
    a. upqdp.ax ドメイン使用
    b. serveirc.com C2 ドメイン活用
3. [Initial Access] Spearphishing Attachment (T1566.001)
    a. RAR 圧縮ファイルが含まれたフィッシングメール
    b. 圧縮ファイル内部 HTA ファイル
4. [Execution] User Execution: Malicious File (T1204.002)
    a. HTA ファイル実行
    b. 難読化された VBScript 実行
5. [Defense Evasion] Obfuscated Files or Information (T1027)
    a. 高度に難読化された VBScript
    b. UI 要素の非表示処理
6. [Defense Evasion] Masquerading (T1036)

a. 公式文書のように偽装
b. エンコードされたネットワークパラメータ使用

7. [Command and Control] Application Layer Protocol (T1071)
   a. 追加コンテンツダウンロード
   b. 外部 URL 再構成
8. [Command and Control] Web Service (T1102)
   a. deads.serveirc.com と C2 通信
   b. serversftp.serveirc.com と C2 通信



[図 7: SectorC08 グループが送信したフィッシングメール]

36) SectorC14 used ClickFix Lure Disguised as CAPTCHA (2025-10-21)

https://cti.nshc.net/events/view/19529

2025 年 5 月、Malware LOSTKEYS の公開以降、国家支援脅威グループが作戦を転換し、5 日以内に新しい Malware ファミリーを開発する。この Malware には NOROBOT という DLL が含まれており、これは欺瞞的な CAPTCHA スタイルの餌を通じて配布される。NOROBOT は多段階感染チェーンを促進し、初期には煩雑な Python バックドアである YESROBOT を使用した後、より効率的な PowerShell バックドアである MAYBEROBOT に転換する。NOROBOT は分析を複雑にするためにキー分割を利用した暗号化を活用し、定期的に進化してきた。感染チェーンは NOROBOT 配信ドメインを通じて取得されたコンポーネントを含み、予約されたタスクを通じて持続性を強化する。MAYBEROBOT のプロトコルは三つのコマンドをサポートし、ダウンロード、コマンド実行、C2 との通信を設定でき、YESROBOT よりも向上した運用の柔軟性を提供する。このグループはファイル名変更およびインフラ回転を通じた回避戦術を使用し、高位人物に対する標的情報収集を継続する。継続的な開発は、検知回避に対する増加した運用速度と集中を示している。

[Attack Flow]

1. [Initial Access] Spearphishing Link (T1566.002)

a. COLDCOPY “ClickFix” ミキ 使用
b. CAPTCHA フォーマット偽装
2. [Execution] Command and Scripting Interpreter: Rundll32 (T1059.003)
a. rundll32 で DLL 実行
b. DLL 内の “humanCheck” エクスポート関数呼び出し
3. [Persistence] Scheduled Task/Job (T1053.005)
a. 永続性確保のためのスケジュールタスク生成
b. ログオンスクリプト構成
4. [Defense Evasion] Obfuscated Files or Information (T1027)
a. 難読化された PowerShell スクリプト
b. ファイルおよびパス名変更
5. [Command and Control] Application Layer Protocol (T1071)
a. HTTPS 基盤通信
b. コマンド処理のためのカスタムプロトコル使用
6. [Collection] Input Capture (T1056)
a. User-Agent にシステム情報を含む
b. ユーザー名エンコーディング
7. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. C2 に確認メッセージを伝達
b. 出力データを C2 パスへ送信

37) SectorC14 used Malware Disguised as Ukrainian Government Emails (2025-10-22)

https://cti.nshc.net/events/view/19560

攻撃対象産業群: 政府・行政、非政府組織(NGO)

2025 年 10 月 8 日に開始された組織的なスピアフィッシングキャンペーンは、国際赤十字社、ユニセフ、戦争救援に関与するウクライナ政府機関内の個人を対象としていた。攻撃者はウクライナ大統領府を装い、武器化された PDF を含むメールを通じて被害者を Zoom に偽装した悪性サイトに誘導し、実際にはロシアインフラにホスティングされていた。被害者は偽の Cloudflare ページに直面し、これは WebSocket ベースの RAT インストールにつながり、リモートコマンド実行とデータ窃取が可能となった。インフラは 1 日間のみ活性化されており、精巧な運用セキュリティを示していた。追加分析の結果、Android デバイスをターゲットにした追加インフラが発見され、偽のアプリケーションを通じて広範なユーザーデータを収集した。攻撃は難読化された PowerShell スクリプトと熟練した社会工学戦術を含む高度な技術能力を示していた。意図はウクライナに関与する主要な人道団体から情報を収集することに重点を置いているように見える。

[Attack Flow]

1. [Reconnaissance] Phishing for Information (T1598)
   a. 標的に対するスピアフィッシングメールの送信
   b. ウクライナ大統領府を装った情報収集の試み
2. [Resource Development] Acquire Infrastructure (T1583)
   a. zoomconference.app ドメイン登録
   b. ロシアを基盤とした VPS サーバーの構築
3. [Initial Access] Spearphishing Link (T1566.002)
   a. PDF 文書に含まれたリンクベースのアクセス誘導
   b. 武器化された文書でユーザーのクリックを誘発
4. [Execution] User Execution: Malicious File (T1204.002)
   a. Cloudflare CAPTCHA に偽装したフィッシングページの表示
   b. ClickFix 系列の社会工学技法でユーザーの実行を誘導
5. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
   a. PowerShell 基盤の持続性スクリプト生成
   b. 難読化されたダウンローダーによる継続的なロード
6. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. 高度難読化された PowerShell スクリプト活用
   b. Execution Policy 回避によるスクリプト実行
7. [Credential Access] Input Capture (T1056)
   a. クリップボード操作を通じた情報の盗み取り
   b. Paste-and-Run 技法を利用したクレデンシャル収集
8. [Discovery] System Information Discovery (T1082)
   a. システム基本情報収集
   b. システム UUID および 環境情報確認
9. [Command and Control] Application Layer Protocol: WebSocket (T1071.001)
   a. WebSocket 基盤 RAT 接続 確立
   b. 暗号化された双方向コマンド・制御通信の実行
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. WebSocket チャネルを通じたデータ流出
    b. Base64 エンコードされた JSON メッセージ送信
11. [Impact] Data Manipulation (T1565)
    a. リモートコマンド実行を通じたシステム操作
    b. 追加 Malware 配布および環境変更

38) SectorD02 used Malware disguised as PDF to deploy UDPGangster (2025-11-14)

https://cti.nshc.net/events/view/20237

攻撃対象産業群: 政府・行政、通信、軍事機関、石油

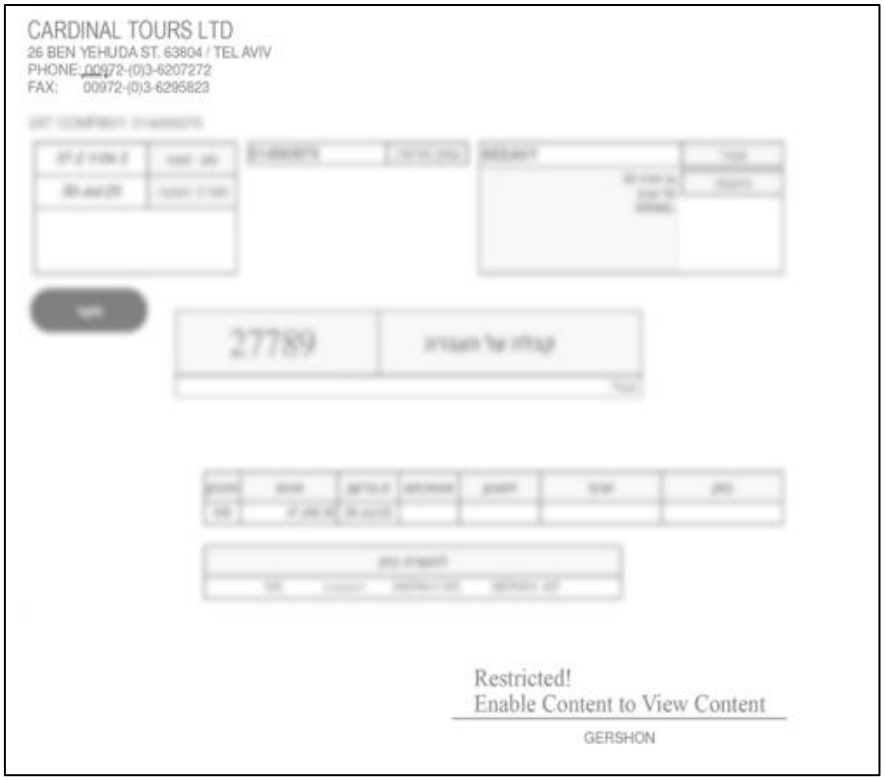
サイバー脅威行為者が特定地域を対象にスピアフィッシング技法を通じて UDPGangster と Phoenix バックドアを配布している。この攻撃はマクロコードを含む PDF および DOC ファイルに偽装した実行ファイルを使用する。ファイルが開かれると、UDPGangster バックドアがインストールされ、スパイ活動を行う。この Malware は検出を避けるために Base64 でエンコードされたファイルをロード時に復号化する方法で巧妙に偽装されている。UDPGangster バックドアはシステム操作、シェルコマンド実行、データ窃取が可能な偽装されたリモートコマンドフレームワークを使用する。攻撃対象は政府、軍事、通信、石油部門にわたり、これは 2017 年以降の脅威行為者の戦略的技術進化を反映し、市販のリモート管理ツールよりカスタムバックドアを優先する。注目すべき点は、バックドアがレジストリ修正を通じて自ら複製し自動起動できる能力である。この攻撃はマクロが含まれた文書と隠蔽された Malware を活用し、隠密で効率的なカスタムスパイフレームワークへの転換を強調する。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
   a. PDF ファイルに偽装した実行ファイル
   b. マクロコードが含まれた DOC 文書
2. [Execution] User Execution: Malicious File (T1204.002)
   a. マクロコード実行
   b. 実行ファイルを開いた後にペイロードが動作
3. [Execution] Command and Scripting Interpreter (T1059)
   a. シェルコマンド実行
   b. PowerShell スクリプト実行
4. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
   a. 自動実行のためのレジストリ Run キーの修正
   b. スタートアップ（Startup）フォルダへのファイル配置
5. [Defense Evasion] Masquerading (T1036)
   a. PDF アイコンを利用した偽装
   b. Base64 エンコーディングおよびデコーディングを通じた内容隠蔽
6. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. C2 サーバーと初期通信の実行

b. 暗号化されたデータ転送

7. [Collection] Data from Local System (T1005)
   a. ホスト情報およびファイル収集
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 暗号化されたデータ流出
   b. コマンド実行結果の送信



[図 8: SectorD02 が活用した文書ファイル]

39) SectorD15 used Phishing and DLL Hijacking on Aerospace Firms (2025-11-18)

https://cti.nshc.net/events/view/20307

攻撃対象産業群: 航空宇宙, IT, 国防, ハイテク

2024 年中盤から洗練された脅威行為者が中東の航空宇宙、航空、防衛産業を対象に諜報活動を行っている。このグループは二重の初期アクセス戦略を使用し、フィッシングキャンペーンを通じて資格情報を奪取したり Malware を配信したりし、第三者のサプライヤー接続を悪用して主要対象の強力な防御を回避するためにセキュリティが低いパートナーを利用する。攻撃期間は 2023 年末から 2025 年までである。攻撃ベクターには IT スタッフにカスタマイズされたフィッシングメール、Citrix、VMWare、Azure サービスを活用したアクセス、DCSYNC 攻撃および DLL ハイジャッキングのような洗練された横移動戦術が含まれる。このグループは TWOSTROKE、LIGHTRAIL、DEEPROOT のようなカスタム Malware と SIGHTGRAB、TRUSTTRAP のようなツールを使用して

データ漏洩および資格情報収集を行い、検出後に活性化される長期間非活性のバックドアを通じて持続性を保証する。彼らの作戦には AWRC および SCCMVNC のようなツールを使用したリモートアクセス技術も含まれ、Malware 検出を回避するためにコード署名証明書を戦術的に使用し、かなりの運用セキュリティと適応力を示しながら諜報効率を維持する。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. 求職関連の内容を含むカスタマイズリンクの使用
2. [Initial Access] Valid Accounts: Third-Party Credentials (T1078.004)
   a. 盗まれた第 3 者アカウントと信頼ベースの接続の活用
3. [Execution] User Execution (T1204)
   a. Malware 添付ファイルまたはリンク実行
4. [Persistence] Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
   a. DLL 検索順序の悪用を通じたカスタムバックドアの起動
5. [Privilege Escalation] Valid Accounts (T1078)
   a. 資格情報収集および DCSync ベースの権限昇格
6. [Defense Evasion] Subvert Trust Controls: Code Signing (T1553.002)
   a. 正常な証明書の悪用およびアプリケーション許可リストの回避
7. [Credential Access] OS Credential Dumping: LSASS Memory (T1003.001)
   a. NTLM ハッシュ収集のための DCSYNCER.SLICK 使用
   b. ブラウザ資格情報収集のための CRASHPAD 活用
8. [Discovery] System Information Discovery (T1082)
   a. AD Explorer を通じた Active Directory 情報の把握
   b. PowerShell 基盤の偵察スクリプト活用
9. [Lateral Movement] Remote Services (T1021)
   a. RDP および PowerShell Remoting を通じた移動
   b. SCCMVNC を利用したリモートアクセス
10. [Collection] Screen Capture (T1113)
    a. SIGHTGRAB を通じた画面キャプチャー
    b. 機微情報の収集対象識別
11. [Command and Control] Ingress Tool Transfer (T1105)
    a. Reverse SSH トンネリング
    b. LIGHTRAIL ツール転送
12. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. TWOSTROKE 基盤 C2 通信を通じたデータ転送
    b. DEEPROOT を利用した外部搬出

40) SectorD30 used TAMECAT Malware disguised as PDF for Espionage (2025-11-18)

https://cti.nshc.net/events/view/20311

攻撃対象産業群: 政府・行政、国防

Sophisticated cyber espionage キャンペーンが国防および政府の高位関係者を対象としており、これは国家的目的のために情報を収集しようとするイラン関連行為者が関与している。この作戦は個別化された社会工学を活用し、成功を高めるために継続的に戦術、技法、手順 (TTP) を適応させる。攻撃者は WhatsApp のようなプラットフォームを通じて対象との長期的な関係構築を通じて信頼を築いた後、"TAMECAT"という PowerShell ベースのバックドアのような技術的手段を展開する。このモジュール型 Malware は Telegram、Discord、WebDAV サーバーのような多角的なチャネルを通じてデータ流出とリモート制御をサポートする。主要な技術的側面には、ファイルレス Malware 実行、偽装された会議ページを通じた資格情報フィッシング、合法的な Windows バイナリとクラウドサービスを活用した高度な持続性メカニズムが含まれる。攻撃インフラはクラウドプラットフォームと洗練された難読化を使用して伝統的なセキュリティ対策を回避し、難読化されたコードとクラウドサービスを指揮および制御作業に活用して部門別の諜報活動を強化する。

[Attack Flow]

1. [Reconnaissance] Gather Victim Information (T1592)
   a. ソーシャルメディア基盤偵察
   b. 専門ネットワーク分析
2. [Resource Development] Acquire Infrastructure (T1583)
   a. クラウドサービス設定
   b. ドメイン登録
3. [Initial Access] Spearphishing Link (T1566.002)
   a. 偽のミーティング招待状の使用
   b. WhatsApp を利用した接触
4. [Execution] User Execution (T1204.001)
   a. LNK ファイル実行
   b. PowerShell スクリプト実行
5. [Persistence] Boot or Logon Autostart Execution (T1547.001)
   a. Run キー 値 修正
   b. UserInitMprLogonScript レジストリ キー 活用
6. [Privilege Escalation] Abuse Elevation Control Mechanism (T1548)
   a. PowerShell 制限言語モード回避
   b. AMSI 回避

7. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Base64 エンコーディング 使用
   b. 文字列オブファスケーション
8. [Credential Access] Input Capture (T1056)
   a. フィッシングページを通じた資格情報の収集
   b. ブラウザデータ抽出
9. [Discovery] System Information Discovery (T1082)
   a. OS およびバージョン情報識別
   b. ネットワーク構成分析
10. [Collection] Data from Local System (T1005)
   a. ドキュメント収集
   b. 画面キャプチャー
11. [Command and Control] Multi-Channel Communication (T1102)
   a. Telegram を基盤とした C2
   b. Discord を基盤とした C2
12. [Exfiltration] Exfiltration Over Alternative Protocol (T1048)
   a. HTTPS データ転送
   b. FTP データ転送

41) SectorD41 used Phishing Emails Disguised as OnlyOffice Links (2025-11-05)
https://cti.nshc.net/events/view/19935

2025 年 6 月から 8 月の間、学界の人物と外交・安全保障分野の専門家を対象に新しい脅威行為者が活動した。該当行為者はイランの国内政治的イシューをミミックとして利用し、対象を誘引し、一般的な会話のテーマと偽造された OnlyOffice ファイルホスティングページを結合し、リモート管理およびモニタリング(RMM)ツールを使用して追加の悪用を試みた。キャンペーンは資格情報の窃取を目的としたフィッシングと RMM ソフトウェアをインストールする MSI ペイロードが含まれた圧縮ファイルの配布を含む。著名人を装ったメールと偽造された URL を使用するなど、いくつかのイラン連携行為者の戦術と類似点が存在するが、特定のグループへの明確な帰属は難しい。また、健康関連および採用関連の Web ドメインを通じた資格情報窃取の試みなど、政策関連イシューを精巧に狙った戦術が観察され、これは高度化されたアプローチを示唆する。既知のグループと戦術が重複する部分があるが、正確な関連性は不明確であり、国家支援型サイバー活動の複雑な様相を明らかにする。

[Attack Flow]

1. [Reconnaissance] Phishing for Information (T1598)
   a. 正常な会話に偽装したアクセス
   b. 専門家を装ったスプーフィングメールの使用
2. [Resource Development] Acquire Infrastructure (T1583)
   a. 健康関連テーマのドメイン登録
   b. 採用関連テーマのドメイン登録
3. [Initial Access] Spearphishing Link (T1566.002)
   a. OnlyOffice URL スプーフィング
   b. Microsoft Teams スプーフィング
4. [Credential Access] Credential Harvesting (T1110.004)
   a. カスタムログインページの使用
   b. 事前に入力されたユーザー情報を含む
5. [Execution] User Execution (T1204)
   a. MSI ファイルの配布
   b. RMM ペイロードが含まれた圧縮ファイル提供
6. [Persistence] Remote Access Software (T1219)
   a. PDQConnect RMM インストール
   b. ISL Online RMM 配布
7. [Command and Control] Application Layer Protocol (T1071)
   a. HTTP ベースの通信
   b. 攻撃者ドメインへの DNS クエリ

42) SectorE04 used PDF Malware disguised as Adobe Reader Update (2025-10-22)

https://cti.nshc.net/events/view/19595

攻撃対象産業群: 政府・行政、外交

2025 年 9 月、ヨーロッパ大使館とスリランカ、パキスタン、バングラデシュを含む複数の南アジア諸国を対象とした大規模なサイバー諜報キャンペーンが発生した。攻撃者は外交的目標に合わせた独特なメールテーマを特徴とする精巧なフィッシング攻撃を活用した。これらのメールは被害者に悪性な Adobe Reader アップデートや脆弱性が含まれた Microsoft Word 文書をダウンロードさせるよう誘導した。配布された Malware である ModuleInstaller と StealerBot は諜報を目的として制作された。このキャンペーンは従来の Word 文書ベクターとは大きく異なる ClickOnce および PDF ベースの感染チェーンを導入した。2025 年 3 月から 9 月まで複数のフィッシング攻撃が発生し、各攻撃は地域の外交および政府機関を集中的に狙った。PDF 感染はユーザーが偽の Adobe Reader をダウンロードするようにし、ジオフェンス(Geofence)ベースの ClickOnce アプリケーションが実行された。これにより攻撃者は合法的アプリケーションの形を装ったサイドローディング(Sideloading)方

式で検出を回避し Malware をインストールした。隠蔽性のための追加技術としては、動的に生成されるジオフェンスベースの URL、短命の多形性ペイロード(Polymorphic Payload)などが活用され、類似ドメイン(Lookalike Domain)で構成されたインフラは検出を回避するために迅速に変更・適応する特徴を示した。攻撃の特性と状況を総合すると、持続的に地政学的緊張が存在する地域を標的とし、同じ悪性ツールおよびインフラを繰り返し使用する点を根拠に特定の APT グループの活動に帰属される。このキャンペーンは南アジア地域で進化するサイバー脅威に対応するために、セキュリティ体制の持続的適応と先制的対応の重要性を再び浮き彫りにした。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
   a. PDF/Word 添付ファイルを利用したメールの餌
   b. 偽の Adobe Reader 更新通知
2. [Execution] User Execution (T1204)
   a. ClickOnce アプリケーションダウンロード
   b. Word 文書における CVE-2017-0199 の悪用
3. [Persistence] Boot or Logon Autostart Execution (T1547.001)
   a. レジストリ Run キー登録
   b. スタートアップフォルダ項目作成
4. [Defense Evasion] Signed Binary Proxy Execution (T1218)
   a. MagTek Inc. アプリケーションサイドローディング
   b. DEVOBJ.dll を利用した DLL ハイジャック
5. [Credential Access] Credential Dumping (T1003)
   a. StealerBot Malware 配布
   b. ModuleInstaller 実行
6. [Discovery] System Information Discovery (T1082)
   a. システムプロファイリング
   b. セキュリティソフトウェア検出
7. [Collection] Data from Local System (T1005)
   a. 自動化されたデータ収集
   b. ライブラリを通じたアーカイビング
8. [Command and Control] Application Layer Protocol (T1071.001)
   a. C2 通信のためのウェブプロトコルの使用
   b. 非対称暗号化を活用した暗号化チャネル
9. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. HTTP/S を通じたデータ流出
   b. 通信時にプロキシ使用

43) SectorE04 used Phishing Domain disguised as Sri Lanka Navy login page (2025-11-14)

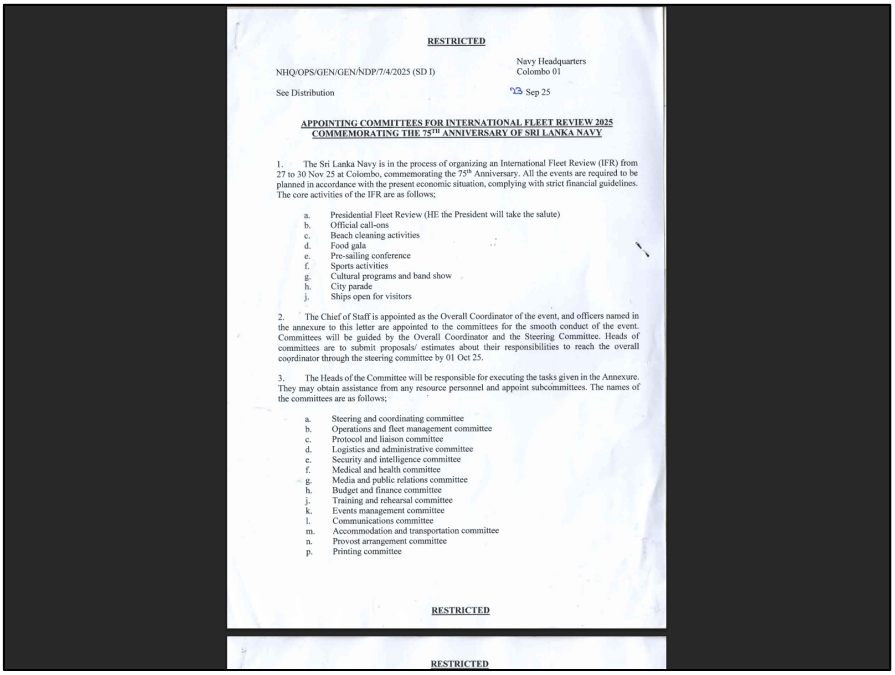
https://cti.nshc.net/events/view/20240

攻撃対象産業群: 軍事機関

Copeparliament[.]github.io/mails[.]navy.lk にホスティングされたフィッシングページは、Zimbra ウェブクライアントのログインインターフェースを装い、資格情報を収集するように設計されている。サイトをロードすると、まず PDF ドキュメントを餌として表示し、その後偽のログインフォームを明らかにする。内蔵されたスクリプトは、URL からユーザー名パラメータを自動的に抽出し、ログインフィールドに挿入することで、合法的なリダイレクトセッションのように見せかける。右クリックなどのユーザーインタラクションは無効化されており、正常なウェブメール動作を模倣するために時間に応じたコンテンツの切り替えが使用される。 被害者が資格情報を送信すると、そのデータは mailsserver-lk[.]com/nxxy/action.php にある攻撃者管理下のエンドポイントへ送られ、不正な資格情報の収集が可能になる。スリランカ海軍テーマのパスと Zimbra スタイルインターフェースの構造的使用は、海軍通信システムに関連するユーザーを対象としていることを示している。PDF 表示、自動フィールド入力、資格情報送信の制御された順序は、軍事関連のメールアカウントを侵害するためのカスタマイズされたフィッシングワークフローを反映している。

[Attack Flow]

1. [Reconnaissance] Gather Victim Organization Information (T1591)
   a. スリランカ海軍対象識別
   b. GitHub Pages 基盤インフラ構築
2. [Resource Development] Acquire Infrastructure: Web Services (T1583.006)
   a. Zimbra Web Client を装ったフィッシングページの作成
   b. ドメイン登録(mailsserver-lk[.]com)
3. [Initial Access] Spearphishing Link (T1566.002)
   a. 偽のログインページ
   b. PDF 文書を利用したミキ提供
4. [Credential Access] Input Capture: Web Portal Capture (T1056.003)
   a. URL パラメーターを通じた自動ユーザー名抽出
   b. 攻撃者サーバーへ資格情報送信
5. [Defense Evasion] Impair Defenses (T1562)
   a. ユーザーインタラクションの無効化(右クリックのブロック)
   b. Web メールと類似した動作のための時間ベースのコンテンツ転換



RESTRICTED

NHQ/OPS/GEN/GEN/NDP/7/4/2025 (SD I)

Navy Headquarters
Colombo 01

See Distribution

Sep 25

APPOINTING COMMITTEES FOR INTERNATIONAL FLEET REVIEW 2025 COMMEMORATING THE 75TH ANNIVERSARY OF SRI LANKA NAVY

1. The Sri Lanka Navy is in the process of organizing an International Fleet Review (IFR) from 27 to 30 Nov 25 at Colombo, commemorating the 75th Anniversary. All the events are required to be planned in accordance with the present economic situation, complying with strict financial guidelines. The core activities of the IFR are as follows;

a. Presidential Fleet Review (HE the President will take the salute)
b. Official call-ons
c. Beach cleaning activities
d. Food gala
e. Pre-sailing conference
f. Sports activities
g. Cultural programs and band show
h. City parade
j. Ships open for visitors

2. The Chief of Staff is appointed as the Overall Coordinator of the event, and officers named in the annexure to this letter are appointed to the committees for the smooth conduct of the event. Committees will be guided by the Overall Coordinator and the Steering Committee. Heads of committees are to submit proposals/ estimates about their responsibilities to reach the overall coordinator through the steering committee by 01 Oct 25.

3. The Heads of the Committee will be responsible for executing the tasks given in the Annexure. They may obtain assistance from any resource personnel and appoint subcommittees. The names of the committees are as follows;

a. Steering and coordinating committee
b. Operations and fleet management committee
c. Protocol and liaison committee
d. Logistics and administrative committee
e. Security and intelligence committee
f. Medical and health committee
g. Media and public relations committee
h. Budget and finance committee
j. Training and rehearsal committee
k. Events management committee
l. Communications committee
m. Accommodation and transportation committee
n. Provost arrangement committee
p. Printing committee

RESTRICTED

RESTRICTED

[図 9: SectorE04 が活用した文書]

44) SectorE05 used WinRAR Vulnerability Disguised as Templates (2025-11-07)

https://cti.nshc.net/events/view/20116

攻撃対象産業群: 政府・行政、軍事機関

最近のサイバー脅威事件は、南アジアの政府、外交使節団、教育機関および防衛産業を対象に、敏感な情報を窃取するために発生し、政治的動機のあるアジェンダを強調している。この攻撃は、WinRAR の脆弱性(CVE-2025-6218)を利用してディレクトリトラバーサル(Directory Traversal)攻撃を実行した。悪性 RAR ファイル "Provision of Information for Sectoral for AJK.rar"は、この脆弱性を悪用して攻撃者が Microsoft Word テンプレートディレクトリに悪性 "Normal.dotm" ファイルを配置できるようにし、これは Word 文書が開かれるときに実行を誘発する。"Normal.dotm"に含まれるマクロは "net use"を通じてリモートディレクトリをマッピングし、"winnsc.exe"のような追加ペイロードをダウンロードしてホストデータをコマンド&コントロールサーバーに送信することでリモートコマンドを実行した。攻撃者がテストしたもう一つのペイロードは、マクロを使用してリモート URL からコマンドをダウンロードし、これは損傷したシステムで持続性と制御を達成するために知られた脆弱性と洗練されたロード配信方法を継続的に使用していることを示している。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. WinRAR ディレクトリ トラバーサル 脆弱性 悪用 (CVE-2025-6218)
   b. 悪性 RAR ファイルの配布
2. [Execution] User Execution (T1204)

a. Malware Normal.dotm マクロ実行
b. Word 文書 実行トリガー
3. [Persistence] Office Application Startup (T1137.001)
a. Templates ディレクトリに Normal.dotm 配置
b. Word 実行時に自動実行
4. [Command and Control] Application Layer Protocol (T1071)
a. リモートディレクトリマッピング(net use)
b. URL を通じたコマンドダウンロード
5. [Collection] Data from Local System (T1005)
a. ホスト名およびユーザー名収集
b. システムバージョン情報収集
6. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. C2 サーバーに POST リクエストを送信
b. teamlogin.esanojinjasvc[.]com にデータ送信
7. [Defense Evasion] Masquerading (T1036)
a. Normal.dotm ファイル偽装
b. 正常な Word テンプレートパスの使用

45) SectorH03 used Linux Malware disguised as Defense Orders (2025-10-23)

https://cti.nshc.net/events/view/19593

攻撃対象産業群: 政府・行政、国防

2025 年 7 月、インド政府機関の Linux ベースのシステムを対象としたフィッシングキャンペーンが検出された。この作戦は 2025 年 6 月に開始され、初期攻撃ベクターとしてフィッシングメールを活用し、しばしばステージングサーバーにホスティングされた ZIP アーカイブに接続する URL を含んでいる。これらのアーカイブには悪性コマンドを含む DESKTOP ファイルが含まれており、実行時に Golang ベースの RAT である DeskRAT をダウンロードして実行する。DeskRAT は WebSocket 通信を通じてコマンド＆コントロールを設定し、戦略的利益に合致するサイバースパイ活動を行うことを目的としている。感染チェーンは多段階ペイロード配信を含み、Bash スクリプトを活用して /tmp/ディレクトリからペイロードをダウンロード、デコード、実行する。このキャンペーンはインド政府で広く使用されている Bharat Operating System Solutions (BOSS)ディストリビューションを対象としている。DeskRAT は Linux に特化した複数の持続性技法を特徴としており、ネットワークトラフィックを偽装するために偽データを使用する。これは WebSockets を通じて C2 サーバーと通信し、クライアント管理およびリモートファイル相互作用のための機能を含んでおり、インドの地域的緊張を悪用するためのスパイ活動目標によって駆動されている。

[Attack Flow]

1. [Initial Access] Spearphishing Link (T1566.002)
   a. URL が含まれたフィッシングメール送信
   b. ステージングサーバーにアップロードされた ZIP アーカイブ使用
2. [Execution] User Execution: Malicious File (T1204.002)
   a. DESKTOP ファイル実行
   b. Bash ワンライナー 実行
3. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. systemd サービス生成
   b. crontab でのジョブ追加
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Base64 エンコーディング 使用
   b. PNG データ挿入
5. [Collection] Data from Local System (T1005)
   a. ファイル検索および収集
   b. ディレクトリー覧の閲覧
6. [Command and Control] Web Protocols (T1071.001)
   a. WebSocket 基盤 通信
   b. C2 サーバー接続
7. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. WebSocket を通じたファイル転送
   b. C2 ベースのデータ流出

46) SectorU01 used LNK Malware disguised as strategic cooperation plan (2025-11-03)

https://cti.nshc.net/events/view/19851

攻撃対象産業群: 政府・行政、運送、鉱業

Sophisticated cyber espionage group が中央アジア政府、ロシア外交機関、そして運送、通信、鉱業分野の企業を対象に攻撃を行っている。このキャンペーンは 2025 年 6 月から 10 月まで追跡され、ドゥシャンベやアスタナのような場所での政府間首脳会談に関連する戦略文書に偽装した悪性 RAR アーカイブを含むスピアフィッシングメールを使用した。これらのアーカイブは GitHub で悪性 PowerShell スクリプトを実行する LNK ファイルを含んでおり、任意のコマンドを実行できる TCP ベースのリバースシェルを提供した。このグループは Silent Loader と LAPLAS のようなカスタム Malware インプラントを使用し、Base64 エンコーディングと Ligolo-ng のようなオープンソースのトンネリングツールを活用した。攻撃は主に諜報と情報収集を目的としており、政治およびインフ

ラ開発に重点を置いていた。また、持続性を維持するための手法として、アクセスを維持するための欺瞞的な予約タスクを含んでいた。この脅威行為者の活動は複数の国にまたがっており、中央アジア地域の外交およびインフラ運営に対する戦略的関心を示していた。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
   a. 悪性 RAR アーカイブ使用
   b. 戦略文書テーマ活用
2. [Execution] User Execution: Malicious File (T1204.002)
   a. LNK ファイル実行
   b. PowerShell スクリプトダウンロード
3. [Execution] Command & Scripting Interpreter: PowerShell (T1059.001)
   a. Base64 エンコーディング コマンド 使用
   b. リバースシェル実行
4. [Persistence] Scheduled Task/Job: Windows Task Scheduler (T1053.005)
   a. WindowsUpdate タスクの作成
   b. 定期的なタスクの実行
5. [Command and Control] Application Layer Protocol (T1071)
   a. TCP ベースのリバースシェル
   b. HTTPS 基盤通信
6. [Command and Control] Proxying & Tunneling (T1071 / T109)
   a. Ligolo-ng トンネリング使用
   b. 暗号化された通信
7. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. C2 を通じたデータ転送
   b. アプリケーションレイヤープロトコル活用

47) SectorU01 used Phishing Emails with Malware (2025-11-06)

https://cti.nshc.net/events/view/19907

攻撃対象産業群: 政府・行政

2025 年 7 月、ロシアのある政府機関が内部ネットワークからのスパムメールを通じてサイバー犯罪者の標的となった。この攻撃は、機密データを奪取しようとする高度なハッキンググループと関連していた。攻撃者はまだ検出されていないバックドアである BackDoor.ShellNET.1 が含まれたフィッシングメールを使用し、これはリバースシェルを通じてリモートコマンド実行を可能にする。この Malware はパスワードで保護されたアーカイブに隠され、一般的なフィッシングキャンペーンを通

じて配信された。攻撃者は Bitsadmin のような Windows ツールを使用して追加の Malware をダウンロードし、そこには文書や画像を奪取するための Trojan.FileSpyNET.5 が含まれていた。その後、彼らは BackDoor.Tunnel.41 およびその他の Malware を配布して、隠密なコマンド実行のための SOCKS5 トンネルを生成した。攻撃者は複数のオープンソースツールとリバースシェルバックドアを使用し、しばしば Malware を見かけ上無害なプログラムに挿入し、Telegram API を活用して制御した。この攻撃は、フィッシング、リバースシェル、そして Malware 配信および持続性のための合法的なシステムツールの使用など、高度な技術を強調している。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
   a. フィッシングメールに含まれた悪性文書
   b. パスワードで保護された圧縮ファイル
2. [Execution] User Execution (T1204)
   a. マルウェア添付ファイルを開く（ドキュメントに偽装）
   b. リバースシェル実行
3. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.003)
   a. Bitsadmin 使用
   b. cmd.exe でツール実行
4. [Persistence] Registry Run Keys / Startup Folder (T1547.001)
   a. レジストリ修正
   b. スタートアップフォルダの活用
5. [Defense Evasion] BITS Jobs (T1197)
   a. 正常なツールの悪用
   b. バックグラウンド作業で活動隠蔽
6. [Credential Access] OS Credential Dumping (T1003)
   a. 資格情報収集
   b. ユーザー情報収集
7. [Discovery] System Information Discovery (T1082)
   a. ネットワーク構成確認
   b. ユーザー列挙
8. [Lateral Movement] Remote Services (T1021)
   a. SOCKS5 トンネル使用
   b. リバースプロキシ設定
9. [Collection] Data from Local System (T1005)
   a. 文書脱取および画像収集

10. [Command and Control] Bidirectional Communication (T1102.002)
    a. リバースシェル接続
    b. Telegram API 制御
11. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. C2 通信を通じたデータ流出
    b. Web サービス基盤の流出

2. サイバー犯罪(Cyber Crime) ハッキンググループ活動

1) SectorJ01 used SSH Backdoor Malware disguised as install.bat Script (2025-11-18)

https://cti.nshc.net/events/view/20305

攻撃対象産業群: 金融, 小売, 観光・宿泊

分析結果、2022 年から少なくとも複数の部門を対象に Malware SSH ベースのバックドアを通じて攻撃を行ったサイバー脅威行為者と関連する複数の疑わしいファイルが識別された。この Malware は、知られているサイバー犯罪グループによって使用されたと疑われ、持続性を確立し、コマンド&コントロール通信のためのリバース(Reverse) SSH トンネルを生成して SFTP を通じたデータ流出を可能にする。攻撃は、リモートサーバーから"install.bat"でラベル付けされたスクリプトを含む ZIP ファイルをダウンロードすることを含む。この Malware は、小売、観光・宿泊、金融サービス関連の産業群で使用されたことが確認されており、POS(point-of-sale) Malware からビッグゲームハンティング(Big Game Hunting)ランサムウェアへと進化した。Malware は寿命が長かったにもかかわらず、Malware のコードには最小限の変化しかなかった。最近のサンプルには、2025 年 9 月に初めて観察されたバックドアインストール ZIP ファイルおよびバッチスクリプトのような多様なコンポーネントが含まれている。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
    a. ZIP ファイルダウンロード
    b. "install.bat" スクリプト実行
2. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.003)
    a. バッチスクリプトの実行
    b. バックドア設置初期化
3. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)

a. 持続性メカニズム設定
b. 開始コンポーネントの修正
4. [Command and Control] Application Layer Protocol: SSH (T1071.004)
a. リバース SSH トンネル生成
b. C2 通信維持
5. [Exfiltration] Exfiltration Over Alternative Protocol: SFTP (T1048.003)
a. SFTP を通じたデータ転送
b. SSH を基盤とした流出の実行

2) SectorJ09 used Malware Disguised as Rogue WordPress Plugin (2025-10-29)

https://cti.nshc.net/events/view/19743

WooCommerce プラグインを使用する WordPress 電子商取引サイトを標的とする精巧な Malware キャンペーンが識別された。この Malware は悪意のある WordPress プラグインに偽装し、カスタム暗号化方法と仮想イメージを使用した高度な難読化を通じてペイロードを隠す。2025 年 8 月 21 日に検出されたこの Malware は、ユーザーデータを記録し、自身の存在を隠しながら AJAX エンドポイントを通じて持続的なバックドアアクセスを設定する。ログイン過程で資格情報をキャプチャし、クッキーを使用してデータの持続性を維持することで、ログイン資格情報とユーザーデータを流出させる。多段階攻撃戦略が使用され、決済ページでクレジットカードスキミング(Skimming)を容易にする。スキミングロジックは偽の PNG イメージに隠されており、リモートコントロールを通じて動的に更新される。この Malware は cURL リクエスト、file_get_contents、メールバックアップを含む様々な方法でデータ流出を行う。戦術、ドメイン、コーディングスタイルの類似性により、既知の脅威行為者との関連性を示唆する証拠がある。主要な侵害指標には特定のクッキーと C&C リクエストパターンが含まれる。このキャンペーンは高い技術的精巧さを示し、サイトセキュリティとユーザーデータの完全性に重大な脅威を与える。

[Attack Flow]

1. [Initial Access] Drive-by Compromise (T1189)
a. 悪意のある WordPress プラグイン使用
2. [Execution] Command and Scripting Interpreter (T1059)
a. PHP コード実行
b. AJAX バックドア アクセス
3. [Persistence] Implant Container Image (T1525)
a. マルウェアプラグインのインストール
b. 難読化された PHP 関数の使用
4. [Defense Evasion] Obfuscated Files or Information (T1027)

a. ユーザー定義の暗号化技法の使用
b. ペイロード隠蔽のための偽装画像の利用
5. [Credential Access] Input Capture (T1056)
a. 資格証明書の盗み取り
b. Cookie を基盤とした保存
6. [Discovery] System Information Discovery (T1082)
a. ユーザー IP 記録
b. ユーザー役割識別
7. [Collection] Input Capture (T1056)
a. クレジットカード情報スキミング
b. クリップボード基盤スキミング
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. cURL リクエストの利用
b. メールバックアップの流出
9. [Command and Control] Application Layer Protocol (T1071)
a. C&C サーバー通信
b. 動的ペイロードアップデート

3) SectorJ109 deployed RoningLoader via fake software installer (2025-11-15)
https://cti.nshc.net/events/view/20157

最近のサイバー脅威キャンペーンでは、攻撃者は Google Chrome や Microsoft Teams のような合法的なソフトウェアに偽装したトロイの木馬化された NSIS インストーラーを使用して、gh0st RAT 変種を配布します。2025 年 8 月に検出されたこのキャンペーンは、主に中国語ユーザーを対象としており、Protected Process Light (PPL) の悪用を通じて Windows Defender を無効化し、署名されたカーネルドライバーを配布してセキュリティプロセスを終了するなどの技術を活用します。攻撃はトロイの木馬化された NSIS インストーラーで始まり、これは追加の悪性コンポーネントのドロッパーとして機能します。ここには、アンチウイルスプロセスを終了するために使用されるドライバー ollama.sys と、VSS サービスのような信頼できるサービスにプロセスを注入するためのシェルコードが含まれます。Malware は複数のステージを活用し、RoningLoader という独自のローダーを含め、AV プロセス終了のためのファントム DLL やシステムプロセスに対するコマンド注入のような洗練された技術を使用して持続性を維持し、コマンド＆コントロール (C2) サーバーと通信します。最終ペイロードである gh0st RAT 変種は C2 通信のために XOR 暗号化を使用し、キー入力ログ、クリップボード監視、アンチウイルス回避のような機能を実装して、持続的かつ進化する脅威として示されます。

[Attack Flow]

1. [Execution] User Execution (T1204)
   a. トロイの木馬化された NSIS インストーラー使用
2. [Execution] Command and Scripting Interpreter (T1059)
   a. バッチスクリプト実行
   b. シェルコード実行
3. [Persistence] Create or Modify System Process (T1543)
   a. サービス生成で持続性確保
   b. サービス再起動用バッチスクリプト使用
4. [Privilege Escalation] Abuse Elevation Control Mechanism (T1548)
   a. レジストリ修正ベースの UAC 回避
   b. runas コマンドを通じた権限昇格
5. [Defense Evasion] Signed Binary Proxy Execution (T1218)
   a. Regsvr32 を利用した DLL 実行
   b. ClipUp.exe を利用した PPL 悪用
6. [Defense Evasion] Modify Registry (T1112)
   a. Windows Defender 無効化
   b. WDAC ポリシー変更
7. [Defense Evasion] Masquerading (T1036)
   a. 正常なソフトウェアに偽装
8. [Credential Access] Input Capture (T1056)
   a. キー入力ロギング
9. [Discovery] System Information Discovery (T1082)
   a. AV 検出のためのプロセススキャン
   b. システムバージョンおよび IP 情報収集
10. [Lateral Movement] Remote Services (T1021)
    a. 信頼されたサービスにプロセスインジェクション
    b. リモートスレッド生成
11. [Collection] Data from Local System (T1005)
    a. クリップボードデータの窃取
    b. アクティブウィンドウのタイトル記録
12. [Command and Control] Encrypted Channel (T1573)
    a. XOR 基盤 C2 通信
    b. Raw TCP ソケット 基盤 通信
13. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. C2 にビコン送信

b. C2 コマンドを通じたデータ流出

4) SectorJ131 exploited ActiveMQ Vulnerability (2025-10-28)

https://cti.nshc.net/events/view/19725

最近のサイバー脅威事件は、行為者が ActiveMQ 脆弱性 CVE-2023-46604 を悪用して Linux と Windows プラットフォーム全般に Malware を配布することを含む。この悪用は OpenWire プロトコルでシリアライズされたクラスタイプを操作してリモートで悪性コマンドを実行し、影響を受けたシステムを制御することを含む。攻撃者は、暗号通貨採掘のための XMRig および PowerShell Empire をサポートする.NET バックドアである Sharpire のような複数のダウンロード型 Malware を含む様々な Malware を配布してきた。これらの活動は、Cobalt Strike や Meterpreter のような精巧なツールを同時に使用して、損傷したシステムをさらに制御し、再利用された SSH 資格情報を利用した側面移動のような技術を使用することで注目に値する。攻撃者は、誤って構成されたサービスと新たに公開された脆弱性を悪用して彼らの作戦を継続してきた歴史を持ち、これはパッチが適用されていない Apache ActiveMQ サーバーに対する継続的な脅威を強調する。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. ActiveMQ CVE-2023-46604 脆弱性 悪用
   b. OpenWire プロトコル 操作
2. [Execution] Command and Scripting Interpreter (T1059)
   a. msiexec を利用した MSI インストール実行
   b. mm13.exe ダウンローダー実行
3. [Persistence] Implant Internal Image (T1547.014)
   a. Sharpire .NET バックドア 配布
   b. PowerShell Empire 使用
4. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
   a. Cobalt Strike 使用
   b. Meterpreter 活用
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. シリアライズされたクラス操作手法使用
   b. Bash スクリプト配布
6. [Credential Access] Unsecured Credentials (T1552)
   a. SSH 資格情報収集
   b. 保存された資格情報へのアクセス
7. [Discovery] System Information Discovery (T1082)

a. ifconfig/ipconfig 実行
b. ps/tasklist 実行
8. [Lateral Movement] Use Alternate Authentication Material (T1550)
a. SSH 資格情報の再利用
b. 誤って構成されたサービスアクセス
9. [Command and Control] Application Layer Protocol (T1071)
a. Cobalt Strike ビーコン 使用
b. Meterpreter セッション活用
10. [Impact] Resource Hijacking (T1496)
a. XMRig マイナー配布
b. 暗号通貨マイニングの実行

5) SectorJ136 used Phishing and Smishing for Gift Card Fraud (2025-10-22)

https://cti.nshc.net/events/view/19561

攻撃対象産業群: 小売

2021 年からモロッコの金銭的動機を持つ攻撃者たちが主導した Jingle Thief キャンペーンは、大規模ギフトカード詐欺のために小売および消費者サービス分野のグローバル企業を標的にする。フィッシングとスミッシングを使用して攻撃者たちは組織の Microsoft 365 環境にアクセスするための資格情報を脱取する。彼らは SharePoint や OneDrive のようなクラウドサービスを活用してギフトカード発行手続きに関する機密情報を収集する。脅威行為者たちは偵察を行い、長期的な持続性を維持し、詐欺の機会が増加する祭りのシーズンに合わせて攻撃を調整する。彼らは Malware を避け、代わりに資格情報の脱取を通じてユーザーを偽装し、無断ギフトカード発行を可能にする。長期間アクセスを維持しながらクラウドベースの資格情報を使用して隠密な内部フィッシング、メール漏洩、持続性のための不良デバイス登録を行うことにおいて適応力を示す。このキャンペーンは詐欺活動のためにクラウド機能を悪用し、主にモロッコ IP から広範な難読化なしで運営され、地域通信インフラを活用する。

[Attack Flow]

1. [Initial Access] Spearphishing Link (T1566.002)
a. Microsoft 365 のログインページを装った フィッシング
b. SMS を基盤としたスミッシング攻撃
2. [Execution] User Execution (T1204)
a. Malware URL クリック
b. 偽のログインポータルに資格情報を入力
3. [Persistence] Account Manipulation (T1098)

a. Microsoft Entra ID に Malware デバイス登録
b. 認証アプリの悪用を通じた MFA 回避
4. [Privilege Escalation] Valid Accounts (T1078)
a. クラウドサービスアクセスのための資格情報再利用
b. セッショントークンの脱取を通じた持続的アクセスの維持
5. [Defense Evasion] Hide Artifacts (T1564)
a. メール非表示ルールの設定
b. メールボックスデータ削除
6. [Credential Access] Credentials from Password Stores (T1555)
a. フィッシングに基づく資格情報収集
b. パスワードリセット機能の悪用
7. [Discovery] Cloud Service Discovery (T1526)
a. SharePoint 偵察
b. OneDrive の探索
8. [Lateral Movement] Internal Spearphishing (T1534)
a. 内部フィッシング(IT 通知偽装)
b. 内部信頼構造悪用を通じた資格証明脱取
9. [Collection] Data from Cloud Storage (T1530)
a. SaaS ファイルダウンロード
b. ギフトカード関連の敏感情報へのアクセス
10. [Exfiltration] Exfiltration Over Web Service (T1567)
a. 自動フォワーディングルールを通じたメール流出
b. クラウドサービス基盤データ流出

6) SectorJ175 used DragonForce Ransomware for global cyber attacks (2025-11-04)

https://cti.nshc.net/events/view/20044

攻撃対象産業群: 小売、保険、管理サービス提供業者

2023 年から活動を開始したサイバー犯罪グループがランサムウェアカルテルに発展し、アフィリエイトにサービスをプロモーションしている。このグループはカスタマイズされたランサムウェアペイロードを提供し、共有インフラと収益を通じて参入障壁を下げ、協力を奨励している。カルテルは競合他社のウェブサイト改ざんから他の犯罪団体との広範な同盟に転換し、小売、航空会社、保険など世界中の 200 以上の被害者を対象としている。最近の活動には、truesight.sys や rentdrv2.sys のような脆弱性を利用してセキュリティ防御を無力化し、暗号化を強化する新しい Malware 変種が含まれており、これは過去の弱点を補完している。英国小売業者に対する注目すべき攻撃は、フィッシングと MFA 回避を専門とする初期アクセスブローカーとの協力に関連していた。カルテルはプロセ

ス終了のための BYOVD を含む高度な技術を使用し、ソーシャルエンジニアリングを活用してアクセス権を得て、共有パートナーシップを通じて範囲を拡大している。流出したコードベースから強化された彼らの Malware は、引き続き適応し、サイバー犯罪の世界での地位を強化している。

[Attack Flow]

1. [Reconnaissance] Gather Victim Identity Information (T1589)
   a. ソーシャルメディア基盤偵察
   b. オープンソース情報(OSINT)収集
2. [Resource Development] Establish Accounts (T1585)
   a. ペルソナ生成
   b. 事前テキスト(pretext) 制作
4. [Initial Access] Exploit Public-Facing Application (T1190)
   a. 脆弱なドライバー悪用
   b. BYOVD を通じたプロセス終了
5. [Execution] Command and Scripting Interpreter (T1059)
   a. RMM ツール配布
   b. トンネリングサービス使用
6. [Persistence] Account Manipulation (T1098)
   a. 攻撃者デバイス登録
   b. 資格証明のリセット
7. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
   a. 脆弱なドライバー悪用
   b. プロセス終了
8. [Defense Evasion] Disable or Modify Tools (T1562)
   a. セキュリティソフトウェア無効化
   b. 保護されたプロセス終了
9. [Credential Access] OS Credential Dumping (T1003)
   a. 資格情報ストアの列挙
   b. Active Directory 情報 列挙
10. [Discovery] System Network Configuration Discovery (T1016)
    a. ネットワークマッピング
    b. SharePoint ナビゲーション
11. [Lateral Movement] Remote Services (T1021)
    a. AWS Systems Manager Inventory 使用
    b. データ収集のための ETL ツール活用
12. [Collection] Data from Information Repositories (T1213)

a. バックアップシステム関連文書の収集
b. VPN 設定情報確保
13. [Exfiltration] Exfiltration Over Web Service (T1567)
a. MEGA ストレージ活用
b. Amazon S3 ストレージ活用
14. [Impact] Data Encrypted for Impact (T1486)
a. ChaCha20 基盤暗号化
b. RSA キー追加適用

7) SectorJ197 used KongTuke TDS with fake CAPTCHA for PowerShell attack (2025-11-18)

https://cti.nshc.net/events/view/20326

精巧なサイバー脅威事件は、ユーザーを欺くために偽の CAPTCHA ページを餌として使用するキャンペーンを含む。この作戦は少なくとも 2024 年 5 月から活動中であり、KongTuke が注入したスクリプトを挿入して損傷したウェブサイトを悪用する。2025 年 11 月 17 日、合法的なウェブサイトが損傷されたことが発見され、感染トラフィックシナリオが引き起こされた。攻撃方法はクリップボードハイジャッキングを使用して悪性テキストを注入し、ユーザーが Windows システム、特に Active Directory 環境で PowerShell スクリプトをダウンロードして実行するよう誘導する。このスクリプトは悪性 Python スクリプトと Windows Python 環境を含む zip アーカイブを取得する。この Python パッケージは AppData¥Roaming ディレクトリに保存され、予約タスクを通じて持続性を確立する。感染は telegra[.]ph で HTTPS トラフィックを生成するが、特定の URL や内容は確認されていない。初期感染に関連する主要 URL は特定の IP の複数のリソースを含み、特に Python パッケージのダウンロードを容易にする。

[Attack Flow]

1. [Initial Access] Drive-by Compromise (T1189)
a. 侵害されたウェブサイト
b. KongTuke が注入したスクリプト
2. [Execution] User Execution (T1204)
a. 偽の CAPTCHA ページ
b. クリップボードハイジャック
3. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
a. 悪意のある PowerShell コマンドの実行
b. スクリプトのダウンロードおよび実行
4. [Persistence] Scheduled Task/Job (T1053)

a. 予約タスクの作成
b. 持続性メカニズムの確保
5. [Defense Evasion] Masquerading (T1036)
a. 正規ユーザーの操作に偽装
b. 偽の CAPTCHA ミカケ 使用
6. [Command and Control] Encrypted Channel (T1573)
a. telegra[.]ph への HTTPS トラフィック
b. 未確認 URL/コンテンツ

8) SectorJ220 used Smishing Disguised as Toll Violation Notices (2025-10-23)

https://cti.nshc.net/events/view/19596

攻撃対象産業群: 銀行

2024 年 4 月から始まった身元不明の脅威行為者が主導する大規模なスミッシングキャンペーンが、アメリカ居住者を対象に偽の通行料違反および誤った配送通知で攻撃している。このキャンペーンは、銀行、医療、法執行、電子商取引、暗号通貨プラットフォームなどの主要部門のサービスを装い、SMS メッセージを通じて巧妙な社会工学的戦術を使用する。攻撃者は、香港に基づく登録機関とアメリカに基づくクラウドホスティングを主に使用して毎週数千の Malware ドメインを登録し消費している。2024 年 1 月時点で、この作戦に関連する 194,000 以上のドメインが確認された。キャンペーンの分散した特性により、数多くのドメインとホスティングインフラを活用して検出が複雑化している。これらのスミッシングメッセージは緊急性を誘発し、現実的なフィッシングページを通じて被害者から機密情報を収集することを目的としており、これは資源が豊富なフィッシング-サービス-提供作戦であることを示唆している。キャンペーンインフラは非常に分散されているが、DNS 管理は数多くのサービスに統合されており、ほとんどがアメリカに位置する IP アドレスを使用している。

[Attack Flow]

1. [Reconnaissance] Gather Victim Information (T1592)
a. 対象電話番号収集
b. 有効な電話番号かどうかの確認
2. [Resource Development] Acquire Infrastructure (T1583)
a. 一回用ドメイン登録
b. 米国拠点のクラウドホスティング使用
3. [Initial Access] Spearphishing Link (T1566.002)
a. スミッシングメッセージ発信
b. Email-to-SMS 機能の活用

4. [Delivery] Phishing Messages (T1204)
    a. SMS を基盤としたソーシャルエンジニアリング手法の使用
    b. 重要サービス詐称
5. [Credential Access] Input Capture (T1056)
    a. ログイン資格情報収集
    b. 機微情報の収集
6. [Command and Control] Web Service (T1102)
    a. 非中央集権化されたドメインの使用
    b. 悪性ドメイン循環適用
7. [Impact] Data Manipulation (T1565)
    a. 緊急性を誘導する虚偽アラートの生成
    b. 実際と類似したフィッシングページの使用

9) SectorJ232 used GitHub tools to deploy AsyncRat (2025-10-28)

https://cti.nshc.net/events/view/19780

攻撃対象産業群: 政府・行政、IT

攻撃者は GitHub プラットフォームの開放性を悪用し、政府および企業の開発者を標的とした攻撃活動を行った。このグループは「SearchFilter」という名前のツールに偽装した悪性 GitHub リポジトリを作成し、中国内のセキュリティ研究者および開発者を誘引した。リポジトリに含まれるインストールファイルには、悪性 JavaScript コードが app.asar ファイル内に隠されており、実行過程で "elevate.exe"プロセスを通じて悪性スクリプトがロードされた。彼らの攻撃チェーンは複数段階のペイロードダウンロードを含んでおり、最終的に AsyncRAT トロイの木馬を"RegAsm.exe"プロセスに注入して被害者の資格情報を窃取した。このような攻撃は、GitHub のような開放型開発者プラットフォームを通じて信頼できないコードをダウンロードする際に発生し得るセキュリティリスクを示しており、サプライチェーン侵害（Supply Chain Compromise）に発展する可能性を示唆している。

[Attack Flow]

1. [Initial Access] Drive-by Compromise (T1189)
    a. 信頼できないツールのダウンロード
    b. 悪性 GitHub リポジトリ アクセス
2. [Execution] User Execution (T1204)
    a. ダウンロードされたペイロード実行
    b. マルウェアインストールスクリプトの実行
3. [Persistence] Boot or Logon Autostart Execution (T1547)

a. 環境変数の修正
b. 予約タスクの作成
4. [Defense Evasion] Obfuscated Files or Information (T1027)
a. 暗号化されたペイロード使用
b. 多段階ローディング技法使用
5. [Credential Access] Credential Dumping (T1003)
a. RegAsm.exe で AsyncRat インジェクション
b. 資格証明情報の漏洩
6. [Discovery] System Information Discovery (T1082)
a. システム情報収集
b. サンドボックス回避の有無確認
7. [Command and Control] Encrypted Channel (T1573)
a. C2 サーバーと通信
b. 複数 C2 エンドポイント 使用
8. [Impact] Resource Hijacking (T1496)
a. クリプトマイニング ソフトウェア インストール
b. メモリ上でペイロード実行

10) SectorJ259 used Custom Browser for Unregulated Gambling Operations (2025-10-23)

https://cti.nshc.net/events/view/19591

2025 年 2 月、調査結果により東南アジア、特にカンボジアで犯罪ネットワークによって運営される複雑な不法オンラインギャンブルおよびサイバー詐欺プラットフォームが明らかになった。この作戦には Universe Browser というカスタムブラウザの配布が含まれており、これは検出を回避しサイバー犯罪活動を促進するために複数のプログラムを密かにインストールする。検閲を回避するためのプライバシーに配慮したブラウザとして宣伝されていたが、リモートアクセス型トロイの木馬に似た機能を持ち、継続的なユーザー監視とデータ窃取を可能にすることが明らかになった。この活動は主要な iGaming ソフトウェア供給業者である Baoying Group とその BBIN ブランドに関連しており、悪名高い組織犯罪組織との関連性を示唆し、地下銀行、人身売買および大規模な資金洗浄に関連する広範なネットワークの一部であることが明らかになった。このブラウザはセキュリティ対策を回避するための洗練された回避技術を使用しており、これらの犯罪ネットワークがもたらす脅威が増大していることをさらに浮き彫りにしている。

[Attack Flow]

1. [Initial Access] Drive-by Compromise (T1189)

a. Universe Browser ダウンロード
b. 隠密なプログラムのインストール
2. [Execution] User Execution (T1204)
a. UB-Launcher.exe 実行
b. Chrome バイナリの置き換え
3. [Persistence] Boot or Logon Autostart Execution (T1547)
a. 開始レジストリ値の修正
b. UB-Launcher.exe 持続性確保
4. [Defense Evasion] Obfuscated Files or Information (T1027)
a. 暗号化された SQLITE3 データベース使用
b. アンチデバッグ技法適用
5. [Credential Access] Input Capture (T1056)
a. キーロギング
b. クリップボードモニタリング
6. [Discovery] System Information Discovery (T1082)
a. システム言語および VM 環境の確認
b. ユーザー位置点検
7. [Command and Control] Encrypted Channel (T1573)
a. プロキシ接続の使用
b. C2 サーバーに SSH 接続
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. SOCKS5 基盤データ流出
b. Google Analytics UID 送信

11) SectorJ260 used VBScript Worm and LOLBins for Cryptomining (2025-10-30)
https://cti.nshc.net/events/view/19737

サイバー脅威キャンペーンは、主に無断暗号通貨マイニングのためにシステムを感染させる Visual Basic Script (VBS)ワームを活用した高度な暗号通貨マイニング作戦を含む。2024 年末に初めて観察されたこのキャンペーンは、様々な産業にわたって世界中の組織を対象としており、持続性と防御回避方法を示している。初期アクセスは感染した USB ドライブを通じて行われ、これは wscript.exe を使用して悪性 VBScript ファイルを実行し、接続されると横方向に拡散する。攻撃チェーンは、printui.exe のような生活型バイナリ(LOLBins)を悪用して悪性ライブラリをサイドロードし、セキュリティ回避のための難読化された PowerShell コマンドのような作業を行う。持続性はレジストリ修正、サービス作成、予約タスクを通じて達成され、Malware はシステムファイルに偽装した悪性バイナリのような回避技法を使用する。主要ペイロードは Monero 暗号通貨をマイニング

するためのツールである XMRig であり、攻撃は財政的動機を持っているが、使用されたベクターは潜在的なシステム不安定性と追加の損傷を含むより広範なセキュリティ脅威を提示する。

[Attack Flow]

1. [Initial Access] Replication Through Removable Media (T1091)
   a. 感染した USB 実行
   b. VBScript ドロッパー配布
2. [Execution] Command and Scripting Interpreter (T1059)
   a. wscript.exe を通じた VBScript 実行
   b. cmd.exe でバッチファイル実行
3. [Execution] Windows Command Shell (T1059.003)
   a. バッチファイル実行
   b. コマンドシェル動作の実行
4. [Persistence] DLL Search Order Hijacking (T1574.001)
   a. printui.exe サイドローディング
   b. Malware DLL ローディング
5. [Privilege Escalation] DLL Injection (T1055.001)
   a. Malware DLL インジェクション
   b. 正常バイナリ悪用
6. [Defense Evasion] Masquerading (T1036)
   a. 偽の System32 ディレクトリ使用
   b. 正常バイナリサイドローディング
7. [Defense Evasion] Impair Defenses (T1562)
   a. Windows Defender 例外設定
   b. 難読化された PowerShell コマンドの使用
8. [Persistence] Create or Modify System Process (T1543)
   a. Malware サービスの生成
   b. 予約タスク設定
9. [Impact] Resource Hijacking (T1496)
   a. XMRig 暗号通貨 マイニング
   b. 未承認のリソース使用

12) SectorJ261 used RPX Relay to build IoT proxy network (2025-10-29)

https://cti.nshc.net/events/view/19742

2025 年 5 月 30 日、サイバー脅威行為者が知られているキャンペーンと関連した "w" という ELF ファイルを配布することが確認された。このファイルは特定の IP アドレスを通じて配布され、これは同じキャンペーンによる新しい作戦を示唆している。このキャンペーンは IoT およびエッジデバイスを悪用し、サイバー犯罪活動のための運用中継ボックス(ORB)ネットワークを生成する。このネットワークは住宅用プロキシに類似しており、長期的な隠蔽とトラフィック難読化に重点を置き、洗練された脅威行為者が回避および出所隠しのために好む。2025 年 8 月と 9 月には RPX_SERVER というリバースプロキシゲートウェイが脅威行為者のネットワークと関連があるというキャンペーンのインフラが明確に報告された。このインフラは 25,000 個以上の感染したデバイスと Alibaba および Tencent クラウドにホスティングされた VPS ノードで 140 個の確認されたアクティブな RPX サーバーを含む。この作戦は RPX_Client を使用してデバイスをプロキシプールにオンボーディングし、リモートコマンドおよびプロキシサービスを許可する。この Malware は脆弱性を通じて配布され、複数の地域にわたってその範囲を難読化し拡張するための一貫した設計および運用戦術を反映している。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. CVE-2023-20118 脆弱性 悪用
   b. スクリプト s 配布
2. [Execution] Command and Scripting Interpreter (T1059)
   a. ELF ファイル w 実行
   b. スクリプト q 実行
3. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. rcS 初期化スクリプト修正
   b. 永続性確保のための rpx.sh 配布
4. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
   a. 権限昇格のための脆弱性悪用
   b. 権限が昇格された状態で RPX_Client を実行
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Obfuscated script q 使用
   b. 構成ファイル暗号化
6. [Credential Access] Unsecured Credentials (T1552)
   a. デバイス UUID 収集
   b. ブランド情報抽出
7. [Discovery] System Information Discovery (T1082)
   a. デバイス種別の識別
   b. 地理的分布データ収集

8. [Lateral Movement] Internal Proxy (T1090.001)
   a. デバイスをプロキシプールに登録
   b. リバース接続構築
9. [Command and Control] Application Layer Protocol (T1071)
   a. HTTP を通じたコマンド実行
   b. ポート 55555 で通信
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. デバイスデータ流出
   b. プロキシノード情報送信
11. [Impact] Network Denial of Service (T1498)
   a. 侵害されたデバイスを利用した DDoS の実行
   b. ORB ネットワークを活用した攻撃

13) SectorJ262 used GitHub tools to deploy Malware (2025-10-28)

https://cti.nshc.net/events/view/19849

攻撃者は GitHub プラットフォームの開放性を悪用し、政府および企業開発者の端末を攻撃対象とした。このグループは中国語で書かれた説明とともに IntelliJ IDEA クラックバージョンを偽装した Malware リポジトリを生成し、開発者を誘引した。リポジトリには install-current-user.vbs スクリプトが含まれており、これは Malware JAR ファイルを実行してリモートから追加ペイロードをダウンロードし、メモリで復号化および実行するよう設計されていた。その後の段階で "WptsExtensions.dll"が使用され、システムサービス(msdtc など)を乗っ取る形のローダー機能を果たし、"oci.dll"を通じて"o.dat"ファイルをダウンロードし、マイニング用ペイロードを積載した。環境変数の修正に失敗した場合には、MSI インストーラーを通じて計画されたタスク(Scheduled Task)を生成し、Malware DLL を注入する方式を使用した。攻撃インフラは複数のコマンドおよびコントロールサーバーとの通信チャネルを維持し、被害システムで暗号通貨マイニングを継続的に実行した。これらの攻撃は開放型プラットフォームを通じたサプライチェーン侵害(Supply Chain Compromise)のリスクを想起させ、検証されていない開発者リソースを使用する行為が深刻なセキュリティ脅威につながる可能性があることを示している。

[Attack Flow]

1. [Reconnaissance] Gather Victim Information (T1592)
   a. セキュリティ研究者対象識別
   b. 中国所在の開発者対象識別
2. [Resource Development] Develop Capabilities (T1587)
   a. 偽装の GitHub リポジトリ生成

b. マルウェアツールおよびスクリプトの開発

3. [Initial Access] Drive-by Compromise (T1189)
   a. GitHub を通じたダウンロード誘導
   b. クラックソフトウェアパッケージ活用
4. [Execution] User Execution (T1204)
   a. 「SearchFilter」マルウェアツールの実行
   b. マルウェアインストールスクリプトの実行
5. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. RegAsm.exe で AsyncRat インジェクション
   b. システムサービスハイジャック
6. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. app.asar 内部に JavaScript を隠す
   b. ペイロードをメモリ上で復号化
7. [Credential Access] Credential Dumping (T1003)
   a. AsyncRat を利用した資格証明の流出
8. [Discovery] System Information Discovery (T1082)
   a. システム情報収集
9. [Command and Control] Application Layer Protocol (T1071)
   a. C2 サーバーと通信
10. [Impact] Resource Hijacking (T1496)
    a. クリプトマイニング用 DLL 配布

14) SectorJ263 used ISO Files to Distribute Grandoreiro Banking Trojan (2025-11-11)

https://cti.nshc.net/events/view/20144

攻撃対象産業群: 銀行

2025 年 11 月、一連のサイバー事件がメキシコ、ブラジル、スペイン、コロンビア、コスタリカの機関を主に狙う Grandoreiro バンキングトロイの木馬を配布する脅威行為者と関連付けられた。このトロイの木馬は複雑なサービス型 Malware(MaaS)で、文字列復号化、ドメイン生成アルゴリズム(DGA)、被害者デバイスの Microsoft Outlook クライアントを悪用して追加のフィッシングメールを拡散する能力などの技法を含む。これは様々なバンキングアプリケーションをターゲットにして資格情報の窃取と詐欺行為を可能にする。脅威行為者は光学ディスクイメージ(ISO)ファイルを使用してトロイの木馬を配信することが観察されており、フィッシングメールにはしばしば含まれたリンクやリンクがある PDF が含まれている。これはメールベースの攻撃ベクターを戦略的に使用して Malware を効果的に配布するグループの戦略を反映している。

[Attack Flow]

1. [Initial Access] Spearphishing Link (T1566.002)
   a. リンクが含まれたメール
   b. Malware リンクが含まれた PDF
2. [Execution] User Execution (T1204)
   a. ISO ファイルの配布
3. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. 文字列復号化
4. [Command and Control] Domain Generation Algorithms (T1483)
   a. C2 通信のための DGA の使用
5. [Credential Access] Input Capture (T1056)
   a. 金融資格証明書の窃取
6. [Collection] Data from Information Repositories (T1213)
   a. Microsoft Outlook 悪用
7. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 資格情報漏洩
8. [Impact] Data Manipulation (T1565)
   a. 金融詐欺行為の支援

15) SectorJ263 used Grandoreiro Malware disguised as Official Emails (2025-11-13)

https://cti.nshc.net/events/view/20148

攻撃対象産業群: 銀行

2025 年 3 月末、南米のあるグループがメキシコとコスタリカで金融脱取作戦を実行したサイバー犯罪事件が発生する。2025 年 2 月 19 日から 3 月 20 日の間にフィッシングキャンペーンがこれらの地域を対象にして Grandoreiro バンキングトロイの木馬を配信する。被害者はフィッシングメールを受け取り、contaboserver[.]net URL から悪性 Visual Basic Script (VBS)を含む ZIP アーカイブをダウンロードするよう誘導される。特に地理的な位置がメキシコやコスタリカの場合はさらにそうである。VBS は実行され、ペイロードをリネームし、これは分析防止チェックを行い、システムデータを収集してコマンド＆コントロール (C2) サーバーに送信する。この作戦はフィルタリングを回避するために DNS over HTTPS を使用することを強調する。Grandoreiro トロイの木馬はサービス型マルウェア (Malware-as-a-Service) として世界中の 1,500 以上のバンキングアプリケーションを対象にし、その構成要素を利用して詐欺を行う。キャンペーンは政府機関を装い、税金や請求書といったテーマを利用する。この活動は少なくとも 2017 年から様々な地理的地域で被害者の資格情報を盗み、詐欺を行い、かなりの金融的影響を与えていると見られる。

[Attack Flow]

1. [Reconnaissance] Phishing for Information (T1598)
   a. 政府機関を装ったフィッシング試み
   b. 税金および請求書をテーマにしたフィッシングメール
2. [Resource Development] Compromise Infrastructure (T1583)
   a. mediafire[.]com を活用したホスティング
   b. contaboserver[.]net を通じたペイロード配信
3. [Initial Access] Spearphishing Link (T1566.002)
   a. Malware メールリンク
   b. ZIP アーカイブダウンロード
4. [Execution] User Execution (T1204)
   a. Malware VBS 実行
   b. 任意の名前のペイロード実行
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. VBS スクリプト難読化
   b. ペイロード Base64 デコード
6. [Defense Evasion] Masquerading (T1036)
   a. 偽の PDF ダイアログボックス表示
   b. 偽の Adobe Reader エラーメッセージの使用
7. [Discovery] System Information Discovery (T1082)
   a. システム情報収集
   b. 公開 IP および 位置情報 収集
8. [Command and Control] Encrypted Channel (T1573)
   a. DNS over HTTPS 基盤 C2 通信
   b. C2 ドメイン文字列復号化
9. [Collection] Input Capture (T1056)
   a. 資格証明書収集
   b. 特定金融アプリケーション対象
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. 収集されたシステムデータを C2 に送信
    b. 追加ペイロードダウンロード

16) SectorJ264 used Cephalus Ransomware via RDP Account Hijacking (2025-11-05)

https://cti.nshc.net/events/view/20140

2025 年 11 月、Cephalus という新しいランサムウェアグループが登場し、彼らは金銭的利益を目的として活動していると推定される。彼らは主に多要素認証がない脆弱な RDP アカウントを通じてシステムに侵入し、特定の組織を対象にデータ流出と暗号化を行う。Cephalus という名前は、攻撃成功に対する自信を反映し、無誤の槍を持つ神話上の人物に由来している。このランサムウェアは Go 言語で書かれており、分析を妨害するために偽の AES キー生成といった難読化技法を使用し、AES-CTR 暗号化と RSA を用いて復号キーを保護する。特に、Cephalus は Windows Defender を無効化し、VSS バックアップを削除し、必要なサービスを停止させて暗号化成功率を高める。このランサムウェアは SecurityMemory 構造を使用してメモリページングと XOR 技法を通じて AES キーの露出を最小化する。暗号化が完了すると、'recover.txt'という名前の身代金要求メモを表示する。強力な戦術にもかかわらず、このグループが他のランサムウェアグループとの関連性やブランド変更の履歴があるかどうかは不明である。

[Attack Flow]

1. [Initial Access] Valid Accounts (T1078)
   a. 盗まれた RDP アカウントの使用
   b. 多要素認証未使用
2. [Execution] Command and Scripting Interpreter (T1059)
   a. Go 言語ベースのランサムウェア実行
   b. 偽の AES キー生成
3. [Defense Evasion] Impair Defenses (T1562)
   a. Windows Defender 無効化
   b. 偽のキー生成による分析回避
4. [Credential Access] OS Credential Dumping (T1003)
   a. SecureMemory 構造 使用
   b. XOR 基盤キー保存
5. [Discovery] System Information Discovery (T1082)
   a. 主要サービス識別
   b. VSS バックアップ 対象 指定
6. [Impact] Data Encrypted for Impact (T1486)
   a. AES-CTR 方式 暗号化
   b. RSA キー保護適用
7. [Impact] Inhibit System Recovery (T1490)
   a. VSS バックアップ 削除
   b. Veeam および MSSQL サービス停止
8. [Exfiltration] Exfiltration Over Alternative Protocol (T1048)
   a. GoFile ストレージ リンク 使用

b. データ流出の痕跡を残す

9. [Impact] Data Manipulation (T1565)
   a. ランサムノート生成
   b. 過去の被害事例に基づく圧力

17) SectorJ265 used Yurei Ransomware for Double Extortion Attacks (2025-11-11)

https://cti.nshc.net/events/view/20115

攻撃対象産業群: IT、物流、マーケティング、食品

2025 年 11 月、Yurei という新しいランサムウェアグループが公開的に確認された。Yurei は典型的なランサムウェアモデルを通じて企業ネットワークに侵入し、データを暗号化しバックアップを削除し、奪取した情報に基づいて身代金を要求する。このグループは専用ダークウェブサイトを通じて運営され、スリランカやナイジェリアのような国と、運送、IT、マーケティング、食品サービスのような産業を対象としている。身代金の金額は各被害者の財政状態に合わせて調整されるが、具体的な金額は公開されていない。Yurei ランサムウェアは Go 言語で作成されており、32 バイトキーと 24 バイトノンスを使用する ChaCha20-Poly1305 アルゴリズムを活用する。これらのキーとノンスは secp256k1-ECIES 方法で暗号化され、暗号化されたファイル内に保存される。ランサムウェアはシステム障害を防ぎ、身代金交渉を保証するために特定のディレクトリ、ファイル拡張子およびファイル名を回避する。ランサムウェアノートは要求が満たされない場合、データの露出および削除を脅かし、特に第三者の復旧サービスを警告する。この脅威はデータベースおよび個人または金融文書のような重要なデータの流出に拡大する。

[Attack Flow]

1. [Initial Access] Valid Accounts (T1078)
   a. 企業ネットワーク侵入
   b. 不正アクセスの実行
2. [Discovery] System Information Discovery (T1082)
   a. ドライブ情報収集
   b. 対象識別
3. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. secp256k1-ECIES 暗号化 使用
   b. 無作為キーおよびノンス生成
4. [Impact] Data Encrypted for Impact (T1486)
   a. ChaCha20-Poly1305 暗号化 適用
   b. ファイル暗号化実行
5. [Impact] Inhibit System Recovery (T1490)

a. バックアップ削除
b. ランサムノート配布

6. [Exfiltration] Data Encrypted (T1048)
   a. データ脱取
   b. データ公開の脅威
7. [Command and Control] Non-Standard Port (T1571)
   a. ダークウェブを基盤とした通信
   b. ランサム要求交渉

今月のサイバー脅威の特徴

今月報告されたサイバー脅威事件は、現代のサイバー攻撃の精巧さと多様性を強調する様々な技術的および戦術的特徴を示している。これらの事件で共通して見られるテーマは、スピアフィッシングを主要な攻撃ベクターとして使用することであり、しばしば政府、国防、重要インフラなどの特定のセクターを対象としている。フィッシングメールにはしばしば悪性添付ファイルやリンクが含まれており、被害者のシステムでMalwareが実行されるように誘導する。例えば、複数のキャンペーンでLNKファイルが使用されており、これは実行されるとPowerShellスクリプトや他の形態のコマンド実行をトリガーしてMalwareペイロードを配布する。LNKファイルの使用は、合法的なショートカットに偽装して伝統的なセキュリティ対策を回避できる能力で注目に値する。

これらの攻撃に使用されたMalwareは、バックドア、トロイの木馬、ランサムウェアなど様々な形態で大きく異なる。注目すべき例としては、PlugXやBeaverTailのようなリモートアクセス型トロイの木馬(RAT)の使用があり、これは攻撃者に損傷したシステムへの広範な制御を提供する。これらのRATは、ファイル転送、コマンド実行、データ窃取などの機能を頻繁に備えている。また、CephalusやYureiのようなランサムウェアグループがAES-CTRやChaCha20-Poly1305のような暗号化アルゴリズムを使用して被害者データをロックし、身代金を要求する活動を行っている。これらのランサムウェア変種は、しばしばセキュリティ機能を無効化し、バックアップを削除し、分析を妨害するために難読化技術を使用する。

高度な回避技術はこれらのキャンペーンの特徴であり、攻撃者はDLLサイドローディング、コード難読化、悪意のある目的で合法的なツールを使用する方法を使用する。例えば、DLLサイドローディングは信頼できるアプリケーションのコンテキスト内で悪性コードを実行して検出を回避するために使用される。同様に、mshta.exeやPowerShellのような生活基盤バイナリ(LOLBins)を使用すると、警告なしにスクリプトやコマンドを実行できる。Cobalt StrikeやMeterpreterのような二重使用ツールの統合は、悪意のある目的で合法的なソフトウェアを活用する傾向をさらによく示している。

もう一つの注目すべき特徴は、しばしば暗号化された通信とペイロードホスティングおよびデータ窃取のための合法的なクラウドサービスを含む精巧なコマンド＆コントロール(C2)インフラの使用である。攻撃者はしばしばBase64エンコーディング、HTTPS、カスタム暗号化アルゴリズムのような技術を使用して通信を保護し、検出を回避する。GitHubやその他のコードリポジトリを一時的なペイロードホスティングに使用することも観察されており、攻撃者がダウンロード後に悪性ファイルを迅速に削除して検出を回避できるようにしている。
これらのキャンペーンはまた、高い適応性と持続性を示しており、脅威行為者はセキュリティ対策に対応して戦術、技術および手順(TTP)を頻繁に更新する。ここには、Microsoft SharePointおよびWindows Server Update Services (WSUS)に影響を与える新たに公開された脆弱性を迅速に採用して不正アクセスを得てMalwareを配布することが含まれる。CVE-2025-61932およびCVE-2025-53770のようなゼロデイ脆弱性の使用は、パッチが適用されていないシステムを識別し悪用する攻撃者の能力を強調する。
感染経路の観点からは、社会工学戦術の使用が際立っており、攻撃者はしばしば合法的な機関を装ったり、対象の聴衆に関連するテーマを使用して成功する侵害の可能性を高める。ここには、偽の求人提案、餌文書、資格情報を収集したりMalwareを配信するために設計された誘引ウェブサイトの使用が含まれる。社会工学戦術を

今月のサイバー脅威の示唆点

今回の月に確認された脅威動向は、多様な侵入手法と複合的な攻撃フローが継続的に活用されていることを示している。特にスピアフィッシング基盤のアプローチ、社会工学手法の精巧化、脆弱性悪用を通じた初期侵入などが同時に観察され、全体的な脅威環境が技術的・戦術的に拡大していることを示している。このような流れは、攻撃者が目標環境に合わせて侵入経路を多様化し、検知回避と権限確保のために高度化された手続きを継続的に適用していることを示唆している。BeaverTail、Comebacker および様々な Remote Access Trojan (RAT)のような精巧な Malware の使用は、資格情報の窃取、機密データの流出、対象ネットワーク内の持続的なアクセスを目指す多段階攻撃の傾向を示している。GitHub および LinkedIn のような一見合法的なプラットフォームを通じた Malware 配布と Microsoft SharePoint および ActiveMQ のような広く使用されるソフトウェアの脆弱性悪用は、攻撃者が正常なネットワークトラフィックに紛れて検知を回避できる能力を強調している。

組織はこれらの脅威がセキュリティ態勢に与える影響を認識する必要がある。Velociraptor および Cobalt Strike のような二重用途ツールを悪意のある目的で使用することは、これらのツールの合法的使用と悪意のある使用を区別できる強力なモニタリングおよび検知機能の必要性を示している。

GitHub のような合法的なサービスを悪意のあるペイロードホスティングに使用し、クラウドサービスをコマンドおよびコントロール作業に悪用する傾向は、クラウドセキュリティ戦略の再評価を必要とする。また、DLL サイドローディング、難読化および暗号化のような高度な回避技術の使用は、組織がこれらの戦術を識別し対応できるより精巧な検知メカニズムを採用する必要があることを要求している。

戦略的観点から、組織は脅威インテリジェンス、インシデント対応および継続的なモニタリングを含む包括的なセキュリティフレームワークの実装を優先すべきである。脅威インテリジェンスは、組織が潜在的攻撃に対して先制的に防御できるよう、新興脅威および攻撃パターンに関する貴重な洞察を提供できる。インシデント対応計画は、組織が事件に迅速かつ効果的に対応できるよう、定期的に更新およびテストされるべきである。ネットワークトラフィックおよびシステム活動の継続的なモニタリングは、異常現象および潜在的侵害指標を検知するために不可欠である。

組織はまた、フィッシングおよび社会工学戦術に対する認識を高めるために、従業員教育プログラムを強化することを考慮すべきである。従業員はしばしばこれらの攻撃に対する最初の防衛線であり、彼らに疑わしい活動を認識し報告する方法を教育することは、成功する攻撃のリスクを大幅に減少させることができる。また、多要素認証（MFA）および最小権限アクセス制御を実装することは、ネットワーク内の無断アクセスおよび横方向移動のリスクを緩和できる。

要約はまた、脆弱性管理およびパッチの重要性を強調している。ゼロデイ脆弱性および既知のソフトウェア欠陥の悪用は、組織が資産の最新リストを維持し、セキュリティパッチを迅速に適用する必要性を強調している。定期的な脆弱性評価および侵入テストは、攻撃者が悪用する前に潜在的な弱点を識別し修正するのに役立つことができる。

結論として、今回の月に観察された多様なサイバー脅威は、組織が技術、プロセスおよび人を組み合わせた多層セキュリティアプローチを採用する必要性を強調している。最新の脅威動向に関する情報を維持

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)

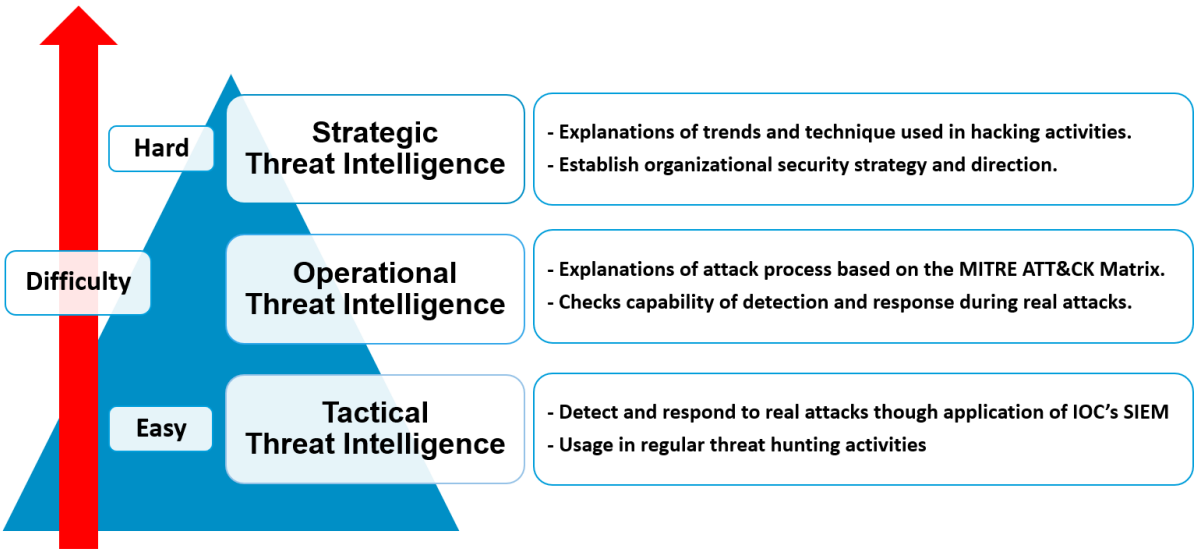
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

- 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

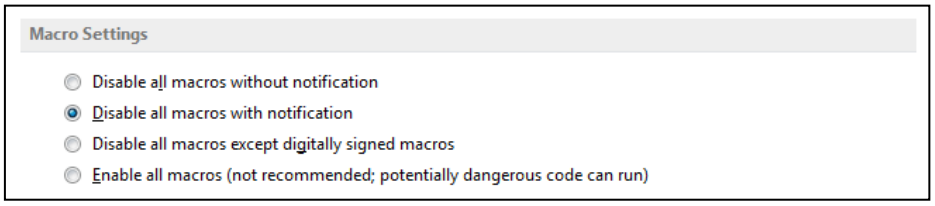
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

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.