NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI2025061902

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

May 2025

NSHC PTE. LTD.

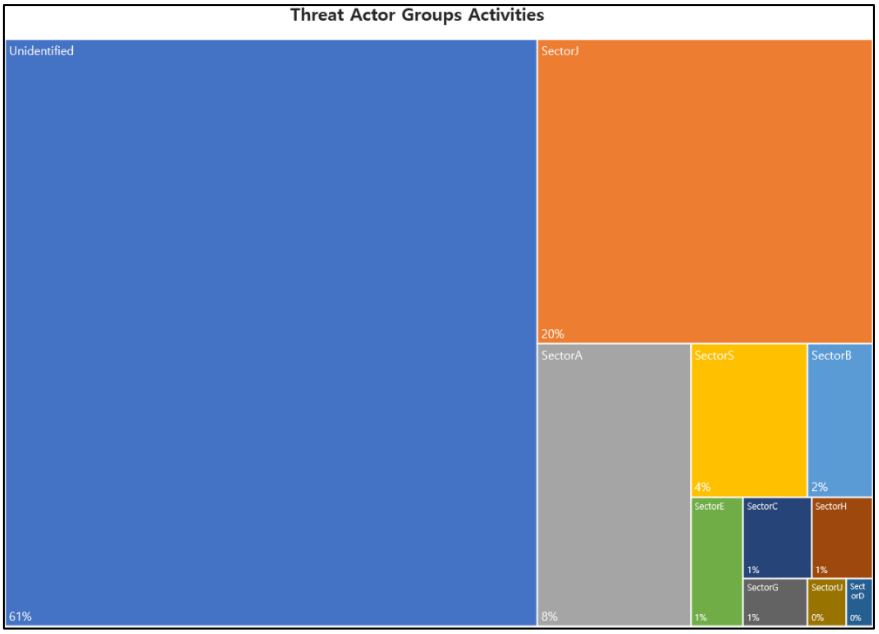
このレポートは 2025 年 4 月 21 日から 2025 年 5 月 20 日まで見つけた政府支援のハッキンググループ活動と関係あるイッシューを説明し、それに伴う侵害事故の情報と ThreatRecon Platform 内のイベント情報を含む。

Table of Contents

- 無断転載禁止(Do not share) ー この著作物の内容は特定の顧客へご提供しております。当コンテンツの内容、画像などの無断転載・無断使用を固く禁じます。
- 秘密保持契約(Non-disclosure agreement) ー この著作物は NDA(秘密保持契約）の同意の上、ご提供しております。これに違反した場合は、法的措置になる恐れがございます。
- 注意 ー このライセンスの許容範囲を含んだその他の著作権関係の事項はサービス担当者を通した上、必ず確認を行った上でご利用ください。

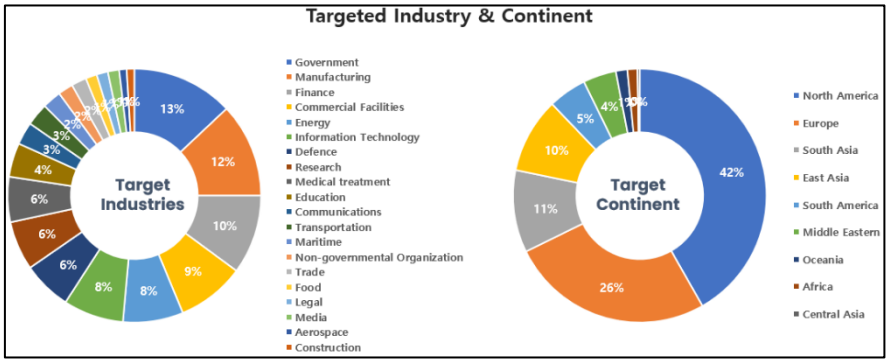
エグゼクティブサマリー

2025 年 4 月 21 日から 2025 年 5 月 20 日までの間に NSHC 脅威分析研究所（Threat Research Lab）が収集したデータと情報に基づいて分析したハッキンググループ（Threat Actor Group）の活動を要約した内容です。
今月 5 月には、合計 74 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 60%で最も多く、SectorJ、SectorA グループの活動がそれに続きました。



[Figure 1: 2025 年 5 月に確認されたハッキンググループ別活動統計]

今年 5 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、製造業および金融分野に従事する関係者またはシステムを対象に最も多くの攻撃を行い、地域別では北アメリカとヨーロッパに位置する国々を対象としたハッキング活動が最も多いことが確認されています。



[Figure 2: 2025 年 5 月に攻撃対象となった産業分野と国の統計]

NSHC©2025 All rights reserved.

2025 年 5 月の 1 ヶ月間、APT およびサイバー犯罪グループは、さまざまな産業分野と地域を対象に精巧な侵入作戦を展開しました。彼らはフィッシング、脆弱性の悪用、サプライチェーンへの侵入、情報の窃取、ランサムウェアの配布など、複合的な手法を駆使し、高度な検知回避技術とオープンソースインフラの悪用が多く観察されました。

SectorA グループは、macOS および Windows ベースのシステムを対象に、Bash スクリプト、Windows ショートカット（LNK）ファイル、PowerShell スクリプトなどの多様な手法を用いた精巧な攻撃を行いました。特に暗号通貨産業を中心に、LinkedIn および GitHub を悪用した採用詐称、偽のインタビューサイトの運営、そしてカスタマイズされた Malware（BeaverTail、InvisibleFerret など）の配布が特徴的でした。また、RoKRAT 系 Malware を通じたファイルレス侵入およびクラウドベースの C2 通信が組み合わさった攻撃も観察されました。彼らはマルチプラットフォームを同時にターゲットにし、認証情報の窃取、システム偵察、バックドアのインストールを行いました。

SectorB グループは、東南アジアおよびヨーロッパを中心に政府および通信産業をターゲットにした侵入作戦を展開しました。DLL サイドローディングを利用した Cobalt Strike、ScreenConnect ベースのリモートコントロール、DslogdRAT を活用した監視型ペイロードなどが代表的であり、SLAAC スプーフィング、API フック、タイムスタンプ操作などの高度な防御回避技術が組み合わされ、長期的な侵入を試みました。彼らはソーシャルエンジニアリングとマルウェアスクリプトを通じて初期アクセスを確保し、その後、暗号化されたチャネルを通じてシステム制御および情報漏洩を行いました。

SectorC グループは主にウクライナおよび東ヨーロッパ諸国の軍事機関および政府機関を対象にサイバー諜報活動を展開しました。ウェブメールソフトウェア（Roundcube、MDaemon など）のゼロデイおよび XSS 脆弱性を悪用して悪性 JavaScript を挿入し、ユーザーのメールアカウントの資格情報およびメール内容を収集しました。特に、SpyPress シリーズと名付けられたカスタムペイロードがプラットフォームごとに設計されて配布され、暗号化された HTTP POST リクエストを通じて C2 チャネルにデータを送信する精密な構造が特徴です。

SectorD グループは、偽の学術機関および技術企業を装った攻撃インフラを長期間準備し、SSH キーの再利用やサーバー証明書の再利用などを通じて、密かに標的システムにアクセスしました。彼らは、社会運動団体や非政府組織（NGO）を含むさまざまな産業を対象に、情報窃取型バックドアを配布し、誘引サーバーのウェブコンテンツと事前に準備されたペイロードを通じて偵察と持続的感染を試みました。

SectorE グループは、ウクライナおよびヨーロッパ圏の NGO や行政機関を対象に、Word 文書を利用したフィッシングキャンペーンを展開しました。彼らは CVE-2023-21716 の脆弱性を利用して RTF 文書にマルウェアを挿入し、これを通じてクリップボードデータ、ブラウザの資格情報、システム情報を収集しました。収集されたデータは HTTP POST リクエストを通じて C2 に送信され、固定された外部ドメインとの通信に基づく短期侵入の形態でした。

NSHC©2025 All rights reserved.

SectorH グループは、エネルギーおよび鉄道インフラを主要な標的として多段階 RAT 攻撃を実行しました。MSI ベースのペイロードを通じて感染を誘導し、その後、SparkRAT や CurlBack などのオープンソース RAT ツールを活用して、コマンド実行、スクリーンショットのキャプチャ、ブラウザクッキーの窃取など、全方位的な情報を収集しました。また、UACMe を利用した権限昇格や定期的なコマンド実行（タスクスケジューラ）の設定を通じて、検出回避と持続性を確保しました。
SectorL グループは、DLL サイドローディング技法を通じて Firefox 実行時に「mozglue.dll」に偽装したマルウェアを注入し、キーロギング、ブラウザパスワードの窃取、FTP アップロードなどを行いました。彼らはデジタル署名されたインストールファイルを利用して感染を誘導し、バックドア機能を通じて持続的なコマンド実行と情報漏洩を行いました。このグループの活動は、ソーシャルエンジニアリングと既存のオープンソースツールを組み合わせた低コスト・高効率の戦略として分析されています。
SectorP グループはルーマニアを拠点とするインフラを活用し、ウェブサイトを装ったフィッシングおよび C2 通信を行いました。彼らは独立系ジャーナリストを装い、悪性 LNK ファイルと PowerShell スクリプトを配布し、PE ファイルをダウンロードして実行し、システム情報を窃取しました。「AppService.log」などのファイル名でデータを隠蔽し、収集された情報は非公式サーバーに送信されました。活動は限定的ですが、身元を偽装する戦略が明確でした。
SectorS グループは、暗号通貨取引所および分散型金融サービスを標的とした攻撃を実行しました。偽のウォレットアプリケーションまたは取引所サイトを通じて APK マルウェアアプリを配布し、感染した Android デバイスからログイン情報、OTP、メッセージ、およびキーストア情報を収集しました。また、iOS ユーザーを対象としたスミッシングも並行して行われ、これによりユーザーの個人ウォレットへのアクセス権を確保し、暗号通貨を盗みました。盗まれた情報は、Telegram C2 チャンネルを通じてリアルタイムで送信されました。
SectorJ グループは収益化戦略を中心に活動を展開し、さまざまなランサムウェア（RALord、Qilin、Interlock など）および情報窃取型のマルウェアを配布しました。彼らはフィッシングメール、悪意のある GitHub リポジトリ、MSI インストールファイル、サプライチェーン侵入などを利用して初期アクセスを確保し、その後ファイルの暗号化、バックアップの削除、データ流出の脅迫サイトの掲載などの戦術を実行しました。また、Amethyst Stealer、TerraStealer、Tycoon 2FA フィッシングキットを通じて資格情報や 2FA セッションを窃取し、Telegram を通じた MaaS の運用および攻撃インフラの配布も観察されました。

詳細情報

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

NSHC©2025 All rights reserved.

1) SectorA01 used Bash Script Malware disguised as macOS Driver Update (2025-05-05)

https://cti.nshc.net/events/view/14947

2025 年 4 月、SectorA01 ハッキンググループは、macOS の正規のドライバーアップデートに偽装したマルウェアキャンペーンを展開しました。このグループは「driverupdate」という名前のファイルを通じてユーザーを欺き、該当マルウェアはセキュリティソリューションの検出を回避するために高度な偽装技術を適用しました。攻撃は「realtekmac.sh」という Bash スクリプトを利用してユーザーに直接実行させるよう誘導し、このスクリプトはシステムアーキテクチャを識別した後、対象環境に適したカスタムアーカイブをダウンロードし、「LaunchAgents」を通じて持続性を確保する方式で動作します。その後に実行される「DriverMinUpdate.app」は正常なアプリケーションのように偽装され、ユーザーの資格情報を収集し、収集された情報は Dropbox ベースのストレージに送信されます。続いて動作する第 2 段階ローダー「cloud.sh」は、Go 言語で書かれた情報窃取ツール「driverupdate.go」を活性化し、アメリカにホスティングされたコマンド＆コントロール（Command and Control）サーバーと暗号化されたチャネルを構築します。このツールはシステム情報とユーザー資格情報を収集し、リモートコマンド実行機能も含んでいると分析されています。

[Attack Flow]

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
   a. ユーザーを騙して「realtekmac.sh」を実行
   b. 正規のドライバーアップデートに偽装
2. [実行] コマンドとスクリプトインタープリタ: Bash (T1059.004)
   a. システムアーキテクチャの確認
   b. カスタムアーカイブのダウンロード
3. [持続性] Plist の変更 (T1547.012)
   a. LaunchAgents に plist ファイルを作成
   b. システム起動時に自動実行を設定
4. [資格情報アクセス] 入力キャプチャ (T1056)
   a. 「DriverMinUpdate.app」で資格情報をフィッシング
   b. 盗まれた資格情報を Dropbox に送信
5. [コマンドとコントロール] 暗号化されたチャネル (T1573)
   a. 「driverupdate.go」で C2 チャネルを設定
   b. RC4 暗号化で通信を保護
6. [収集] ローカルシステムからのデータ (T1005)
   a. システムデータの収集
   b. 資格情報とブラウザクッキーの窃取

NSHC©2025 All rights reserved.

7. [流出] C2 チャネルを介した流出 (T1041)
   a. 盗まれたデータを C2 サーバーに送信
   b. リモートコマンドの実行をサポート

2) SectorA01 used BeaverTail and InvisibleFerret in crypto job scams (2025-04-24)

https://cti.nshc.net/events/view/14686

攻撃対象産業群: 技術

SectorA01 グループは、暗号通貨業界を標的としたサイバー脅威キャンペーンを通じて Malware を配布しました。彼らは架空の会社である「BlockNovas LLC」、「Angeloper Agency」、「SoftGlide LLC」を通じて暗号通貨の採用応募者を狙いました。ハッキンググループは「BeaverTail」、「InvisibleFerret」、「OtterCookie」という Malware を「インタビュールア」として使用し、被害者のシステムに侵入しました。AI 生成のプロフィールを LinkedIn、GitHub、求人サイトに投稿してユーザーを欺き、汚染された GitHub リポジトリ、サーバー構成エラー、フィッシングウェブサイトを利用してペイロードを配信しました。この Malware は、資格情報や暗号通貨ウォレット情報を含む機密データを盗み、ブラウザハイジャックコンポーネントや FTP サーバーデータの窃盗を通じて送信します。主要なデスクトップオペレーティングシステムを対象としており、携帯型ネットワーキングツールで隠蔽して検出を回避しました。攻撃インフラは「lianxinxiao[.]com」と「attisscmo[.]com」ドメインと接続され、クラウドサービスを利用してデータを盗みました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 偽の採用インタビューの餌
   b. フィッシングウェブサイトの使用
2. [実行] ユーザー実行 (T1204)
   a. マルウェアの GitHub リポジトリ実行
   b. 汚染されたファイルのダウンロード
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. Windows レジストリキーの追加
   b. Linux 自動開始ファイルの作成
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. コードの難読化
   b. AI 生成プロファイルの使用
5. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. 暗号通貨ウォレット拡張機能からの資格情報収集

NSHC©2025 All rights reserved.

b. FTP サーバーへのデータ転送
6. [発見] システム情報の発見 (T1082)
a. システム OS およびバージョン情報の収集
b. ユーザーIP アドレスの確認
7. [収集] 情報リポジトリからのデータ (T1213)
a. 暗号通貨ウォレット情報の収集
b. ブラウザに保存された資格情報の収集
8. [コマンド＆コントロール] ツール転送の侵入 (T1105)
a. C2 サーバーへのデータ転送
b. FTP を通じたペイロード転送
9. [流出] ウェブサービスを介した流出 (T1567)
a. クラウドサービスの使用
b. FTP サーバーを通じたデータの盗難

3) SectorA01 used Beavertail Malware disguised as Job Interview Tasks (2025-04-23)

https://cti.nshc.net/events/view/14667

SectorA01 グループは、偽の会社の採用インタビューを装って LinkedIn や Upwork などのプラットフォームを通じて応募者を誘引します。応募者は、暗号通貨、Web3、ブロックチェーン技術に関連する職務を餌にして、マルウェアをダウンロードして実行するように誘導され、この過程で該当グループは攻撃対象システムへのアクセス権を得ます。技術的には、ロシアの IP アドレス範囲を使用し、VPN、プロキシ、RDP セッションを通じた複雑な匿名化ネットワークを利用して活動を調整しています。また、信頼できるコードリポジトリと採用プラットフォームを利用したソーシャルエンジニアリング技法を活用し、攻撃対象の機密データを窃取することが主な目的であると分析されています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
a. LinkedIn と Upwork を通じた偽の求人広告
b. 偽の会社ウェブサイトへの誘導
2. [実行] ユーザー実行 (T1204)
a. 技術課題の解決を装った Malware 実行
b. "easydriver.cloud"から Malware ダウンロード
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
a. システム再起動時の自動実行設定

NSHC©2025 All rights reserved.

b. システムログオン時に Malware 実行
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. コード難読化技術の使用
b. 正当なコードリポジトリを通じた信頼性構築
5. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
a. "Beavertail" C&C サーバーとの通信
b. ロシア IP を通じた C2 接続
6. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. 機密データを C2 チャネルを通じて外部に送信
b. 暗号通貨関連情報の窃取
7. [影響] データ操作 (T1565)
a. 暗号通貨の窃取および操作
b. 攻撃対象産業のデータ損傷および操作

4) SectorA01 used Exploited Innorix Agent Vulnerability in S.Korea (2025-04-24)

https://cti.nshc.net/events/view/14641

攻撃対象産業群: 金融、IT、通信、半導体

SectorA01 グループは昨年 11 月から、韓国のソフトウェア、IT、金融、半導体製造および通信産業に属する少なくとも 6 つの組織を攻撃しました。彼らはウォータリングホール攻撃とソフトウェアの脆弱性の組み合わせを使用して、攻撃対象のシステムに侵入しました。このグループは「Cross EX」や「Innorix Agent」といった韓国で開発されたソフトウェアの脆弱性を悪用し、内部ホストに追加の Malware をインストールすることができました。この攻撃チェーンは「ThreatNeedle」、「Agamemnon ダウンローダー」、「wAgent」、「SIGNBT」、「COPPERHEDGE」といった Malware の実行を含んでおり、プロセスインジェクション、ラテラルムーブメント、モジュール化といった機能を示しています。彼らは韓国で開発されたソフトウェアを悪用して追加の Malware をインストールする戦略を使用しました。また、このキャンペーンでは、攻撃対象のシステムが初期感染する間に韓国のオンラインメディアサイトを通じて開始し、合法的なウェブサイトをコマンド＆コントロールサーバーとして使用しました。

[Attack Flow]

1. [初期アクセス] ドライブバイ妥協 (T1189)
a. 韓国のオンラインメディアサイトを通じた初期感染
b. 悪性スクリプト実行を通じた脆弱性悪用
2. [実行] コマンドとスクリプトインタープリタ (T1059)
a. "ThreatNeedle"を通じたマルウェア実行

NSHC©2025 All rights reserved.

b. "Agamemnon ダウンロード"で追加ペイロード実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
a. "ThreatNeedle"の持続性のためのサービス登録
b. "wAgent"の持続性維持
4. [権限昇格] プロセスインジェクション (T1055)
a. "SyncHost.exe"でプロセス注入
b. "SIGNBT"を通じた権限昇格
5. [防御回避] ファイルまたは情報のデオブスクエート/デコード (T1140)
a. "wAgent"の AES-128-CBC アルゴリズムを通じた復号化
b. "COPPERHEDGE"のパラメータ難読化
6. [資格情報アクセス] ファイル内の資格情報 (T1081)
a. "SIGNBT"を通じた資格情報ダンプ
b. "COPPERHEDGE"を通じた内部ネットワーク探索
7. [発見] システム情報発見 (T1082)
a. システム情報収集
b. ネットワーク接続情報収集
8. [横移動] リモートサービス (T1021)
a. "Innorix Agent"の脆弱性悪用
b. "ThreatNeedle"を通じた追加マルウェアインストール
9. [収集] ローカルシステムからのデータ (T1005)
a. システムログ収集
b. ネットワークトラフィック収集
10. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
a. C2 サーバーとの HTTP 通信
b. JSON 形式のデータ送信
11. [データ流出] C2 チャネルを通じたデータ流出 (T1041)
a. 暗号化されたデータ送信
b. C2 との通信を通じたデータ流出

5) SectorA01 used OtterCookie Malware in Contagious Interview Campaign (2025-05-08)

https://cti.nshc.net/events/view/15244

攻撃対象産業群: 金融

SectorA01 グループは、2024 年 9 月から「OtterCookie」というマルウェアを金融機関、暗号通貨オペレーター、フィンテック企業を対象に活発に配布していると分析されています。このグループは

NSHC©2025 All rights reserved.

2023 年から様々なマルウェアを利用したキャンペーンを展開しており、最近では「OtterCookie」の機能を継続的に強化しています。「OtterCookie」はバージョン v1 から v4 までアップデートされており、各バージョンは様々なモジュールを通じて複数の作業を行います。2025 年 2 月に確認された「OtterCookie v3」は、レガシー機能を含むメインモジュールと、非 Windows 環境で収集した文書や暗号通貨関連ファイルをハードコーディングされたコマンドを通じて C2 サーバーに送信するアップロードモジュールで構成されています。2025 年 4 月から観察された「OtterCookie v4」は、2 つの新しい情報窃取モジュールと拡張されたメインモジュールを含んでおり、仮想環境検出機能を追加してサンドボックス環境と実際の感染を区別しようとしています。Chrome のログインデータ処理方式の違いは、これらのモジュールが異なる開発者によって開発されたことを示唆しています。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. マルウェアファイルが添付されたメールの送信
   b. メール受信者にクリックを誘導
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
   a. ハードコーディングされたコマンドの実行
   b. リモートサーバーとの通信開始
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. システム起動時に自動実行設定
   b. 持続的な感染の維持
4. [防御回避] 仮想化/サンドボックス回避 (T1497)
   a. 仮想環境検出機能の使用
   b. サンドボックス環境と実際の感染の区別
5. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. 収集されたファイルを C2 サーバーに送信
   b. 暗号通貨関連データの窃取
6. [認証情報アクセス] 認証情報ダンピング (T1003)
   a. Chrome のログインデータの収集
   b. 窃取データの解読および送信

6) SectorA01 used PyYAML Vulnerability for Cryptocurrency Heist (2025-05-06)

https://cti.nshc.net/events/view/14933

SectorA01 グループは 2025 年 2 月に大規模な暗号通貨盗難事件を引き起こしました。彼らは主要なマルチシグネチャウォレットプロバイダー「Safe{Wallet}」との信頼関係を悪用し、サプライチェーンをターゲットにしました。このグループはソーシャルエンジニアリングを通じて開発者のワー

NSHC©2025 All rights reserved.

クステーションにアクセスし、その過程で Telegram や Discord のようなプラットフォームを利用した可能性があります。初期アクセスは「PyYAML」逆シリアル化の脆弱性を利用したマルウェア Python アプリケーションを通じて行われました。彼らは攻撃対象のワークステーションを掌握した後、多要素認証（MFA）で保護された AWS セッショントークンを盗み、AWS 環境への不正アクセスを試みました。永続的なアクセスを得るために MFA デバイスの登録を試みましたが失敗しました。侵入過程には IAM ロールと S3 資産に対する偵察活動が含まれていました。その後、このグループは「Next.js」静的ウェブアプリケーションを改ざんし、ハッキンググループの制御ウォレットに資金を迂回させる JavaScript ペイロードを注入しました。このマルウェアスクリプトは特定の取引条件下でのみアクティブ化され、検出を回避するように設計されていました。macOS では Docker ベースの技術を使用して隠密性を保ち、従来の検出システムを回避しました。

[Attack Flow]

1. [初期アクセス] フィッシング: スピアフィッシングリンク (T1566.002)
   a. ソーシャルエンジニアリングで開発者にアクセス
   b. マルウェアの Python アプリケーションを実行
2. [実行] クライアント実行のためのエクスプロイト (T1203)
   a. "PyYAML" の逆シリアル化脆弱性を利用
   b. "Docker" 関連要素を活用
3. [持続性] 有効なアカウント (T1078)
   a. "AWS" セッショントークンの窃取
   b. MFA デバイスの登録を試みる
4. [権限昇格] 権限昇格制御メカニズムの悪用: Setuid と Setgid (T1548.001)
   a. 一時セッショントークンで IAM ロールを探索
   b. "AWS" 環境で権限を拡大しようとする
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. JavaScript ペイロードを隠蔽
   b. 特定の取引条件でのみ活性化
6. [資格情報アクセス] ウェブセッションクッキーの窃取 (T1539)
   a. AWS セッショントークンの窃取
   b. 開発者環境で資格情報を収集
7. [探索] クラウドサービス探索 (T1580)
   a. IAM ロールと S3 バケットを探索
   b. "AWS" 環境内の資産を調査
8. [収集] ローカルシステムからのデータ (T1005)
   a. "macOS" で SSH キーを収集
   b. ブラウザデータおよび資格情報を収集

NSHC©2025 All rights reserved.

9. [コマンド＆コントロール] ウェブサービス: 双方向通信 (T1102.002)
    a. マルウェアスクリプトで C2 サーバーと通信
    b. "Python" ローダースクリプトを通じた持続的通信
10. [影響] データ操作 (T1565)
    a. "Next.js" ウェブアプリケーションを修正
    b. マルチシグネチャ取引を操作して資金を転送

7) SectorA02 used LNK Malware disguised as a Think Tank Invite (2025-05-12)

https://cti.nshc.net/events/view/15232

攻撃対象産業群: 社会運動団体

SectorA02 グループは 2025 年 3 月、精巧なスピアフィッシングキャンペーンを通じて北朝鮮関連の活動家を対象に攻撃を行いました。彼らは韓国の国家安全保障シンクタンクを装い、実際の学術フォーラム招待状を偽装したメールを通じて、Dropbox リンクで悪意のある LNK ファイルを配布しました。このファイルは実行時にメモリ内に隠された「RoKRAT」マルウェアを活性化し、ファイルレス攻撃技術を使用して検出を回避しました。該当グループは Dropbox をはじめ、「pCloud」や「Yandex」などの合法的なクラウドサービスをコマンド＆コントロール（C2）サーバーとして活用し、「Living off the Land（LotL）」に似た戦術を駆使しました。この攻撃は Windows システムを超えて Android および macOS ユーザーまでを標的とし、複数のシステムでゼロデイ脆弱性を利用しました。「RoKRAT」はシステム偵察、スクリーンショット収集、暗号化された通信を通じた情報漏洩を行います。また、クラウドサービスを利用した複雑な C2 通信は、「Dropbox」と「Yandex」API を悪用して悪意のある操作を行ったと分析されています。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
    a. メールを通じてスピアフィッシング攻撃を実行
    b. "Dropbox" リンクで悪性 LNK ファイルを配信
2. [実行] ユーザー実行 (T1204)
    a. ユーザーが LNK ファイルを実行
    b. メモリ内シェルコードを通じて "RoKRAT" マルウェアを活性化
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
    a. ファイルレス攻撃技術を使用
    b. メモリ内コード実行を通じた検出回避
4. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
    a. "Dropbox", "pCloud", "Yandex" API を通じた C2 通信
    b. クラウドサービスを活用して悪性通信を実行

NSHC©2025 All rights reserved.

5. [収集] スクリーンキャプチャ (T1113)
   a. システムのスクリーンショットを収集
   b. 収集した情報を暗号化後、C2 サーバーに送信
6. [データ流出] C2 チャネルを通じた流出 (T1041)
   a. 暗号化されたデータを C2 に流出
   b. 複数段階の暗号化を適用後に送信
7. [影響] データ破壊 (T1485)
   a. 悪性スクリプトの削除を通じて攻撃の痕跡を除去
   b. システムに対する悪性行動完了後、証拠を隠滅

8) SectorA02 は、学会情報に偽装した LNK マルウェアを使用しました（2025-05-12）

https://cti.nshc.net/events/view/15928

攻撃対象産業群: シンクタンク、社会運動団体

SectorA02 グループは 2025 年 3 月に北朝鮮関連の活動に従事する個人を対象にスピアフィッシング攻撃を実行しました。この攻撃は「韓国国家安全保障戦略シンクタンク」の学術会議案内メールを装い、Dropbox にホスティングされた ZIP ファイル形式の悪性リンクを含んでいました。ZIP ファイルにはショートカット（LNK）タイプのマルウェアが含まれており、実行時に追加のマルウェアを活性化します。該当グループは Dropbox のような信頼できるクラウドサービスをコマンド＆コントロール（C2）サーバーとして悪用する LoTS（Living off Trusted Sites）技法を活用しました。Windows システムだけでなく、Android や macOS プラットフォームでも攻撃を実行し、ゼロデイ脆弱性を利用しました。マルウェアは RoKRAT シリーズとして識別され、PowerShell を活用したファイルレス実行、メモリ内シェルコードのロード、AES-CBC-128 暗号化を利用した C2 通信などの高度な技法を使用しました。システム情報とスクリーンショットをリアルタイムで収集し、Dropbox、pCloud、Yandex API を通じて C2 サーバーに送信しました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. 韓国国家安全保障戦略イベントを装ったメール送信
   b. Dropbox リンクを含む ZIP ファイル添付
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. LNK ファイルの実行で追加の Malware を活性化
   b. PowerShell コマンドを通じたファイルレス実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. システム起動時の自動実行設定
   b. 一時フォルダにファイル生成

NSHC©2025 All rights reserved.

4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. PowerShell コマンドの引数難読化
   b. XOR ロジックによるデータ変換
5. [資格情報アクセス] OS 資格情報ダンピング: LSASS メモリ (T1003.001)
   a. メモリ内にシェルコードをロード
   b. メモリデータの窃取
6. [探索] システム情報探索 (T1082)
   a. システム情報の収集
   b. ユーザーおよびコンピュータ名の収集
7. [収集] スクリーンキャプチャ (T1113)
   a. リアルタイム画面のスクリーンショット保存
   b. JPEG 形式でファイル化
8. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. クラウドを通じた C2 通信
   b. AES-CBC-128 暗号化の使用
9. [流出] ウェブサービスを介した流出 (T1567)
   a. Dropbox API を通じたデータ流出
   b. pCloud と Yandex API の使用

9) SectorA05 used LNK Malware disguised as PDF Document (2025-04-22)

https://cti.nshc.net/events/view/14636

SectorA05 グループは、スピアフィッシング攻撃を通じて個人を対象にバックドアマルウェアを配布しました。攻撃は全 4 段階で進行し、初期侵入、持続性の維持、足場の確保、追加のマルウェア配布の順です。初期アクセスは「LNK」ファイルを通じて行われ、これは合法的な文書に偽装されています。ファイル実行時に Mshta を通じて JavaScript が実行され、これは PowerShell スクリプトを呼び出します。これらのスクリプトは持続性を維持するためにタスクスケジューラとレジストリキーを登録し、「Dropbox」およびコマンド＆コントロール（C2）サーバーとの通信を通じてマルウェアを配布します。彼らはまた、パッチされたシステム「DLL」を利用して「RDP」認証を回避し、「UACMe」のようなツールを使用して権限昇格を試みます。これは攻撃戦術の変化を示しており、攻撃効率を継続的に向上させるための適応を反映しています。

[Attack Flow]

1. [初期アクセス] サービスを介したスピアフィッシング (T1566.003)
   a. "LNK"ファイルを合法的な文書に偽装
   b. "mshta.exe"で"JavaScript"を実行

NSHC©2025 All rights reserved.

2. [実行] PowerShell (T1059.001)
   a. "PowerShell"スクリプトを呼び出し
   b. マルウェア配布のためのスクリプトを実行
3. [持続性] スケジュールされたタスク/ジョブ (T1053.005)
   a. スケジュールされたタスクを登録
   b. レジストリキーを登録
4. [防御回避] システム DLL の変更 (T1070.004)
   a. パッチされた"DLL"で"RDP"認証を回避
5. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. "UACMe"ツールで権限昇格を試みる
6. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. "Dropbox"と通信
   b. コマンド＆コントロール(C2)サーバーと通信

10) SectorA05 used LNK Malware disguised as Safe Work Plans (2025-05-13)

https://cti.nshc.net/events/view/15293

攻撃対象産業群: 政府・行政

SectorA05 グループは 2025 年 2 月に、ウクライナ政府機関を対象にフィッシングキャンペーンを展開しました。このキャンペーンは、ロシアのウクライナ侵攻による影響を把握するための情報収集を目的としており、資格情報の窃取と Malware の配布を含んでいます。ハッキンググループは無料のメールサービスを利用して架空のシンクタンク所属の人物に偽装し、最近のウクライナの政治事件をテーマにした誘引文書をフィッシングメールに挿入して攻撃対象を惑わせました。Malware は HTML および CHM ファイルを通じて配布され、これらのファイルには埋め込まれた PowerShell スクリプトが含まれており、ユーザーが実行すると感染プロセスが開始されます。フィッシングメールの本文には MEGA のようなファイルホスティングサービスのリンクが含まれており、被害者がこれを通じてパスワードで保護された RAR 圧縮ファイルをダウンロードすると、解凍後に悪意のある PowerShell スクリプトが実行されるように設計されています。該当の誘引文書にはウクライナ軍の人物の画像が含まれており、ユーザーが悪意のあるスクリプトをクリックするように誘導します。実行されたスクリプトは、被害ホストに対する偵察を行った後、収集された情報をコマンド＆コントロールサーバーに送信する機能を含んでいます。

[Attack Flow]

1. [リソース開発] 侵害されたアカウント (T1586)
   a. "Proton Mail" アカウントを通じた偽の "Microsoft" 警告送信
   b. 以前に知られている侵害されたドメインの使用

NSHC©2025 All rights reserved.

2. [初期アクセス] スピアフィッシングリンク (T1566.002)
   a. "Freemail" アカウントを使用して偽のシンクタンクメンバーを装う
   b. 最近のウクライナの政治事件に基づく誘引物を挿入
c. "MEGA" ファイルホスティングサービスリンクを含む
d. パスワード保護された "RAR" アーカイブのダウンロード
4. [実行] コマンドとスクリプトインタープリタ: PowerShell (T1059.001)
   a. "HTML" および "CHM" ファイルに埋め込まれた "PowerShell" スクリプトを含む
   b. "PowerShell" を通じて感染チェーンを開始
5. [持続性] ブートまたはログオン自動開始実行: レジストリ実行キー / スタートアップフォルダ (T1547.001)
   a. "state.bat" ファイルを "APPDATA" に保存
   b. バッチファイルを自動実行ファイルとして登録
6. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. "Base64" エンコーディングを使用して情報を転送
   b. "PowerShell" スクリプトの複雑性を増加
7. [資格情報アクセス] 情報のフィッシング: スピアフィッシングリンク (T1598.002)
   a. 偽の "Microsoft" 警告メッセージで資格情報を収集しようとする
   b. 認証試行の確認を要求
8. [収集] ローカルシステムからのデータ (T1005)
   a. "ipconfig /all", "systeminfo" コマンドを使用
   b. 最近のファイル名およびディスク情報を収集
9. [流出] C2 チャネルを介した流出 (T1041)
   a. "POST" リクエストを通じてデータを転送
   b. "Base64" エンコーディングされた情報を転送。

11) SectorA05 は NDA ドキュメントファイルに偽装したマルウェアを使用しました (2025-05-12)

https://cti.nshc.net/events/view/15266

SectorA05 グループは「NDA.pdf.msc」という名前のマルウェアファイルを利用した攻撃を実行しました。このファイルは表面的には PDF ドキュメントのように見えますが、実際にはマルウェアを含む Windows 管理コンソール(.msc)ファイルであり、ソーシャルエンジニアリング技術を通じて被害者に実行を促す方法です。このグループはファイル名を「秘密保持契約書(NDA)」に偽装して攻撃対象を欺き、内部には base64 でエンコードされた悪意のあるスクリプトが含まれていました。このスクリプトは多段階デコードを経て最終的に実行され、その過程でオランダに位置する外部サーバーから「kaptsole_x.rar」アーカイブと「UnRAR.exe」実行ファイルをダウンロードし、復号化され

NSHC©2025 All rights reserved.

たペイロードを露出させました。その後、露出したスクリプトはシステム API を利用して実行ウィンドウを隠し、追加のマルウェアペイロードをダウンロードした後、これを一般的なドキュメントに偽装する方法で感染を拡大させました。特に、このペイロードはゲーム産業のデジタル資産に関連するコンテンツを含んでおり、攻撃対象がゲーム関連業界または関連データを保有する人物であると推測されます。このように、SectorA05 グループはファイル偽装、多段階エンコード、システム API 操作、外部サーバー利用など多層的な隠蔽および分析回避技術を組み合わせて、精巧な攻撃戦術を展開しました。

[Attack Flow]

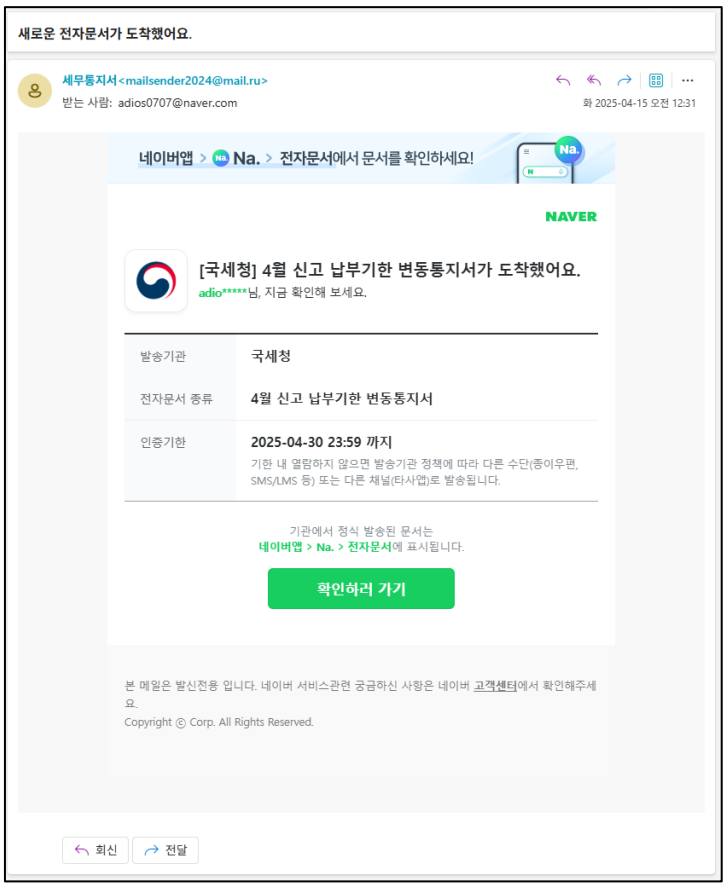
1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. "NDA.pdf.msc" ファイルをメール添付ファイルとして送信
   b. PDF ファイルに偽装された "msc" 拡張子を利用
2. [実行] スクリプティング (T1059)
   a. Base64 エンコードされたスクリプトの多重デコード
   b. PowerShell スクリプトの実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. Base64 エンコードの使用
   b. 複数段階のデコード
4. [コマンド＆コントロール] ツール転送の受信 (T1105)
   a. 外部サーバーから "kaptsole_x.rar" および "UnRAR.exe" をダウンロード
   b. オランダのサーバーを使用
5. [防御回避] アーティファクトの隠蔽 (T1564.003)
   a. ShowWindow() API で実行ウィンドウを隠す
   b. PowerShell ウィンドウを隠す
6. [実行] コマンドおよびスクリプトインタープリター (T1059.001)
   a. Invoke-Expression でスクリプトを実行
   b. 外部ペイロードをダウンロードして実行
7. [収集] ローカルシステムからのデータ (T1005)
   a. "kaptsole_x.txt" ファイルの内容を読み取り、変数に保存
   b. システムメモリから情報を収集
8. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. 収集されたデータを C2 チャネルに送信
   b. C2 サーバーへのデータ送信を通じた情報の窃取

12）SectorA05 は税務通知アラートを装ったフィッシングメールを使用しました（2025-05-08）

https://cti.nshc.net/events/view/14983

NSHC©2025 All rights reserved.

SectorA05 グループが「国税庁」を装ってフィッシングメールを通じて攻撃を行った。このメールは「mail(.)ru」サーバーを通じてロシアの IP アドレス「89[.]221[.]237[.]132」から送信され、「国税庁」を装った送信者アドレスを使用していた。メールは受信者を偽の「NAVER」ログインページに誘導し、アカウント情報を盗むように設計されていた。メールには「SPF」、「DKIM」、「DMARC」認証を通過する設定が適用されており、受信者がメールの真偽を疑わないようにしていた。これは「mail(.)ru」のポリシーと一致するため可能なことだった。また、「User-Agent」情報がなく自動送信されたものと見られ、「ARC チェーン」メール認証を活用して出所を隠し、「NAVER」アカウントへの不正アクセスを試みた。この攻撃は、韓国のユーザーを対象とした巧妙なメールスプーフィングおよび資格情報窃取技術を活用したフィッシング試みと見なすことができる。



[図 3: SectorA05 グループが使用したフィッシングメール]

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 「国税庁」を装ったフィッシングメールの送信
   b. 受信者を偽の「ネイバー」ログインページに誘導
2. [認証情報アクセス] 入力キャプチャ (T1056)

NSHC©2025 All rights reserved.

a. 偽のページでパスワード入力を誘導
b. 入力されたパスワードでアカウント情報を窃取
3. [防御回避] メール認証バイパス (カスタム)
a. 「SPF」、「DKIM」、「DMARC」認証を通過
b. 「ARC チェーン」メール認証で出所を隠蔽
4. [実行] スクリプティング (T1064)
a. 自動化されたメール送信スクリプトの使用
b. 「User-Agent」情報なしでメール送信
5. [収集] 認証情報収集 (T1589.002)
a. 収集されたアカウント情報の保存と送信
b. 不正アクセス試行のための情報利用

13) SectorA05 used Phishing Page disguised as Naver Login Notice (2025-05-20)
https://cti.nshc.net/events/view/15697

2025 年 5 月 20 日、SectorA05 グループが「国税庁」を装ったフィッシングキャンペーンを実行しました。このキャンペーンは、個人に公式の税金申告期限通知を装ったメールを送信し、攻撃対象を欺きました。該当グループは、ユーザーの ID を事前に入力した状態で被害者がパスワードを入力するよう誘導する偽のログインページを使用しました。このページは、韓国の有名なメールプロバイダーの合法的なポータルのように見え、被害者が情報を入力すると資格情報を盗み取った後、実際のメールサービスページにリダイレクトされました。フィッシングサイトはモスクワと関連するドメインでホスティングされ、メールは「inbox.ru」アドレスから送信されました。SPF、DKIM、DMARC チェックを通過し、メールの信頼性を高めました。メールに含まれたリンクはプライバシーポリシーを装っていましたが、実際にはフィッシングサイトに接続されていました。この攻撃は、政府の通信を模倣して個人情報を収集するために戦略的に設計されたフィッシング手法でした。

[Attack Flow]
1. [初期アクセス] スピアフィッシングリンク (T1566.002)
a. 「国税庁」を装ったメール送信
b. 「inbox.ru」アドレス使用
2. [資格情報アクセス] フィッシング (T1566)
a. 事前入力されたユーザーID
b. 偽のログインページでパスワード入力を誘導
3. [実行] ユーザー実行 (T1204)
a. クリックするとフィッシングページに移動
b. プライバシーポリシーリンクに偽装

NSHC©2025 All rights reserved.

4. [コマンド＆コントロール] ウェブサービス (T1102)
   a. モスクワドメインに接続
   b. 資格情報を盗んだ後リダイレクト
5. [防御回避] 信頼された関係 (T1199)
   a. SPF、DKIM、DMARC チェックを通過
   b. 正当なメールで信頼性を確保

14) SectorA05 used PowerShell Malware disguised as text files (2025-05-12)

https://cti.nshc.net/events/view/15533

SectorA05 グループは、XWorm RAT（リモートアクセス型トロイの木馬）を拡散するために高度に洗練された PowerShell ベースのペイロードを活用したマルウェアキャンペーンを実施しました。このグループは、Base64 でエンコードされたスクリプトと多段階感染チェーンを通じてセキュリティメカニズムを回避し、対象システムに密かに侵入してリモート制御を確立することに焦点を当てています。彼らは検出を回避するためにファイルレス方式とともに Living-off-the-Land Binaries and Scripts（LOLBAS）技法を積極的に活用し、攻撃初期段階でデコードを経て悪意のある行為が明らかになる Base64 エンコード PowerShell スクリプトを使用しました。このスクリプトは、悪意のある IP アドレス（例：185[.]235[.]128[.]114, 92[.]119[.]114[.]128）からパスワードで保護された RAR アーカイブ、実行ファイル、追加の PowerShell スクリプトをダウンロードし、これらは無害なテキストファイルに偽装されて分析を回避します。また、PowerShell に C#コードをインライン挿入して ShowWindow API を呼び出すことで実行ウィンドウを隠し、ユーザーの注意をそらすために偽の PDF ドキュメントを同時にダウンロードする社会工学的手法も含まれています。最終段階では、グループポリシーを回避してマルウェアの実行持続性を確保し、Windows イベントロギング機能を無効化することで感染の痕跡を最小限に抑えます。パスワードで保護されたアーカイブは UnRAR ツールを利用して自動抽出され、隠されたペイロードは Invoke-Expression を通じて実行されます。このキャンペーンは、高度な難読化、非標準化されたデータエンコーディングを利用したコマンド＆コントロール（C2）通信、システムに組み込まれたバイナリの広範な活用など、さまざまな回避戦略を組み合わせており、ハイパーバイザー環境を回避し RDP（リモートデスクトッププロトコル）アクセスを通じて高価値エンティティを集中的に狙うなど、目標に基づいた精密な攻撃戦術を明らかにしました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング (T1566)
   a. "Base64" エンコードされた "PowerShell" スクリプトの使用
   b. マルウェア IP からのファイルダウンロード
2. [実行] コマンドとスクリプトインタープリター (T1059)

NSHC©2025 All rights reserved.

a. "PowerShell" スクリプトのデコードと実行
b. "C#" コードのインライン挿入
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. ファイルレス実行
b. "Windows" イベントロギングの無効化
4. [持続性] 有効なアカウント (T1078)
a. パスワード保護されたアーカイブの抽出
b. ポリシー回避の実行
5. [コマンド＆コントロール] 非標準ポート (T1571)
a. 非標準データエンコーディングの使用
b. C2 通信の設定
6. [データ搾取] C2 チャネルを介したデータ搾取 (T1041)
a. 機密データの窃取
b. C2 チャネルを通じたデータ転送

15) SectorA05 は、税務通知 PDF に偽装した LNK マルウェアを使用しました（2025-04-22）
https://cti.nshc.net/events/view/14584

SectorA05 グループは、マルウェアの Windows ショートカット（LNK）ファイルを配布したと分析されています。このファイルは地方税の通知書に偽装されており、ユーザーが実行すると、ハッキンググループのサーバーから追加の HTA ファイルを temp フォルダにダウンロードして実行します。この HTA ファイルには、圧縮ファイル（ZIP）とおとり文書（PDF）が含まれており、ZIP には 4 つのファイル（1.log、2.log、1.ps1、1.vbs）が存在します。この中で、1.log と 2.log は Base64 でエンコードされた PowerShell スクリプトを含んでおり、1.log は情報収集とハッキンググループのコマンド実行を、2.log はキーロギングを行います。特に 1.vbs スクリプトの一部には、ハッキンググループが残した韓国語のコメントが確認されました。このグループは国内ポータルサイトに偽装した URL を通じてこの LNK ファイルを配布し、これを通じてブラウザ情報、公認認証書、デジタル証明書などの貴重なデータを収集します。攻撃の主な目的は、国内ユーザーの機密情報を盗むことにあります。LNK ファイルの配布に使用された URL は、hxxps://nid-naveroup.servepics[.]com/docs/revenue.zip で確認されました。

[Attack Flow]
1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
a. "LNK"ファイルを「地方税収入通知書」に偽装
b. 悪性の"LNK"ファイル実行誘導
2. [実行] ユーザー実行 (T1204)

NSHC©2025 All rights reserved.

a. "LNK"ファイル実行時に"HTA"ファイルをダウンロードおよび実行
b. "temp"フォルダに"HTA"ファイル保存
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. "1.log"、"2.log"に Base64 エンコードされた PowerShell スクリプト
b. ハングルコメントを挿入して混乱を誘導
4. [収集] 入力キャプチャ (T1056)
a. "2.log"を通じたキーロギング実行
5. [収集] 情報リポジトリからのデータ (T1213)
a. ブラウザ情報、公認認証書、デジタル証明書の収集
6. [コマンド＆コントロール] コマンド＆コントロールプロトコル (T1071)
a. "1.log"を通じたハッキンググループのコマンド実行
b. 収集された情報をハッキンググループに送信

16) SectorA07 used LNK Malware disguised as a Proposal PDF (2025-04-24)

https://cti.nshc.net/events/view/14642

攻撃対象産業群: 金融

SectorA07 グループは、「提案書.pdf.lnk」という名前で偽装されたマルウェアショートカット（LNK）ファイルを利用した攻撃を実行しました。このファイルは、実行時にコマンドプロンプト（CMD）を通じて様々な作業を行う PowerShell スクリプトを呼び出すように設計されています。初期段階でスクリプトはシステム内の「rshell.exe」ファイルを探索して実行し、これはリバースシェル機能またはコマンド＆コントロール（C2）通信手段として利用される可能性があります。その後、特定の LNK ファイルを識別し、Stir 関数と XOR 演算を組み合わせた方法でマルウェアペイロードを復号化するプロセスを進めます。攻撃はこれ以外にも追加のペイロードを CAB 圧縮ファイル形式で含んでおり、これをドキュメントフォルダ内に解凍した後、自動実行します。感染の最終段階では、「start.vbs」スクリプトを呼び出してマルウェア活動を完了し、実行に使用されたショートカット（.lnk）および CAB ファイルを削除することで痕跡を消す機能も含まれています。補助 PowerShell スクリプトは、ユーザーディレクトリ内のファイルリストとシステム情報を収集し、該当グループのサーバーにアップロードしますが、これは攻撃対象環境に対する偵察目的の活動と解釈されます。また、このマルウェアは RC4 暗号化と base64 エンコーディングを組み合わせて収集された情報を暗号化し、HTTP POST リクエストを通じて事前に指定されたアップロード URL にデータを密かに送信します。全体のキャンペーンは、偽装、多段階復号化、自動化された情報収集および精巧なデータ暗号化技術を組み合わせることで、検出回避を最大化し、機密情報の隠蔽された流出に重点を置いた高度な攻撃様相を示しています。

[Attack Flow]

NSHC©2025 All rights reserved.

1. [実行] コマンドとスクリプトインタープリター (T1059)
   a. cmd.exe を通じた PowerShell スクリプトの実行
   b. "rshell.exe"ファイルの探索と実行
2. [防御回避] 偽装 (T1036)
   a. "제안서.pdf.lnk"ファイルに偽装
   b. .lnk ファイルを使用してペイロードを暗号化
3. [発見] ファイルとディレクトリの発見 (T1083)
   a. ユーザーディレクトリとシステム情報の収集
   b. d1.txt, d2.txt, d3.txt, d4.txt ファイルに情報を保存
4. [収集] ローカルシステムからのデータ (T1005)
   a. ユーザーディレクトリのコンテンツを収集
   b. システム情報の収集と保存
5. [流出] C2 チャネルを介したデータ流出 (T1041)
   a. 収集したデータを指定されたサーバーにアップロード
   b. RC4 および base64 を使用したデータの暗号化
6. [防御回避] ホスト上のインジケーターの削除 (T1070)
   a. .lnk および CAB ファイルの削除で痕跡を除去
   b. アップロード成功時に関連ファイルを削除

17) SectorB01 used Cobalt Strike via DLL Sideloading Disguised as Apps (2025-04-29)

https://cti.nshc.net/events/view/14722

SectorB01 グループは、DLL サイドローディング技法を利用して Cobalt Strike ペイロードを配信するマルウェアキャンペーンを展開しました。このグループは、通常のプログラムと共にロードされる DLL をマルウェア版に置き換える典型的なサイドローディング方式に加え、破損または期限切れのデジタル署名を含むインストーラを利用して信頼性を偽装しました。特に、彼らはシステムクロックを操作して期限切れの証明書を一時的に有効と認識させる方法で署名検証を回避しました。攻撃の初期段階は、韓国のオンラインゲーム開発者に関連するデジタル署名付きインストーラを通じて開始され、この過程で Windows API 呼び出しを操作するために Minhook ライブラリが使用されました。Minhook はフック機能を通じて API の正常な動作を傍受し、マルウェアロジックを挿入するために利用され、これは検出回避およびコード隠蔽において重要な役割を果たしました。全体のキャンペーンは三つの主要なサイドローディングシナリオで構成され、それぞれは MiracastView、PrintDialog、SystemSettings など Windows の合法的なコンポーネントをローダーとして使用しました。これらのローダーは、マルウェア DLL を通常の DLL の代わりにロードして暗号化された Cobalt Strike ペイロードを実行する構造になっています。実行後、プロセスインジェクション技法を通じてマルウ

NSHC©2025 All rights reserved.

ェアが通常のプロセス内部に注入されて実行され、C2 通信は Cobalt Strike 固有のコマンド＆コントロールサーバーを通じて行われます。この過程で通信フローは通常のシステム活動に偽装され、API フックおよびエンコーディング技法を複合的に利用して検出を効果的に回避しました。

[Attack Flow]

1. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. コマンドインタープリタの使用
   b. スクリプトの実行
2. [防御回避] 偽装 (T1036)
   a. "Cobalt Strike" ペイロードの偽装
   b. 正常なシステムファイルの偽装
3. [防御回避] プロセスインジェクション (T1055)
   a. プロセスメモリへのコード挿入
   b. 正常プロセスへのマルウェア注入
4. [資格情報アクセス] アプリケーションアクセス トークンの窃取 (T1528)
   a. アプリケーションアクセス トークンの窃取
   b. 認証情報の収集
5. [持続性] DLL サイドローディング (T1073)
   a. "MiracastView", "PrintDialog", "SystemSettings" DLL の悪用
   b. 正規の DLL ファイルの置換
6. [防御回避] 有効なアカウント (T1078)
   a. 侵害されたアカウントの使用
   b. 権限のあるアカウントでのアクセス
7. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
   a. HTTP を通じた C2 サーバー通信
   b. "Cobalt Strike" ビーコンの使用
8. [収集] ローカルシステムからのデータ (T1005)
   a. ローカルシステムデータの収集
   b. ファイルおよび情報の収集
9. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. C2 チャネルを通じたデータ流出
   b. ネットワークを通じた情報の送信

18) SectorB02 used Sideloaded Malware for Espionage in Southeast Asia (2025-04-22)

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

NSHC©2025 All rights reserved.

攻撃対象産業群: 政府・行政、通信、建設

SectorB02 グループは、2024 年 8 月から 2025 年 2 月にかけて、東南アジアの複数の組織を対象にサイバー諜報キャンペーンを実施しました。攻撃対象には、政府機関、航空交通管制組織、通信事業者、建設会社が含まれ、他の東南アジア諸国のニュースエージェンシーや航空貨物組織も侵害されました。彼らは、ローダー、資格情報窃取ツール、リバース SSH ツールなどの複数のカスタムツールを展開しました。主要な手法の一つは、「Trend Micro」と「Bitdefender」の正規ソフトウェアを利用した DLL サイドローディングで、悪性 DLL をロードして追加の悪性活動を可能にしました。具体的には、「tmdbglog.exe」と「bds.exe」といったバイナリを使用して、「tmdglog.dll」と「log.dll」という悪性 DLL をサイドローディングし、暗号化された Malware の内容を実行しました。また、「Sagerunex」バックドアの新しいバリアントを展開し、これはレジストリの修正による持続性を特徴としています。「ChromeKatz」や「CredentialKatz」といったツールは、「Chrome」ブラウザの資格情報を狙い、リバース SSH ツールはリモートアクセスのために展開されました。該当グループは、「datechanger.exe」を使用してファイルのタイムスタンプを操作し、フォレンジック分析を複雑にしました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
    a. スピアフィッシングメール送信
    b. 添付されたマルウェア文書を開く
2. [実行] DLL サイドローディング (T1574.002)
    a. "tmdbglog.exe" および "bds.exe" の使用
    b. "tmdglog.dll" および "log.dll" のロード
3. [持続性] レジストリ実行キー / スタートアップフォルダ (T1547.001)
    a. レジストリの修正
    b. サービスとして実行し持続性を維持
4. [資格情報アクセス] 資格情報ダンピング (T1003)
    a. "ChromeKatz" および "CredentialKatz" の使用
    b. "Chrome" ブラウザの資格情報を奪取
5. [防御回避] タイムスタンプ (T1070.006)
    a. "datechanger.exe" の使用
    b. ファイルのタイムスタンプを操作
6. [コマンド＆コントロール] インバウンドツール転送 (T1105)
    a. リバース SSH ツールの使用
    b. ポート 22 で SSH 接続を受信
7. [探索] システム情報探索 (T1082)

NSHC©2025 All rights reserved.

a. システム情報の収集
b. ネットワーク環境の探索

19) SectorB108 used Cisco IOS XE WebUI Vulnerabilities for Attacks (2025-04-25)

https://cti.nshc.net/events/view/14693

攻撃対象産業群: 政府・行政、通信

SectorB108 グループは主要な通信事業者を対象に、ネットワークデバイスインターフェースの既知の脆弱性を利用して攻撃を行いました。彼らは「Sophos Firewalls」、「Cisco IOS XE WebUIs」、「Ivanti Connect Secure」、「Fortinet FortiClient EMS」システムを通じて初期侵入を試みました。過去 6 ヶ月間でこれらのデバイスの露出は 25%減少し、特に「Sophos Firewall」の場合は 35%減少したことが示されています。しかし、「Cisco IOS XE」は露出が 7%増加し、深刻なリスクを引き起こしています。このシステムの脆弱性である「CVE-2023-20198」（権限昇格）と「CVE-2023-20273」（コマンドインジェクション）は、影響を受けるデバイスに対する完全な制御を許可します。これらの脆弱性は、未承認のアクセスと持続的なインフラ操作を可能にし、GRE トンネルのような隠密な手法を使用します。

[Attack Flow]

1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. "Sophos Firewalls"のリモートコード実行脆弱性の利用
   b. "Cisco IOS XE"の Web UI 脆弱性の悪用
2. [持続性] アカウント作成 (T1136)
   a. "Cisco IOS XE"での権限昇格を通じたユーザーアカウントの作成
   b. "Ivanti Connect Secure"の認証回避による持続的なアクセスの維持
3. [実行] コマンドおよびスクリプトインタープリター (T1059)
   a. "Cisco IOS XE"のコマンドインジェクションを通じたコマンド実行
   b. "Ivanti Connect Secure"のコマンドインジェクション脆弱性の活用
4. [防御回避] ツールの無効化または変更 (T1562)
   a. ログの無効化
   b. ネットワークトラフィック回避のための GRE トンネルの設定
5. [資格情報アクセス] 保護されていない資格情報 (T1552)
   a. 盗まれた認証情報でのシステムアクセス
   b. デバイス設定の変更を通じた権限強化
6. [影響] データ操作 (T1565)
   a. デバイス構成の変更
   b. 攻撃の持続のためのインフラ操作

NSHC©2025 All rights reserved.

20) SectorB112 used Spellbinder for IPv6 Lateral Movement Attacks (2025-04-30)

https://cti.nshc.net/events/view/14755

SectorB112 グループは、2022 年に初めて発見されたマルウェアツール「Spellbinder」を利用して、IPv6 SLAAC（Stateless Address Autoconfiguration）スプーフィングに基づく Adversary-in-the-Middle（中間者攻撃）を実行しました。このキャンペーンは、フィリピン、カンボジア、アラブ首長国連邦（UAE）、中国本土および香港地域のシステムを主なターゲットとしており、特に中国語入力ソフトウェアを悪用してマルウェアダウンロードプログラム「WizardNet」を配布する戦略を使用しました。Spellbinder は WinPcap ライブラリを基にネットワークパケットをキャプチャし、ICMPv6 ルーター広告（RA）パケットを生成して攻撃対象に悪意のあるルーター設定を伝達することで、ネットワークトラフィックを該当グループの制御下にあるデバイスに誘導します。彼らはさらに DNS スプーフィング技術を用いて「Tencent」などの正規ソフトウェアのアップデート要求を傍受し、正規のアップデートファイルをマルウェアペイロードに置き換える攻撃も実行しました。これにより、被害者は信頼できるアップデートに偽装されたマルウェアファイルを無意識にインストールし、最終的に主要ペイロードである「WizardNet」が実行されます。該当ペイロードは.NET ベースのモジュールを活用してマルウェア機能を拡張しており、コマンド＆コントロール（C2）通信過程で暗号化を適用することで、検出および分析を回避しています。このグループはネットワークベースの脅威とソフトウェア偽装技術を組み合わせた複合的な攻撃パターンを示し、中間者攻撃を通じて全体の感染経路を密かに構築することに焦点を当てています。

[Attack Flow]

1. [リソース開発] インフラストラクチャの取得: ドメイン (T1583.001)
   a. ドメイン登録
   b. サーバーインフラの構築
2. [リソース開発] インフラストラクチャの取得: サーバー (T1583.004)
   a. マルウェア更新提供サーバーの確保
   b. C&C サーバーの確保
3. [リソース開発] 能力の開発: マルウェア (T1587.001)
   a. "WizardNet" バックドアの開発
   b. "Spellbinder" ツールの開発
4. [リソース開発] 能力の取得: ツール (T1588.002)
   a. "WinPcap" のインストール
   b. ネットワークパケットキャプチャの準備
5. [初期アクセス] コンテンツインジェクション (T1659)
   a. DNS 応答メッセージの送信

NSHC©2025 All rights reserved.

b. アップデートハイジャック
6. [実行] コマンドとスクリプトインタープリタ: Windows コマンドシェル (T1059.003)
a. コマンドの実行
b. ツールのダウンロードと実行
7. [実行] ネイティブ API (T1106)
a. プロセスの実行
b. シェルコードの注入
8. [権限昇格] プロセスインジェクション (T1055)
a. コードの注入
b. プロセス権限の昇格
9. [防御回避] 実行ガードレール: 相互排除 (T1480.002)
a. ミューテックスの作成
b. バックドアの重複実行防止
10. [コマンドとコントロール] ツールの転送 (T1105)
a. ツールおよびモジュールの配布
b. C&C サーバーとの通信
11. [コマンドとコントロール] 非アプリケーション層プロトコル (T1095)
a. TCP/UDP の使用
b. AES 暗号化の適用
12. [コマンドとコントロール] 暗号化チャネル: 対称暗号 (T1573.001)
a. 対称暗号化の使用
b. C&C サーバーとの安全な通信

21) SectorB113 used Supply Chain Attacks Targeting Military and Satellite (2025-05-13)

https://cti.nshc.net/events/view/15280

攻撃対象産業群: 軍事機関、技術、メディア・報道

SectorB113 グループは、2023 年から 2024 年にかけて「VENOM」と「TIDRONE」という 2 つの主要なキャンペーンを実施し、台湾と韓国のさまざまな産業を攻撃対象としました。「VENOM」キャンペーンは、サプライチェーンの上流セクションを通じてソフトウェアサービスプロバイダーに侵入することを目的としており、オープンソースツールを使用して活動を隠蔽しました。一方、「TIDRONE」キャンペーンは、CXCLNT や CLNTEND のようなカスタムツールを活用し、軍事および衛星産業を対象にサイバースパイ活動を行いました。このグループは、初期アクセスのために古典的なコードインジェクション手法と一般的な信頼悪用方法を組み合わせてサプライチェーン攻撃技術を利用しました。持続性はオープンソースプロキシとリモートアクセスツール（RAT）を通じて維持

NSHC©2025 All rights reserved.

され、資格情報のダンピングと特殊なバックドアを使用して密かにデータを流出させました。また、繊維ベースの Malware 技術を使用して検出を回避するための高度な回避技術を適応させました。両キャンペーンは攻撃対象とインフラを共有しており、同じハッキンググループが信頼できるネットワークを狙い、下位の高価値エンティティに到達することを目的としていると見られます。

[Attack Flow]

1. [初期アクセス] サプライチェーンの妥協 (T1195)
   a. ウェブサーバーの脆弱性悪用
   b. 正当なソフトウェアアップデートパッケージの置換
2. [実行] コマンドとスクリプトインタープリター (T1059)
   a. コマンドラインを通じたマルウェア実行
   b. シェルコマンドを通じたリモートシェル実行
3. [持続性] システムプロセスの作成または変更 (T1543)
   a. スケジュールされたタスクの作成
   b. 正当な実行ファイルの置換
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. UAC バイパスの実行
   b. プロセストークンを使用した再起動
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 実行順序依存性の活用
   b. エントリーポイントの検証
6. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. Mimikatz を通じた資格情報ダンピング
   b. NTDS データのターゲット
7. [探索] システム情報探索 (T1082)
   a. システム情報の収集
   b. システム構成の更新
8. [横移動] リモートサービス (T1021)
   a. 信頼できる通信チャネルの活用
   b. リモートモニタリングツールの使用
9. [収集] スクリーンキャプチャ (T1113)
   a. スクリーンキャプチャツールのインストール
   b. スクリーンショットの送信
10. [コマンドとコントロール] 暗号化されたチャネル (T1573)
    a. HTTPS を通じた暗号化通信
    b. SSL を通じたカスタムプロトコルの使用

NSHC©2025 All rights reserved.

11. [流出] C2 チャネルを通じた流出 (T1041)
    a. C&C サーバーを通じたデータ流出
    b. バイナリデータの送信
12. [影響] データ破壊 (T1485)
    a. 痕跡の消去
    b. ローダーおよびペイロードの削除

22) SectorB22 used Claimloader with Politically-Themed Lures (2025-05-15)

https://cti.nshc.net/events/view/15822

攻撃対象産業群: 政府・行政、軍事機関、外交

SectorB22 グループは、2024 年末から始まった疑わしいサイバー諜報キャンペーンを通じて、武器化された ZIP アーカイブを利用して Pubload と Toneshell バックドアを配布しています。この攻撃は、フィリピン、アメリカ、パキスタンの政府、軍事、外交関係者を主なターゲットとしており、地政学的なテーマを餌として使用しています。該当グループは「Claimloader」マルウェアを利用して持続的なアクセスを確保し、台湾では「USB」ワームを活用して悪性ペイロードを拡散しています。「Claimloader」マルウェアは DLL サイドローディングを通じてペイロードを実行し、「AES」と「DES」復号化を使用してレジストリと予約タスクを通じて持続的なアクセスを設定します。「Pubload」と「Toneshell」マルウェアは「C2」通信を通じてシステム情報を伝達し、リモートコマンド実行を可能にするリバースシェルを生成します。このグループの攻撃は、多様なマルウェアアーセナル、様々な暗号化方式、高度なローディング技術を使用して機密情報を抽出しようとする巧妙さを強調しています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
    a. 武器化された「ZIP」アーカイブ添付
    b. 地政学的な餌の使用
2. [実行] DLL サイドローディング (T1574.002)
    a. 「Claimloader」を利用した「DLL」実行
    b. 正規の実行ファイルを通じた Malware ロード
3. [持続性] レジストリ実行キー / スタートアップフォルダ (T1547.001)
    a. レジストリに持続性キーを生成
    b. 「Scheduled Task」を通じた定期的実行
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
    a. 暗号化および難読化されたペイロードの使用
    b. ファイル属性を隠しに設定

NSHC©2025 All rights reserved.

5. [収集] 入力キャプチャ (T1056)
   a. システム情報の収集
   b. ユーザー名、コンピュータ名の取得
6. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
   a. 「C2」サーバーとの暗号化された通信
   b. 「TLS」パケット形式でのデータ送信
7. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. 収集されたデータを「C2」サーバーに送信
   b. リバースシェルを通じたデータ流出
8. [横移動] リモートファイルコピー (T1105)
   a. 「USB」ワームを通じたペイロードの拡散
   b. 台湾内ネットワークへの拡散

23) SectorB86 used DslogdRAT with CVE-2025-0282 for Web Shell Attacks (2025-04-24)

https://cti.nshc.net/events/view/14644

SectorB86 グループはゼロデイ脆弱性「CVE-2025-0282」を悪用して攻撃対象の組織に侵入しました。該当グループは「Perl CGI」スクリプトで構成されたウェブシェルを配布し、特定の「Cookie」ヘッダー値を通じてコマンドを実行しました。これにより「DslogdRAT」Malware を配布し、悪意のある活動を行いました。「DslogdRAT」は実行時に複数のプロセスを生成し、2 番目の子プロセスが主要な機能を管理します。この機能には「XOR」関数でエンコードされたハードコーディングされた設定データをデコードし、「C2」サーバーとのソケットデータ転送を通じて通信を設定し、コマンドを実行することが含まれます。設定データは業務時間内の通信を通じて検出を避けるための作戦パラメータを詳細に示しています。この Malware はプロキシ通信をサポートし、ファイル操作やコマンド実行を含む様々なコマンドを実行することができます。

[Attack Flow]

1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. CVE-2025-0282 の悪用
   b. Web シェルの配布
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. 特定の Cookie ヘッダー値の利用
   b. 任意コマンドの実行
3. [持続性] システムプロセスの作成または変更 (T1543)
   a. DslogdRAT の複数プロセス生成

NSHC©2025 All rights reserved.

b. 子プロセスの管理
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. XOR 関数による設定データのエンコード
b. ハードコーディングされた設定データ
5. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
a. ソケットデータの送信
b. プロキシ通信のサポート
6. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. C2 サーバーとの通信
b. コマンドおよびデータの送信

24) SectorB91 used ROAMINGMOUSE in Spear-Phishing Campaign (2025-04-30)

https://cti.nshc.net/events/view/14786

攻撃対象産業群: 政府・行政

SectorB91 グループは、日本の政府機関および公共機関を対象に精巧なサイバーキャンペーンを実施しました。彼らはスピアフィッシング戦術を使用して攻撃を行い、新しいバージョンの「ANEL」バックドアを配布して諜報活動を行う可能性が高いです。このグループは、損傷した OneDrive リンクを利用して悪意のある Excel ファイルを配布しました。これらのファイルはドロッパーとして機能し、マクロを使用して Malware をインストールしました。以前のキャンペーンとは異なり、今回の攻撃ではマウスの動きイベントの代わりにクリックイベントで悪意のあるプロセスをトリガーしました。攻撃には「ROAMINGMOUSE」、「ANELLDR」、「NOOPDOOR」などのコンポーネントが含まれ、「DLL サイドローディング」、暗号化、「DNS over HTTPS」（DoH）を活用して検出を回避しました。彼らは情報窃取を目的として、「tasklist」や「net localgroup」などのバックドアコマンドを実行し、被害者の環境を調査し潜在的なデータを探索しました。強化された事後搾取戦術も観察され、「NOOPDOOR」を配布して持続性を確保し、メモリ内で「Beacon Object Files」を実行できる新しいコマンドサポートを通じて技術的アプローチの進化を示しました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング (T1566.001)
a. スピアフィッシングメール送信
b. マルウェアの「OneDrive」リンク使用
2. [実行] ユーザー実行 (T1204.002)
a. クリックイベントでマクロ実行
b. マルウェアの「Excel」ファイルドロッパーとして動作
3. [持続性] ブートまたはログオン自動開始実行 (T1547)

NSHC©2025 All rights reserved.

   a. 「NOOPDOOR」持続性確保
4. [防御回避] DLL サイドローディング (T1574.002)
   a. 「DLL サイドローディング」技法使用
5. [コマンド＆コントロール] 暗号化チャネル (T1573)
   a. 暗号化された通信チャネル使用
   b. 「DNS over HTTPS」(DoH) 活用
6. [探索] システム情報探索 (T1082)
   a. 「tasklist」コマンド実行
   b. 「net localgroup」コマンド実行
7. [収集] ローカルシステムからのデータ (T1005)
   a. ローカルシステム情報収集
8. [実行] コマンドおよびスクリプトインタープリター (T1059)
   a. 「Beacon Object Files」メモリ内実行

25) SectorB95 Used DUNLOADER Malware in Southeast Asia Campaign (2025-04-25)

https://cti.nshc.net/events/view/14785

攻撃対象産業群: 通信、政府・行政

SectorB95 グループは最近、東南アジアの政府および通信産業を対象としたキャンペーンで、さまざまなマルウェアを配布しました。該当グループは脆弱性を利用してマルウェアをインストールしたと分析されています。このハッキンググループは不正アクセスを通じてターゲットシステムを損傷した後、複数のドメインおよび IP アドレスを活用してコマンド＆コントロール（Command and Control, C2）チャネルを構築しようと試みました。彼らは「MORIYA」や「KMLOG」といった高度なバックドアを使用して長期間の持続性を確保し、セキュリティ検出を回避したと分析されています。攻撃は主にこれらのバックドアを中心とした侵入ベクターを通じて行われ、損傷した C2 インフラを基にシステム内で不正行為を行い、機密データを窃取しました。また、マルウェア配布過程で高度な技術を駆使し、プロセスインジェクションおよびコード難読化技法を適用することで、セキュリティソリューションの検出を効果的に回避したと見られます。

[Attack Flow]

1. [初期アクセス] スピアフィッシング (T1566)
   a. 詐欺的なメール送信
   b. マルウェア添付ファイルを含む
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. スクリプトを通じたマルウェア実行
   b. リモートコマンド実行

NSHC©2025 All rights reserved.

3. [持続性] バックドアのインプラント (T1547)
   a. "MORIYA"、"KMLOG" などを通じて持続性維持
   b. システム再起動後も持続性確保
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. 脆弱性の悪用
   b. 管理者権限の取得
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. ファイルの難読化
   b. コードの難読化
6. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. 資格情報の抽出
   b. システムデータへのアクセス
7. [探索] システム情報の探索 (T1082)
   a. システム環境情報の収集
   b. ネットワーク構成の把握
8. [横移動] リモートサービス (T1021)
   a. リモートサービスを通じた移動
   b. ネットワーク内部の拡張
9. [収集] ローカルシステムからのデータ (T1005)
   a. ローカルシステムからのデータ収集
   b. 重要ファイルの収集
10. [コマンドとコントロール] C2 通信 (T1071)
    a. 侵害された C&C サーバーとの通信
    b. ネットワークトラフィックの隠蔽
11. [流出] 外部ネットワークへのデータ転送 (T1048)
    a. 外部ネットワークへのデータ送信
    b. 機密データの窃取

26) SectorC01 used XSS Exploits on Webmail for Data Theft (2025-05-15)
https://cti.nshc.net/events/view/15375
攻撃対象産業群: 防衛、軍事機関

SectorC01 ハッキンググループは、2023 年から 2024 年にかけて東ヨーロッパを含む世界中の高価値なウェブメールサーバーを標的とした高度なサイバー諜報作戦を展開しました。彼らは「Roundcube」、「Horde」、「MDaemon」、「Zimbra」など広く使用されているウェブメールソフトウェアのセキュリティ脆弱性を悪用し、公開された XSS 脆弱性だけでなくゼロデイ脆弱性も

NSHC©2025 All rights reserved.

活用して、Malware JavaScript をシステム内部に挿入する方法で侵入を試みました。主な攻撃目的は、メールアカウントへの継続的なアクセス権を確保することによる機密情報の収集であり、特にウクライナ紛争に関連する政府機関や防衛産業などの組織が集中的なターゲットとなりました。彼らは「Roundcube」の CVE-2023-43770 および「MDaemon」の CVE-2024-11182 のような脆弱性を積極的に活用し、これを通じて資格情報の窃取、メール本文および添付ファイルの流出、二要素認証の回避など高度な侵害行為を行うことができました。攻撃に使用されたペイロードは、ウェブメールプラットフォームごとの特性を反映した 4 つの JavaScript モジュールで構成されており、各モジュールはアカウント情報の窃取およびメール収集機能を果たすように設計されていました。これらの Malware スクリプトは、正常なメールに偽装されたメッセージ内部に挿入された形で配信され、受信者がメールを開く瞬間に自動的に実行されて被害者のセッション情報を収集しました。窃取された情報は、暗号化された HTTP POST リクエストを通じてコマンド＆コントロール（Command and Control）サーバーに送信され、この過程はウェブトラフィック内で正常な通信に偽装されて検出を困難にしました。

[Attack Flow]

1. [リソース開発] インフラストラクチャの取得: ドメイン (T1583.001)
   a. ドメイン購入
   b. サーバーレンタル
2. [リソース開発] 能力の開発: エクスプロイト (T1587.004)
   a. XSS 脆弱性の開発
   b. JavaScript スティーラーの開発
3. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. Web メールソフトウェアの XSS 脆弱性の悪用
   b. マルウェアメールの送信
4. [実行] クライアント実行のためのエクスプロイト (T1203)
   a. Web メールクライアントページでの JavaScript コードの実行
   b. メール確認時にマルウェアの実行
5. [防御回避] ファイルまたは情報の難読化 (T1027)
   a. JavaScript ペイロードの難読化
   b. 文字列および URL の暗号化
6. [資格情報アクセス] 強制認証 (T1187)
   a. ユーザーログアウトの誘導
   b. 偽のログインページの表示
7. [資格情報アクセス] 認証プロセスの変更: 多要素認証 (T1556.006)
   a. 2FA トークンの奪取
   b. アプリケーションパスワードの生成

NSHC©2025 All rights reserved.

8. [探索] アカウント探索: メールアカウント (T1087.003)
    a. メールアカウント情報の収集
    b. 連絡先リストの照会
9. [収集] 入力キャプチャ: ウェブポータルキャプチャ (T1056.003)
    a. 隠されたログインフォームの作成
    b. ブラウザおよびパスワードマネージャーの欺瞞
10. [収集] 自動収集 (T1119)
    a. 資格情報およびメールメッセージの自動収集
    b. 大量メールの収集
11. [収集] メール収集: リモートメール収集 (T1114.002)
    a. メールのリモート収集
    b. メールメッセージの漏洩
12. [収集] メール収集: メール転送ルール (T1114.003)
    a. メール転送ルールの追加
    b. ハッキンググループ制御のメールへの転送
13. [コマンド＆コントロール] アプリケーション層プロトコル: ウェブプロトコル (T1071.001)
    a. HTTPS を通じて C&C サーバーと通信
    b. HTTP POST リクエストの使用
14. [コマンド＆コントロール] アプリケーション層プロトコル: メールプロトコル (T1071.003)
    a. メール転送を通じた漏洩
    b. メールプロトコルの活用
15. [データ流出] 自動流出 (T1020)
    a. 資格情報およびメールメッセージの自動流出
    b. C&C サーバーへのデータ送信
16. [データ流出] C2 チャネルを介した流出 (T1041)
    a. C&C チャネルを通じたデータ流出
    b. 暗号化されたデータの送信

27) SectorC14 used LOSTKEYS Malware disguised as Maltego Software (2025-05-08)

https://cti.nshc.net/events/view/14985

攻撃対象産業群: 政府・行政、軍事機関、非政府組織(NGO)、ジャーナリスト、シンクタンク

SectorC14 グループは、「ロストキーズ（LOSTKEYS）」という新しい Malware を 2025 年初頭に配布しました。この Malware は、偽の CAPTCHA があるウェブサイトを通じて多段階感染チェーンを開始します。感染は、ユーザーが偽の CAPTCHA を認証した後、クリップボードにコピーされた PowerShell スクリプトを実行する際に始まります。このスクリプトは後続のステップを取得し、デ

NSHC©2025 All rights reserved.

バイスごとの MD5 ハッシュを確認する手法で検出を回避します。最終段階は、ロストキーズという Visual Basic Script 形式の Malware で、機密ファイル、システム情報、および実行中のプロセスを盗む機能を備えています。このグループは主に NATO 政府の管理者、西側政府の顧問団、およびウクライナ関連の人物を含む高位の人物を対象に、資格情報フィッシングおよびデータ窃取活動を行っています。2023 年 12 月に遡るいくつかの亜種は、ソフトウェアパッケージに偽装した PE 形式のファイルを使用しました。これらのオペレーションの主な目的は、戦略的目的のための情報収集であると見られます。COLDRIVER は、高位の人物の個人メールアドレスまたは非政府組織（NGO）のアドレスを主に攻撃し、アカウントにアクセスした後、メールと連絡先リストを盗みます。彼らは特定のケースで Malware を攻撃対象システムに投入することもあります。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 偽の CAPTCHA ウェブサイトの活用
   b. ユーザーに悪性 PowerShell スクリプトを実行させる誘導
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. PowerShell スクリプトの実行
   b. 後続ステップのダウンロードと実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. デバイス別の MD5 ハッシュ確認
   b. 仮想マシン検出技術の適用
4. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. Visual Basic Script で持続的実行を設定
   b. システム再起動時の実行維持
5. [収集] ローカルシステムからのデータ (T1005)
   a. 機密ファイルの窃取
   b. システム情報およびプロセスの収集
6. [流出] C2 チャネルを介したデータ流出 (T1041)
   a. 収集されたデータを C2 サーバーに送信
   b. 継続的なデータ窃取の試み

28) SectorC30 used OAuth Phishing Impersonating EU Officials (2025-04-22)

https://cti.nshc.net/events/view/14591

攻撃対象産業群: 政府・行政、非政府組織(NGO)

SectorC30 グループは、2025 年 3 月から Microsoft OAuth 2.0 認証ワークフローを悪用した巧妙なフィッシングキャンペーンを展開しました。この作戦は、ウクライナおよび人権関連分野の個人お

NSHC©2025 All rights reserved.

よび組織を主なターゲットとし、グループは Signal や WhatsApp などのメッセージアプリケーションを利用してヨーロッパ諸国の政治関係者を装い、被害者との一対一の接触を試みました。ソーシャルエンジニアリングに基づくアプローチを通じて、被害者に Microsoft OAuth 認証コードの共有を促し、グループはそのコードを利用して Microsoft 365 アカウントへの不正アクセス権を取得することができました。特に、グループは Visual Studio Code 環境およびデバイス登録メカニズムを活用して Microsoft OAuth インフラを悪用し、ユーザー認証手続きを正常なワークフローに偽装して攻撃の隠密性を強化しました。この過程は、多段階の相互作用を基に被害者の信頼を徐々に確保した後、敏感な認証情報を収集する方法で進行し、ユーザー自身がセキュリティ手続きを回避するように仕向ける高度なソーシャルエンジニアリング技術が適用されました。彼らはウクライナ、ブルガリア、ルーマニアなどの外交代表団を装い、Microsoft 365 公式ログインポータルに似たフィッシングサイトを配布し、被害者がログインするように誘導しました。また、彼らは実際のウクライナ政府所属の合法アカウントを乗っ取り、そのアカウントから攻撃メッセージを送信し、被害者の Microsoft Entra ID 環境に悪性デバイスを登録することで長期的なアクセスを試みました。これらの手法は、認証回避のための追加のソーシャルエンジニアリング戦術と組み合わされ、二要素認証手続きを無力化したり、被害者が直接それを無視するように誘導しました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 「Signal」と「WhatsApp」を通じてヨーロッパの政治関係者を装う
   b. 「Microsoft 365」ログインポータルに接続するフィッシング URL を送信
2. [実行] ユーザー実行 (T1204)
   a. 被害者がフィッシング URL をクリック
   b. 「Microsoft OAuth」コード収集のためのインタラクションを誘導
3. [資格情報アクセス] ファイル内の資格情報 (T1081)
   a. 「Microsoft OAuth」認証コードを要求
   b. コード収集後にアクセストークンを生成
4. [持続性] アカウント操作 (T1098)
   a. 「Microsoft Entra ID」に新しいデバイスを登録
   b. 持続的なアクセスのためのデバイス登録
5. [防御回避] 防御の無効化 (T1562)
   a. 正当な「Microsoft」サービスを利用してセキュリティソリューションを回避
   b. ハッキンググループの行為が検出されないように OAuth ワークフローを悪用
6. [収集] メール収集 (T1114)
   a. 「Microsoft Graph API」を通じてメールデータをダウンロード
   b. 「Outlook」および「Teams」データにアクセス
7. [コマンド＆コントロール] 暗号化されたチャネル (T1573)

NSHC©2025 All rights reserved.

a. 「Signal」と「WhatsApp」を通じた継続的な通信
b. 暗号化されたメッセージでフィッシングキャンペーンを操作

29) SectorD01 used SSH Key Reuse and Fake Domains to Impersonate Firms (2025-04-22)

https://cti.nshc.net/events/view/14609

攻撃対象産業群: 政府・行政、通信、教育、エネルギー、非政府組織(NGO)

SectorD01 グループは、2024 年 11 月から 2025 年 4 月の間に、イラク内の学術機関および架空の英国拠点の技術会社を装うためのマルウェアインフラを構築しました。この期間中に多数の新規ドメインとサーバーが設定され、このインフラは本格的な作戦開始前の段階で事前運用準備の兆候を明確に示しました。特に、共有 SSH キーの繰り返し使用、類似した SSH フィンガープリント、誘引 HTTP 応答パターンの再利用などは、一貫した設定戦略を反映しており、これは過去にこのグループが使用した初期インフラの特性と類似した形で観察されました。一部のサーバーはポート 8080 で「404 Not Found」メッセージを意図的に返すように構成されており、これは一般的なエラーページのように偽装して検出を回避すると同時に、外部の分析者の収集活動に混乱を誘導する戦術と解釈されます。この戦術は、彼らが過去に使用した「偽 404 応答」技法と一致する様相を示しています。ドメインの一つである biam-iraq[.]org は、当初 Host Sailor のインフラでホスティングされていましたが、その後ルーマニア拠点の M247 Europe SRL 所属の IP に転換され、これと類似した.eu ドメインも同じ M247 系列の IP アドレスに接続されました。これらのドメインは長期間非活性状態を維持していましたが、メールサーバー設定や証明書発行履歴、サーバー応答ログなどを基に分析すると、フィッシングおよび資格情報収集作戦のための事前インフラとして機能した可能性が提起されます。ほとんどのドメインは P.D.R. Solutions LLC を通じて登録され、Let's Encrypt 証明書を使用して暗号化通信をサポートするように設定されました。これと共に、このグループはストックイメージと一貫性のないブランドアイデンティティを活用してウェブサイト上でマーケティングまたはソフトウェア開発企業として偽装し、これを通じてドメインおよびインフラの合法性を付与する戦略を使用しました。

[Attack Flow]

1. [偵察] 被害者ネットワーク情報の収集 (T1590)
   a. イラクの学術機関を装う
   b. 英国拠点の仮想企業を装う
2. [リソース開発] インフラの取得 (T1583)
   a. ドメインの登録と管理
   b. IP 変換と運用準備
3. [初期アクセス] フィッシング (T1566)

NSHC©2025 All rights reserved.

a. ドメインを通じたフィッシング準備
b. 資格情報収集のためのインフラ構築
4. [コマンド＆コントロール] 非標準ポート (T1571)
a. ポート 8080 の使用
b. 偽の 404 応答の提供
5. [防御回避] ホスト上のインジケーター削除 (T1070)
a. SSH キーの再利用
b. 一貫した HTTP 動作パターンの使用

30) SectorD02 used Avast-themed Phishing Email to Deploy ScreenConnect Malware (2025-04-29)

https://cti.nshc.net/events/view/14698

攻撃対象産業群: IT、民間

SectorD02 ハッキンググループは、イスラエルの企業と個人を標的にした精巧に設計されたサイバーキャンペーンを実施したことが判明しました。この攻撃は、Avast アンチウイルス購入確認書を装ったフィッシングメールを通じて開始され、被害者が専門的に作られたブランディング、偽の請求書、そしてダウンロードリンクが含まれたメールとやり取りすることで侵害が引き起こされました。メールに含まれるリンクは多段階リダイレクトチェーンを経て、最終的に GitHub から偽の「Avast.exe」ファイルをダウンロードするよう誘導しました。この実行ファイルは、作動時に対象がイスラエルのユーザーであることを確認した後、「ScreenConnect」を含む複数のマルウェア構成要素をシステムにドロップします。その後、システム設定を変更して持続性を確保し、特定のドメイン名に基づいてコマンド＆コントロール（Command and Control）サーバーと暗号化された通信チャネルを構築しました。本キャンペーンでは、Windows 認証パッケージの操作、ScreenConnect ベースのリモートアクセスなどの高度な技術が投入され、ハッキンググループが感染したシステムに対して広範な制御権を確保することができました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
a. Avast 購入確認書に偽装したフィッシングメール送信
b. 偽の請求書およびダウンロードリンクを含む
2. [実行] ユーザー実行 (T1204)
a. ユーザーが「Avast.exe」ファイルをダウンロードおよび実行
b. 環境確認後に Malware コンポーネントをドロップ
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
a. Windows サービスの作成

NSHC©2025 All rights reserved.

b. システム設定の修正
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. サイレントインストール引数の使用
b. 認証パッケージ登録の修正
5. [資格情報アクセス] 資格情報ダンピング (T1003)
a. Windows 認証パッケージの修正
b. ScreenConnect を通じたキーストロークロギング
6. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
a. 暗号化された C2 チャネルの設定
b. 特定のドメイン名を利用した通信
7. [影響] データ操作 (T1565)
a. システム復元ポイントの作成
b. システム安定性維持のためのバックアップメカニズムの準備

31) SectorD05 used Fake Site to Impersonate German Model Agency (2025-05-07)

https://cti.nshc.net/events/view/15006

攻撃対象産業群: ジャーナリスト、社会運動団体、反体制団体

SectorD05 グループは、ドイツのモデルエージェンシーを装った偽のウェブサイトを運営し、訪問者の詳細情報を収集する脅威作戦を実行しました。このウェブサイトは、ブラウザのフィンガープリンティング、IP アドレス、その他のデバイス固有のデータを収集するために難読化された「JavaScript」を使用していました。ウェブサイトには、社会工学的攻撃をターゲットにした偽のモデルプロフィールが含まれており、将来の悪意のある活動を示唆する非アクティブなリンクが存在します。該当グループは、WebRTC（Web Real-Time Communication）に基づく IP アドレス漏洩やキャンバスフィンガープリンティングなどの高度な技術を利用して特定の個人を識別し、ターゲットにしました。これらのキャンペーンの複雑さと手法は、海外に拠点を置くイランの反体制派および批判者を対象としたイランのサイバースパイ活動の進化段階を示唆しています。この作戦は、イランの活動家コミュニティに関連する組織や個人に対するリスクの高まりを強調しています。
「megamodelstudio[.]com」ドメインは、偽のウェブサイトのサーバーIP アドレス「64.72.205[.]32」と接続されており、メインページおよび「Shir Benzion」の偽プロフィールページに続く URL を含んでいます。

[Attack Flow]

1. [コレクション] 情報リポジトリからのデータ収集 (T1213)
a. ブラウザフィンガープリントの収集
b. デバイス別データの収集

NSHC©2025 All rights reserved.

2. [資格情報アクセス] ウェブ資格情報の窃取 (T1539)
   a. "WebRTC"を通じた IP アドレスの漏洩
   b. "canvas fingerprinting"を通じたデバイス固有ハッシュの生成
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 難読化された"JavaScript"の使用
   b. データ収集ルーチンの偽装
4. [ソーシャルエンジニアリング] 情報を得るためのフィッシング (T1598)
   a. 偽のモデルプロフィールの使用
   b. 非アクティブリンクを通じたソーシャルエンジニアリング誘導

32) SectorD05 used LNK Files Disguised as Biography PDF to Deploy Trojan (2025-05-07)

https://cti.nshc.net/events/view/14986

攻撃対象産業群: メディア、社会運動団体

SectorD05 グループは 2012 年から活動しているハッキンググループで、最近中東地域を対象にサイバー攻撃を行いました。該当グループは「Biography of Mr.leehu hacohn.lnk」というマルウェアの Windows ショートカット（LNK）ファイルを初期攻撃ベクターとして使用しました。このファイルを実行すると、攻撃対象を混乱させるための PDF ファイルと、複数の DLL および暗号化されたデータファイルを含む ZIP アーカイブが解凍されます。この中の「Wow.dll」ファイルは「regsvr」を通じてマルウェアを実行し、検出を避けるために混乱化技術を使用しました。攻撃は「Base64」と「AES」暗号化を重ねて適用し、「PowerShell」スクリプトを解読してロードする方式で進行され、これは「PowerLess」トロイの木馬を配布してデータを流出させることを目的としていました。「PowerLess」のバージョン 3.3.4 は、テレグラム（Telegram）API を使用してシステム情報を送信し、ファイルリストの照会、コマンドの実行、データの窃取などの命令を実行しました。

[Attack Flow]

1. [初期アクセス] 悪意のある LNK ファイル (T1204.002)
   a. 悪性「LNK」ファイルのクリック誘導
   b. 被害者システムに「PDF」および「zip」ファイルを生成
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. 「regsvr」コマンドで「DLL」を登録および実行
   b. 「PowerShell」スクリプトのロード
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 「Wow.dll」に難読化技法を適用
   b. 「AMSI」および「ETW」の回避

NSHC©2025 All rights reserved.

4. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. 「PowerLess」トロイの木馬の自己実行設定
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. システム情報の収集および送信
6. [コマンドと制御] アプリケーション層プロトコル (T1071)
   a. 「Telegram API」を通じた C2 サーバーとの通信
7. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. 「PowerLess」トロイの木馬を通じたデータの窃取
   b. ファイルリストおよびコマンド実行結果の送信

33) SectorE04 used Word malware disguised as cybersecurity advisories (2025-05-20)

https://cti.nshc.net/events/view/15520

攻撃対象産業群: 銀行、政府・行政、軍事機関

SectorE04 グループは最近、スリランカ、バングラデシュ、パキスタンの政府機関を対象にサイバーキャンペーンを実施しました。このグループは「CVE-2017-0199」と「CVE-2017-11882」の脆弱性を悪用し、スピアフィッシングメールを通じて攻撃対象にマルウェアを含むコンテンツを配信しました。マルウェアを含む Word と RTF 文書を初期感染ベクターとして使用し、これらの文書は多段階攻撃チェーンを通じてシェルコードベースのローダーとサーバーサイドポリモーフィズム（多形性）を利用して検出を回避しました。最終ペイロードとして「スティーラーボット（StealerBot）」を配布し、資格情報の窃取とデータ漏洩を可能にしました。これは諜報活動とサイバー犯罪要素を組み合わせた形態でした。よく知られた Microsoft Office の脆弱性を一貫して使用し、リモートでマルウェアペイロードを実行することができ、これを動的シェルコード注入と DLL サイドローディング技術を通じて配信しました。特に、C2 インフラは頻繁な更新パターンを示し、これは運用成熟度を示しています。今回のキャンペーンは、対象政府環境における古いソフトウェア構成の高いリスクを強調しました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. マルウェアが含まれた Word および RTF 文書の添付
   b. スピアフィッシングメールの送信
2. [実行] クライアント実行のためのエクスプロイト (T1203)
   a. "CVE-2017-0199" 脆弱性の悪用
   b. "CVE-2017-11882" 脆弱性の悪用
3. [防御回避] 難読化されたファイルまたは情報 (T1027)

NSHC©2025 All rights reserved.

a. シェルコードベースのローダー使用
b. サーバーサイドポリモーフィズムの適用
4. [持続性] DLL サイドローディング (T1574.002)
a. DLL サイドローディング技法の使用
b. "TapiUnattend.exe" 実行による持続性の確保
5. [資格情報アクセス] 資格情報ダンピング (T1003)
a. "StealerBot"を通じた資格情報の窃取
b. 情報の窃取および収集
6. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
a. コマンド＆コントロールサーバーとの通信
b. 頻繁な C2 インフラの更新
7. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. 窃取した情報の C2 チャネルを通じた流出
b. 暗号化通信を通じたデータ送信

34) SectorH03 used ClickFix malware disguised as Indian Ministry site (2025-05-05)
https://cti.nshc.net/events/view/14987
攻撃対象産業群: 政府・行政、軍事機関、外交

セクターH03 グループは、インドの「国防省」に関連する偽ブランドを利用してクロスプラットフォームのマルウェアを配布しました。該当グループは、「国防省」の報道資料ポータルを模倣した詐欺ウェブサイトを作成し、マルウェアを配布するために侵害されたドメインを使用しました。このキャンペーンは、ClickFix という手法を通じて Windows と Linux システムの両方を対象としており、これはソーシャルエンジニアリングを利用して悪意のあるペイロードを実行する方式です。Linux ユーザーには CAPTCHA ページを通じて攻撃対象を欺き、クリップボードシェルコマンドを実行させ、侵害されたと見られるドメインからシェルスクリプトをダウンロードしました。Windows では、「For Official Use Only」という警告と共に JavaScript 関数が静かに悪意のある「mshta.exe」コマンドをコピーし、難読化された「.NET」ベースのローダーを配布しました。攻撃インフラは、政府のサブドメインをスプーフィングし、悪意のある活動とよく関連付けられるレジストラサービスを悪用しました。

[Attack Flow]
1. [偵察] フィッシング (T1598)
a. 「国防部」の報道資料ポータルを模倣したウェブサイトの作成
b. 損傷したドメインを利用して Malware を配布
2. [初期アクセス] ドライブバイ妥協 (T1189)

NSHC©2025 All rights reserved.

a. ソーシャルエンジニアリング技法でユーザーのクリックを誘導
b. 「ClickFix」技法を通じて悪性ペイロードを実行
3. [実行] コマンドとスクリプトインタープリター (T1059)
a. Linux の場合、「CAPTCHA」ページを通じてシェルコマンドを実行
b. Windows の場合、「mshta.exe」を通じて悪性コマンドを実行
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. 難読化された「.NET」ベースのローダーを使用
b. JavaScript の難読化を使用して分析を妨害
5. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
a. リモートスクリプト実行を通じた通信
b. ハッキンググループの制御インフラとの接続を維持

35) SectorH03 used Crimson RAT in Pahalgam-themed PDF phishing (2025-04-30)

https://cti.nshc.net/events/view/14745

攻撃対象産業群: 政府・行政、防衛

SectorH03 グループは、インド政府および防衛関連の人物を対象とした精巧なサイバーキャンペーンを発見しました。この作戦は 2025 年 4 月に検出され、パハルガム（Pahalgam）テロをテーマにした文書を使用して、資格情報フィッシングとマルウェアペイロードの配布を含んでいます。該当グループは、ジャンムー＆カシミール警察とインド空軍を装った偽のドメインを通じて攻撃を実行しました。フィッシング文書は、欺瞞的な名前で攻撃対象を誘導し、マルウェア URL にアクセスさせ、これはインドの公式サイトを模倣した偽のログインページに接続されます。アクセス時に資格情報がハッキンググループに送信されます。また、マルウェアマクロが含まれた PowerPoint アドインを通じて「Crimson RAT」ペイロードが実行され、システム制御およびデータの窃取が可能になります。技術的要素としては、ドメインのなりすまし、PPAM ファイルに含まれたマルウェアマクロ、政府通信を模倣した C2 インフラが含まれます。

[Attack Flow]

1. [偵察] 情報を求めるフィッシング (T1598.003)
a. フィッシング文書の作成
b. 偽のログインページの設定
2. [リソース開発] インフラの取得 (T1583.001)
a. 偽のドメイン登録
b. インフラの設定
3. [初期アクセス] フィッシング (T1566.001)

NSHC©2025 All rights reserved.

a. フィッシング文書および URL の送信
b. ユーザーのクリック誘導
4. [実行] ユーザー実行 (T1204.001)
a. フィッシング URL のクリック
b. マクロの実行
5. [持続性] ブートまたはログオン自動開始実行 (T1547.001)
a. レジストリキーを通じた持続性の維持
b. 自動開始フォルダの設定
6. [発見] システム情報の発見 (T1082)
a. システム情報の収集
b. ユーザー情報の収集
7. [収集] ローカルシステムからのデータ (T1005)
a. ローカルシステムデータの収集
b. スクリーンショットの収集
8. [流出] C2 チャネルを介した流出 (T1041)
a. C2 チャネルを通じたデータ送信
b. 情報流出の実行

36) SectorH03 used Crimson RAT Malware disguised as PDFs (2025-05-14)

https://cti.nshc.net/events/view/15474

攻撃対象産業群: 政府・行政

SectorH03 グループは、悪意のある PDF 文書とマクロが挿入された Excel ファイルを利用したフィッシング攻撃を通じて、Crimson RAT（Crimson Remote Access Trojan）を配布しました。このフィッシングキャンペーンは、巧妙なソーシャルエンジニアリング技術に基づいて設計されており、被害者が添付ファイルを開くように誘導し、Malware の初期実行を引き起こします。配布された Crimson RAT は、感染後に被害システムへの継続的なアクセス権を確保し、コマンド＆コントロール（C2）サーバーとの通信を通じて機密情報を窃取します。主な機能には、キーロギング、ファイル収集、オーディオ録音、画面キャプチャなどが含まれ、さまざまな偵察および監視機能が統合されています。この Malware は、自動実行メカニズムを通じて感染後の再起動環境でも持続性を維持し、セキュリティ製品の検出を回避するために難読化された通信プロトコルと暗号化されたペイロード配信方式を使用します。また、RAT 実行前の段階で、ファイルマクロや文書内の埋め込みスクリプトを通じてバックグラウンドで悪意のある行為を隠蔽したまま感染を進行させる方式が特徴です。

[Attack Flow]

NSHC©2025 All rights reserved.

1. [初期アクセス] フィッシング (T1566)
   a. マルウェアの「PDF」ファイル使用
   b. マクロを含む「Excel」ファイル使用
2. [実行] ユーザー実行 (T1204)
   a. ユーザー実行によるマルウェアの活性化
   b. マクロ実行で「Crimson RAT」インストール
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. 持続性維持のための自動開始設定
   b. システム再起動時にマルウェア実行継続
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. ファイルおよびコードの難読化
   b. 検出回避のための暗号化技法使用
5. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. コマンド制御サーバーとの通信
   b. 「CyberChef」を利用した C2 構成
6. [収集] 入力キャプチャ (T1056)
   a. オーディオ録音機能使用
   b. システム情報収集
7. [流出] C2 チャネルを介した流出 (T1041)
   a. 盗まれた情報を C2 チャネルを通じて送信
   b. 敏感情報を外部に流出

37) SectorH03 used Malware disguised as chat app in phishing attack (2025-04-27)

https://cti.nshc.net/events/view/14701

攻撃対象産業群: 航空宇宙、農業、政府・行政、軍事機関

SectorH03 グループは 2023 年 8 月、インドの軍事、農業、航空産業を標的にした高度なサイバースパイキャンペーンを実施しました。このキャンペーンは、Android ベースのマルウェアアプリケーションを安全なチャットソフトウェアに偽装して配布する方法で進められ、「Vibe」という名称のアプリを通じて機密データを収集しました。このアプリはユーザーの疑念を避けるために通常のチャット機能を含んでおり、実際の機能の背後で広範な情報の窃取が行われました。該当グループは Google Play ストアの公式配布ページを模倣したフィッシングサイトを開設し、Vibe アプリを配布して被害者がこれをインストールするよう誘導しました。アプリはインストール後、ユーザーから位置情報、連絡先、テキストメッセージ、通話履歴などのさまざまな機密情報を収集し、チャット活動と共にこれをコマンド＆コントロール（C2）サーバーに送信しました。チャット機能と窃取機能は同じサーバーインフラを共有するように設計されており、正式なアプリのように見える UI と改ざん

NSHC©2025 All rights reserved.

されていない正常動作を通じてユーザーの疑念を最小限に抑えました。特にこのキャンペーンは Firebase リアルタイムデータベースを C2 インフラとして活用し、これを通じて収集されたデータをクラウド環境に保存し、ハッキンググループがリアルタイムでアクセス可能に構成されていました。また、Firebase 内の設定値を通じてアプリの特定機能をリモートで制御したり動作を停止させたりするコマンド機能も実装されており、検出を回避し、隠密な制御が可能になるよう設計されていました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. Google Play ページを模倣したフィッシングサイトの構築
   b. フィッシングサイトを通じてマルウェアアプリ「Vibe」を配布
2. [実行] ユーザー実行 (T1204)
   a. ユーザーがマルウェアアプリをダウンロードおよびインストール
   b. アプリ実行時にデータ窃取機能が有効化
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. アプリインストール時に自動実行設定
   b. 持続的なユーザー監視のための自動化
4. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. Firebase リアルタイムデータベースを使用したコマンド制御
   b. 敏感なデータのリモート送信
5. [収集] ローカルシステムからのデータ (T1005)
   a. 連絡先、通話履歴、SMS の収集
   b. WhatsApp メディアファイルおよび外部ストレージファイルの窃取
6. [流出] C2 チャネルを介したデータ流出 (T1041)
   a. 収集されたデータを C&C サーバーに送信
   b. 新しいアドレスを通じたアプリの自己更新

38) SectorL03 exploited Output Messenger CVE-2025-27920 flaw (2025-05-12)

https://cti.nshc.net/events/view/15249

攻撃対象産業群: IT、政府・行政、通信

SectorL03 グループは 2024 年 4 月から Output Messenger ソフトウェアのゼロデイ脆弱性（CVE-2025-27920）を悪用した標的攻撃を実行しました。彼らはセキュリティパッチが適用されていないユーザーアカウントを中心に攻撃を展開し、主要なターゲットはイラク内のクルド軍関連組織およびインフラであることが確認されました。該当グループは事前段階で Output Messenger ユーザー識別のための偵察を行い、その後ディレクトリトラバーサル脆弱性を利用して OMServerService.vbs

NSHC©2025 All rights reserved.

などのマルウェアスクリプトをサーバーの自動実行ディレクトリにアップロードすることで初期感染を誘導しました。攻撃インフラは DNS ハイジャックとタイプミスドメインベースのフィッシングを組み合わせて資格情報を奪取し再利用し、その後 Go 言語で作成されたカスタムバックドアを通じて追加ペイロードを投入し、内部システムへの拡張を試みました。該当バックドアはコマンド＆コントロール（C2）機能とデータ流出機能を統合しており、システム権限の昇格や内部情報の偵察、非認可アクセス権の確保を含む一連の複合攻撃チェーンを構成しました。この過程で該当グループは Output Messenger サーバーのアーキテクチャを操作してマルウェアスクリプトの持続的実行を保証し、これを基に機密ユーザーデータを奪取することに成功したと推定されます。一方、このキャンペーンに関連して 2 番目の脆弱性である CVE-2025-27921 も発見されましたが、現在までに該当脆弱性が実際に悪用されたという状況は確認されていません。

[Attack Flow]

1. [初期アクセス] 有効なアカウント (T1078)
   a. DNS ハイジャックを通じた資格情報の傍受
   b. タイポドメインを利用したログイン情報の収集
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
   a. "OMServerService.vbs" の実行
   b. "OM.vbs" ファイルの呼び出し
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. マルウェアファイルをサーバーのスタートディレクトリにアップロード
   b. "OMServerService.exe" をビデオディレクトリに保存
4. [資格情報アクセス] アプリケーションアクセス トークンの窃取 (T1528)
   a. ユーザー資格情報の再利用
   b. システムアクセス権の確保
5. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. "api.wordinfos[.]com" を通じたデータ流出
   b. "plink" を使用したデータ送信
6. [影響] データ破壊 (T1485)
   a. GoLang バックドアを通じたシステム操作
   b. ユーザーデータの窃取および改ざんの可能性

39) SectorP02 used Revenge-RAT disguised as Clean New.exe filename (2025-04-21)

https://cti.nshc.net/events/view/14550

攻撃対象産業群: 反政府勢力

NSHC©2025 All rights reserved.

SectorP02 グループは 2024 年 12 月に中東地域の PC を対象とする新しいサンプルで再登場しました。この攻撃は「Clean New.exe」という名前の 32 ビット PE ファイルにマルウェアペイロードを埋め込み、シリアやトルコなど近隣諸国の反体制派を集中的に狙いました。このファイルは VB.NET で作成されており、ペイロードは「Revenge-RAT」リモートコントロールソフトウェアを復号化して実行し、C2 サーバーと接続してコマンドを受信しました。該当グループはバイト置換や動的バインディング（LateBinding）などの動的コード実行技法を使用して検出を困難にしました。
「Revenge-RAT」は情報の窃取、システムコマンドの実行、プラグインのロードなどの作業を可能にしました。ネットワーク情報は RAT の構成にハードコーディングされており、データ収集から自己削除に至るまでの様々な制御コマンドをサポートしていました。

[Attack Flow]

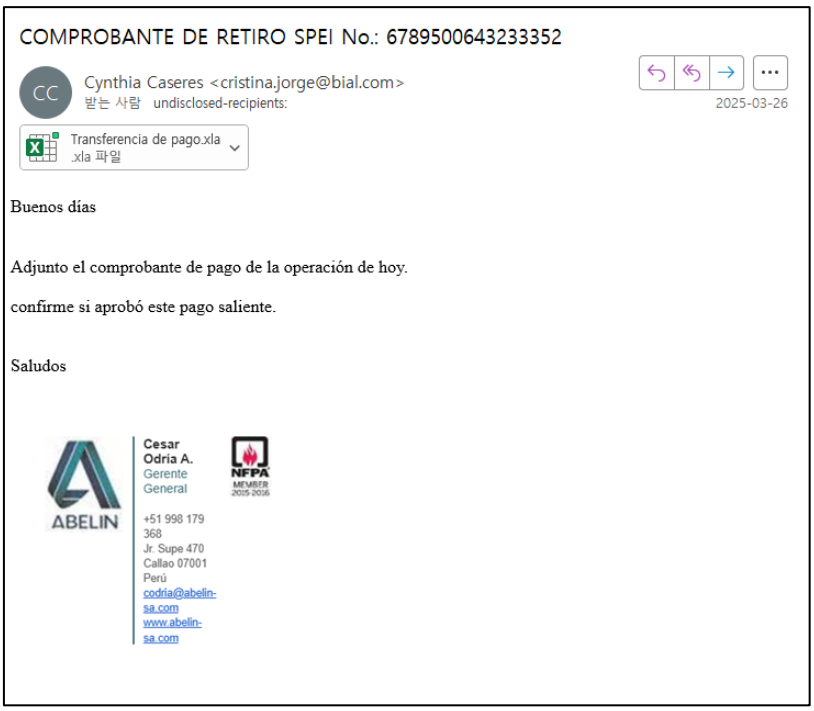
1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. "Clean New.exe" ファイルを通じた添付ファイルの実行
   b. ソーシャルエンジニアリング技法を通じたアクセス誘導
2. [実行] ユーザー実行 (T1204)
   a. ユーザーによるファイル実行の誘導
   b. "Revenge-RAT" の復号化および実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. バイト置換技法の使用
   b. 動的コード実行のための LateBinding の使用
4. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. C2 サーバーとのネットワーク通信
   b. ハードコーディングされた IP アドレスの使用
5. [収集] ローカルシステムからのデータ (T1005)
   a. 情報収集コマンドの実行
   b. システムコマンドの実行および結果の収集
6. [流出] C2 チャネルを介した流出 (T1041)
   a. 収集されたデータの送信
   b. C2 チャネルを通じた情報の窃取
7. [影響] システム回復の妨害 (T1490)
   a. 自己削除コマンドの実行
   b. システム回復の妨害

40) SectorS01 used Agent Tesla for Data Theft and Evasion Techniques (2025-05-14)

https://cti.nshc.net/events/view/15361

NSHC©2025 All rights reserved.

SectorS01 グループは「CVE-2017-0199」脆弱性を悪用して攻撃対象システムを感染させるサイバー脅威活動を行いました。該当グループは「InstallUtil.exe」ユーティリティをターゲットにしたプロセスホローイング技法を使用して悪性活動を隠しました。Malware は「foeMMBIG.txt」というファイルを通じて配信され、このファイルは逆順に変換され、Base64 でデコードされてペイロードを実行します。Agent Tesla はスパイウェアおよびキーロガーとして機能し、毎 60 秒ごとにスクリーンキャプチャを行い、ブラウザ、FTP クライアント、メールソフトウェアなど様々なアプリケーションからデータを窃取できる広範な機能を備えています。データ漏洩はハードコーディングされた資格情報と暗号化されたデータを使用して FTP を通じて行われます。この Malware は 3DES、Rijndael、AES 暗号化を混合して通信を難読化し、検出を回避します。また、仮想マシンとデバッガをチェックするなどの分析抵抗技法を実装しています。Malware はファイルパスと一時ディレクトリを操作して感染したシステムで持続性を維持する回避戦略を使用します。



[図 4: SectorS01 グループが利用したフィッシングメール]

[Attack Flow]

1. [実行] コマンドとスクリプトインタープリター (T1059)
   a. "foeMMBIG.txt" ファイルを逆順変換し、Base64 デコード
   b. "InstallUtil.exe" ユーティリティを使用したプロセスホローイング
2. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. "C:¥Users¥<user>¥AppData¥Roaming¥roSKM¥roSKM.exe" パスで持続性維持
   b. 一時ディレクトリにマルウェアのコピーを移動
3. [防御回避] 難読化されたファイルまたは情報 (T1027)

NSHC©2025 All rights reserved.

a. 3DES、Rijndael、AES 暗号化による通信の難読化
b. 仮想マシンおよびデバッガーの検出
4. [資格情報アクセス] 資格情報ダンピング (T1003)
a. 様々なブラウザおよびアプリケーションから資格情報を収集
b. Discord セッションおよび MFA トークンの収集
5. [収集] スクリーンキャプチャ (T1113)
a. 60 秒ごとに画面をキャプチャ
6. [流出] C2 チャネルを介したデータ流出 (T1041)
a. FTP を通じたデータ流出
b. ハードコーディングされた資格情報の使用
7. [発見] システム情報の発見 (T1082)
a. プロセッサ ID、マザーボードシリアル番号、MAC アドレスの収集
b. オペレーティングシステムおよびパブリック IP アドレスの収集

2. サイバー犯罪（Cyber Crime）ハッキンググループの活動

1) SectorJ09 used Fake GIF Files and new Domains for a FormJacking Attack (2025-04-25)

https://cti.nshc.net/events/view/14695

SectorJ09 グループは、Magento の電子商取引プラットフォームの旧バージョン 1.9.2.4 を対象に高度なフォームジャッキング攻撃を実行しました。彼らはセキュリティパッチが適用されていないシステムを狙い、ユーザーからクレジットカード情報、ログイン資格情報、クッキーなどの機密データを盗むために、さまざまな偽装および回避技術を組み合わせた複合攻撃を展開しました。このグループは、改ざんされた JavaScript コードとマルウェアリバースプロキシサーバー、そして「偽の GIF ファイル」に偽装されたリダイレクトパスを利用しました。特に、悪意のある JavaScript は合法的な分析タグである Bing UET（Bing Universal Event Tracking）に偽装されており、/media/magentothem/img/line.gif?<timestamp>パスを通じてロードされるように構成されていました。このパスには実際に悪意のある PHP スクリプトが含まれており、そのスクリプトはクライアントのリクエストを傍受し、ハッキンググループが制御するリバースプロキシサーバーに送信しました。プロキシサーバーは受信した HTTP リクエストのヘッダーを改ざんすることで検出回避を試み、中間者攻撃の形でデータを盗みました。また、このグループは Magento のチェックアウトページ内のテンプレートファイルを改ざんし、ブラウザの sessionStorage に動的にユーザーごとのユニークキーを挿入し、そのキーが有効化された条件でのみ悪意のあるロジックが実行されるように設計し

NSHC©2025 All rights reserved.

ました。これにより、チェックアウトページに到達したユーザーが気づかないうちにクライアント側で機密データの収集が行われ、ほとんどの悪意のある活動がサーバーではなくユーザーブラウザ環境で行われるため、検出が非常に困難な状態でした。

[Attack Flow]

1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. "Magento" プラットフォームの旧バージョンの脆弱性を悪用
   b. ソリューションの更新およびセキュリティパッチが未適用のシステムを対象
2. [実行] コマンドおよびスクリプトインタープリター (T1059)
   a. "JavaScript" 操作を通じた Malware 実行
   b. "偽の gif ファイル"を通じて Malware "PHP スクリプト"を実行
3. [持続性] リバースプロキシのインプラント (T1098)
   a. Malware "リバースプロキシ" サーバーのインストール
   b. ウェブトラフィックの傍受およびヘッダーの操作
4. [データ流出] 代替プロトコルを介したデータ流出 (T1048)
   a. ユーザーの機密データをハッキンググループのサーバーに送信
   b. "sessionStorage"を利用したデータの窃取
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. "JavaScript" および "PHP" コードの難読化
   b. "Bing UET タグ" 内に Malware を偽装
6. [影響] データ操作 (T1565)
   a. チェックアウトテンプレートファイルの改ざん
   b. ユーザー定義の攻撃トリガーのための動的キーの注入

2) SectorJ47 distributed Backdoor Malware through fake resume sites (2025-05-02)

https://cti.nshc.net/events/view/14991

SectorJ47 グループは、特定の攻撃対象を狙い、高度な技術的手法とツールを駆使して精巧なサイバー攻撃を実行しました。彼らはコードホスティングプラットフォームで合法的に見えるリポジトリを利用し、サプライチェーンをターゲットにした攻撃を通じてマルウェアペイロードを配信しました。攻撃はプログラミングプロジェクトファイル内にトロイの木馬を挿入する方法で行われ、これはコンパイル時に自動実行されるように設計されていました。また、彼らは人気のあるペネトレーションテストツールを武器化し、エクスプロイトプラグインを挿入することで自分たちの活動を隠蔽しました。ハッキンググループは難読化技術とプロセスインジェクション手法を効果的に使用し、隠密性と持続性を強化し、合法的な API を通じてセキュリティ制御を回避して通信しました。これらの高度な

NSHC©2025 All rights reserved.

戦術は、長期的に不正アクセスを維持し、潜在的に攻撃対象システムから機密データを窃取することを目的としていると考えられます。

[Attack Flow]

1. [初期アクセス] サプライチェーンの妥協 (T1195)
   a. 合法的に見えるストレージの活用
   b. マルウェアペイロードの配信
2. [実行] ユーザー実行 (T1204)
   a. トロイの木馬の自動実行
   b. コンパイル時の実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 難読化技術の使用
   b. エクスプロイトプラグインの挿入
4. [防御回避] プロセスインジェクション (T1055)
   a. プロセスインジェクション技術の使用
   b. セキュリティ制御の回避
5. [持続性] DLL サイドローディング (T1073)
   a. DLL ホローイング技術の使用
   b. 持続性の維持
6. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. 合法的な API を通じた通信
   b. セキュリティ制御の回避
7. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. 敏感なデータの窃取
   b. 長期的な不正アクセスの維持

3) SectorJ47 used More_Eggs Malware disguised as job applications (2025-05-17)

https://cti.nshc.net/events/view/15470

SectorJ47 グループが運営する「More_Eggs」マルウェアは、HR 部門を主要な攻撃対象とする JavaScript ベースのバックドアで、Malware-as-a-Service（MaaS）形式で提供されます。このマルウェアは主に採用応募メールを装って配布されます。最近分析されたサンプル「Sebastian Hall.zip」には、デコイ画像と悪意のある Windows ショートカット（LNK）ファイルが含まれており、LNK ファイルを通じてユーザーに Microsoft Word を実行させ、悪意のある動作を隠します。この LNK ファイルはバッチスクリプトを使用してコマンドを実行し、.inf ファイルを生成してエンコ

NSHC©2025 All rights reserved.

ードされた悪意のあるデータを含め、システムファイル「ieuinit.exe」を一時ディレクトリにコピーして悪意のあるパラメータと共に実行します。この過程で難読化された変数名を使用して追加の悪意のあるペイロードをダウンロードするなど、複雑なコード難読化と回避戦略を使用します。分析の結果、合法的なツールと複雑なコード難読化を利用して JavaScript ベースのバックドアをダウンロードおよび実行し、データ窃取と C2 通信を行うことが明らかになりました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. メールを通じて HR 部門を対象に偽装された採用応募書類を配布
   b. ZIP ファイル添付、デコイ画像を含む
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
   a. LNK ファイルを通じて cmd.exe を実行
   b. Microsoft Word を実行してユーザーを欺く
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. バッチスクリプトで難読化されたコマンドを実行
   b. 変数名の難読化で分析を妨害
4. [持続性] システムプロセスの作成または変更 (T1543)
   a. "ieuinit.exe"を一時ディレクトリにコピー
   b. .inf ファイルを作成し、マルウェアパラメータで実行
5. [コマンド＆コントロール] ツールの転送 (T1105)
   a. 難読化された変数名を使用して外部サーバーからペイロードをダウンロード
   b. JavaScript ベースのバックドアを実行し、C2 サーバーとの通信を開始

4) SectorJ47 used Stealer Malware for Credential Theft and Data Exfiltration (2025-05-02)

https://cti.nshc.net/events/view/14782

SectorJ47 グループは 2025 年 1 月から 4 月の間に、2 つの新しいマルウェアファミリーである「TerraStealerV2」と「TerraLogger」を開発しました。「TerraStealerV2」は、ブラウザの資格情報、暗号通貨ウォレットデータ、ブラウザ拡張情報などの機密情報を収集するように設計されています。このマルウェアは「Chrome」の「Login Data」データベースを標的としていますが、最新バージョンの「Chrome」に導入されたアプリケーションバウンド暗号化（ABE）を回避できないため、コードが古いか開発中であることを示唆しています。収集されたデータは、テレグラム（Telegram）とドメイン「wetransfers[.]io」を通じて外部に漏洩されます。配布方法には「LNK」、「MSI」、「DLL」、「EXE」ファイルが含まれ、「regsvr32.exe」や「mshta.exe」といった Windows ユーティリティを活用して検出を回避します。「TerraLogger」はスタンドアロンのキー

NSHC©2025 All rights reserved.

ロガーで、低レベルのキーボードフックを使用してキー入力をキャプチャしますが、データ漏洩機能はなく、初期開発段階にあるモジュールである可能性があります。これら 2 つのマルウェアファミリーは依然として活発に開発中であり、ソーシャルエンジニアリングや信頼できるソフトウェアの悪用を含む様々な戦術を通じて配布されています。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. マルウェアの「LNK」ファイルをメールに添付
   b. マルウェアの「MSI」ファイルをメールに添付
2. [実行] コマンドとスクリプトインタープリタ: Windows コマンドシェル (T1059.003)
   a. 「regsvr32.exe」で「DLL」ファイルを実行
   b. 「mshta.exe」で「LNK」ファイルを実行
3. [持続性] ブートまたはログオン自動開始実行: レジストリ実行キー/スタートアップフォルダ (T1547.001)
   a. スタートアップフォルダに「EXE」ファイルを追加
   b. レジストリの「Run」キーに「DLL」を登録
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. コード難読化
   b. 文字列暗号化
5. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. 「Chrome」の「Login Data」データベースにアクセス
   b. 暗号通貨ウォレットデータの抽出
6. [収集] 入力キャプチャ: キーロギング (T1056.001)
   a. 低レベルキーボードフックのインストール
   b. キーストローク記録ファイルの生成
7. [流出] ウェブサービスを介したデータ流出 (T1567.002)
   a. 「Telegram」を通じたデータ流出
   b. 'wetransfers[.]io'を通じたデータ送信

5) SectorJ49 distributed Malware via phishing emails (2025-04-30)

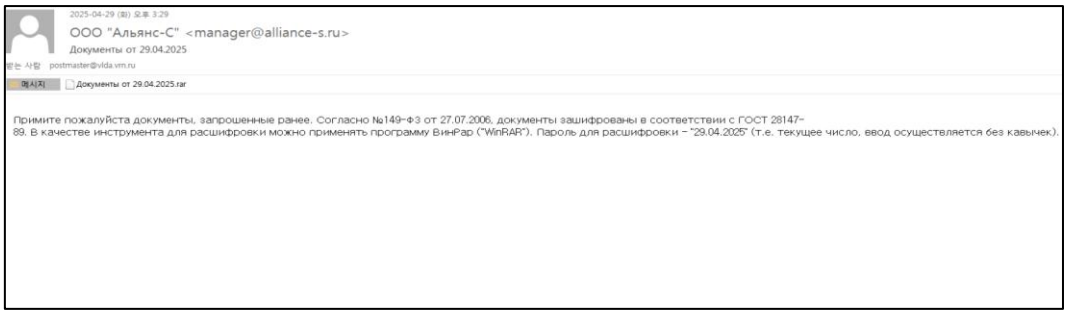
https://cti.nshc.net/events/view/14944

攻撃対象産業群: 金融、製造、通信、観光、エネルギー、運輸、小売、保険、医生命、IT、銀行

SectorJ49 グループは 2025 年 4 月 29 日にロシアの様々な産業を対象に大規模なフィッシングキャンペーンを実施しました。この攻撃はメディア、観光、金融、製造、小売、エネルギー、通信、輸送、バイオテクノロジーなどの産業を狙いました。攻撃者は実在の組織を装ったメールを使用し、

NSHC©2025 All rights reserved.

「Док-ты от 29.04.2025.rar」のような名前のパスワードで保護されたアーカイブファイルを送信しました。このアーカイブファイルには修正された「ダークウォッチマン」Malware が含まれていました。メールは「manager@alliance-s[.]ru」から 550 人以上の受信者に送信されました。このグループは金銭的動機を持つ組織で、2022 年 2 月から活動しています。彼らは「alliance-s[.]ru」のようなドメインを再利用し、以前のキャンペーンで使用された「voenkomat-mil[.]ru」や「absolut-ooo[.]ru」とも関連しています。これらのパターンは既存のリソースを活用しようとする傾向を示しています。添付ファイルを開くと、Malware が従来のセキュリティ対策を回避するためにシステムに展開されます。攻撃対象はロシア、ベラルーシ、リトアニア、エストニア、カザフスタンで特定されました。



[図 5: SectorJ49 グループが利用したフィッシングメール]

[Attack Flow]

1. [戦術] 初期アクセス (T1566)
   a. フィッシングメール送信
   b. パスワードで保護されたアーカイブ添付
2. [戦術] 実行 (T1204)
   a. 添付ファイル実行
   b. "ダークウォッチマン"マルウェア配布
3. [戦術] 防御回避 (T1027)
   a. マルウェア暗号化
   b. 伝統的なセキュリティ対策回避
4. [戦術] 指令と制御 (T1071)
   a. 再利用されたドメインを通じた C2 通信
   b. "alliance-s[.]ru"ドメイン使用
5. [戦術] 永続性 (T1053)
   a. 既存インフラ再利用
   b. 攻撃ドメイン登録および活用

6) SectorJ72 used HTA files to execute its DLL payload (2025-05-06)

NSHC©2025 All rights reserved.

https://cti.nshc.net/events/view/15268

SectorJ72 グループは複雑な感染チェーンを使用しました。最初の段階は、".7z"拡張子を持つ初期の zip アーカイブから始まります。このアーカイブには追加の zip ファイルが含まれており、これを抽出すると"HTA"ファイルが現れます。この"HTA"ファイルは"WebDAV"サーバーから"DLL"を含む".cab"ファイルを取得するように誘導します。実行されると、"DLL"が Malware の配布を容易にします。攻撃は自動検出メカニズムを継続的に回避するために、動的に変化する"WebDAV"サーバーパスを活用してターゲットの".cab"ファイルをダウンロードしました。感染後、このグループは Tor トラフィックを開始し、悪意のある活動に関連する通信を曖昧にします。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1193)
   a. ".7z" 拡張子を持つ初期 zip アーカイブの使用
   b. 攻撃対象システムの関心を引くためのスピアフィッシング添付ファイル
2. [実行] ユーザー実行 (T1204)
   a. ユーザーによる "HTA" ファイルの実行
   b. ハッキンググループの意図に従った "HTA" ファイルからのマルウェア実行
3. [防御回避] 偽装 (T1036)
   a. ".cab" ファイルを通じて正常なファイルに偽装
   b. "WebDAV" パスの頻繁な変更による検出回避
4. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
   a. "Tor" ネットワークを通じた暗号化通信
   b. マルウェア活動の通信を曖昧にして検出回避
5. [持続性] DLL 検索順序ハイジャック (T1574.001)
   a. "Raspberry Robin DLL" を通じた持続性の確保
   b. システム再起動時の自動実行を保証

7) SectorJ119 used Steganographic Techniques to Conceal .Net Payload (2025-04-25)

https://cti.nshc.net/events/view/14676

SectorJ119 グループは、「PNG」ファイル内にマルウェアペイロードを隠すステガノグラフィ技術を使用しました。PNG ファイルは「.Net」形式のバイナリを含んでおり、これはセキュリティツールの検出を回避するために「UTF-16」で難読化されています。マルウェアは反射的コードローディングを利用して、実行中に動的にコードを含めることができました。外部の「URL」から「Bitmap」画像をダウンロードし、ピクセル操作、特に赤色成分の値を通じて隠されたデータを抽出し、2 次ペ

NSHC©2025 All rights reserved.

イロードを再構成しました。このペイロードは抽出後に「PE32」実行ファイルとして現れ、主に悪意のある活動を展開するために使用されます。内蔵されたマルウェアは、コマンド＆コントロールサーバーを使用して追加の作業を行うことが確認されました。主な実行ファイルは「voice_recording.bat」であり、これは「XWorm」系の脅威に属し、高度な難読化およびステガノグラフィ技術を使用して既存の検出方法を回避し、データ漏洩または追加のネットワーク侵害を容易にします。

[Attack Flow]

1. [実行] リフレクティブコードローディング (T1218)
   a. 動的コードを含む
   b. メソッド .Load(), .LoadFrom() の使用
2. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. "UTF-16" 難読化技術
   b. 変数名、関数名の難読化
3. [コマンド＆コントロール] コマンド＆コントロールサーバー (T1071)
   a. コマンド＆コントロールサーバーとの通信
   b. "cryptoghost[.]zapto[.]org" の使用
4. [データ流出] データ流出 (T1041)
   a. データの流出
   b. ネットワーク追加侵害の可能性
5. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. マルウェア "PNG" ファイルの使用
   b. メール添付ファイルとして送信の可能性
6. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. "voice_recording.bat" 実行ファイルの使用
   b. システム起動時の自動実行の可能性
7. [発見] システムネットワーク構成の発見 (T1016)
   a. ネットワーク設定の探索
   b. 追加情報のためのシステム調査
8. [横移動] リモートサービスの悪用 (T1210)
   a. リモートサービスの悪用
   b. ネットワーク内移動の可能性

8) SectorJ149 used Firefox Trojan disguised as mozglue.dll filename for data theft (2025-04-23)

https://cti.nshc.net/events/view/14599

NSHC©2025 All rights reserved.

SectorJ149 グループは最近、高度な多段階トロイの木馬攻撃を実行したと分析されています。彼らの攻撃は主に Windows システムを標的としており、Mozilla Firefox モジュールに偽装して開始されます。このグループは「mozglue.dll」という偽の Firefox ファイルを実行し、システムプロセス「cmd.exe」と「MsBuild.exe」を変更します。トロイの木馬は「MsBuild.exe」にキーロガーを注入してキー入力をキャプチャし、このデータを「%temp%」フォルダに保存して後の漏洩に備えます。攻撃手法には間接的なシステムコール、動的シェルコード、分析防止技術が含まれ、合法的なプロセスに自身を挿入して検出を回避します。持続性を保証するために、スタートアップフォルダに悪性リンクファイルのパスを追加し、メモリ注入を行い、コマンドプロンプトを通じて悪性ペイロードを実行します。第二段階では「cmd.exe」がシステムをさらに操作して感染を維持し、第三段階では「MsBuild.exe」のキーロガーがキー入力を記録し、「Dinamic-Tigo-191-92-96-62[.]tigo[.]com[.]co」のコマンド＆コントロールサーバーにポート 5757 を通じて送信します。これはデータ窃盗および長期的なシステムアクセスを目的としています。

[Attack Flow]

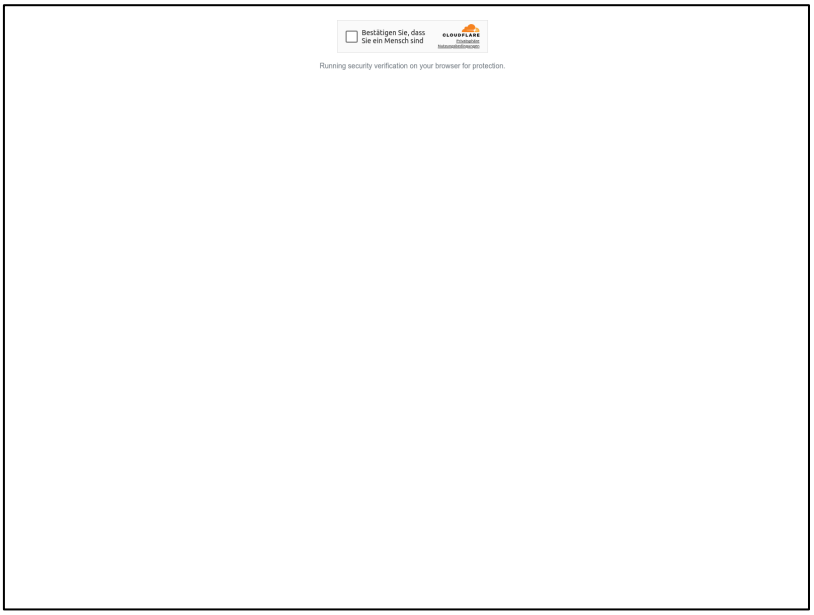
1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. "mozglue.dll"を含むマルウェアファイルの実行
   b. Firefox モジュールに偽装
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
   a. "cmd.exe"を通じたコマンド実行
   b. "MsBuild.exe"へのペイロード注入
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. スタートアップフォルダにマルウェアリンクファイルを追加
   b. システム起動時に自動実行設定
4. [防御回避] プロセスインジェクション (T1055)
   a. 正当なプロセスに自身を挿入
   b. 分析防止技術の使用
5. [資格情報アクセス] 入力キャプチャ (T1056)
   a. キー入力のキャプチャ
   b. "%temp%"フォルダにログを保存
6. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. キャプチャされたキー入力データを C2 サーバーに送信
   b. "Dinamic-Tigo-191-92-96-62[.]tigo[.]com[.]co:5757"に送信

9) SectorJ160 used Phishing Domains powered by Tycoon 2FA (2025-05-14)

https://cti.nshc.net/events/view/15300

NSHC©2025 All rights reserved.

SectorJ160 グループが利用した Tycoon 2FA フィッシングキットは、Microsoft 365 と Gmail の二要素認証（2FA）を回避する点でますます洗練されています。2023 年 10 月に初めて確認されたこのキットは、2025 年までに大幅に進化し、フィッシング・アズ・ア・サービス（PhaaS）モデルを使用しています。該当グループは、攻撃対象が資格情報を入力し 2FA プロセスを完了した後、セッションクッキーをキャプチャしてセッションを再利用できる「中間者攻撃（AiTM）」技法を活用します。フィッシングページを配布するために、該当グループはリバースプロキシサーバーを使用し、これは動的コード生成、難読化、トラフィックフィルタリングを含み、検出を回避します。このキットは、準備されたフィッシングページと直感的な管理パネルを通じて、様々な技術レベルのサイバー犯罪者の間で広く使用されています。[Attack Flow]には、複数の回避ステップが含まれます：初期 URL 難読化、ドメイン確認、偽エラーページリダイレクト。高度な回避技術には、CAPTCHA、ペイロード暗号化、サンドボックス環境を検出する機械学習の統合が含まれます。最新のアップデートは、ブラウザーフィンガープリンティングと CAPTCHA の変形、複雑な難読化および暗号化メカニズムを特徴としており、従来の検出方法に継続的に挑戦しています。



[図 6: SectorJ160 グループが利用したフィッシングサイト]

[Attack Flow]

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
   a. マルウェア URL クリック
   b. 初期 URL 難読化
2. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. コード難読化
   b. "Nomatch" 値比較

NSHC©2025 All rights reserved.

3. [防御回避] ドメインフロント (T1568.002)
   a. ドメイン確認
   b. 偽の "Litespeed 404" エラーページリダイレクト
4. [防御回避] ユーザー実行 (T1204)
   a. CAPTCHA 使用
   b. デバッガタイミング確認
5. [防御回避] コマンド＆コントロール (T1071.001)
   a. C2 サーバーにクエリ送信
   b. GET リクエストおよび応答に基づく進行決定
6. [資格情報アクセス] 入力キャプチャ (T1056.001)
   a. 偽のログインページ提供
   b. ブラウザ検出
7. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. データ暗号化および送信
   b. C2 ドメインへの盗難データ送信
8. [防御回避] ブラウザフィンガープリンティング (T1078)
   a. ブラウザ環境の詳細情報収集
   b. サンドボックス検出および合法サイトへのリダイレクト
9. [防御回避] 暗号化チャネル (T1573)
   a. AES 暗号化使用
   b. ペイロード暗号化/復号化
10. [防御回避] ウェブサービス (T1102)
    a. Google reCAPTCHA 使用
    b. 様々な CAPTCHA バリエーション使用

10) SectorJ172 used Formbook Malware Exploiting CVE-2017-11882 (2025-04-22)

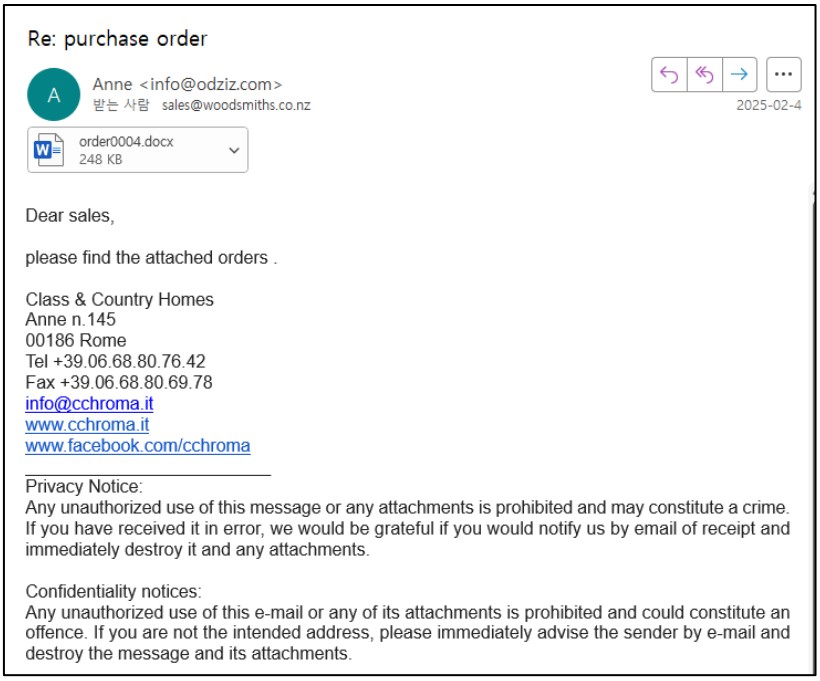
https://cti.nshc.net/events/view/14603

攻撃対象産業群: 製造

SectorJ172 グループは、Windows ユーザーを対象にマルウェアを含む Word 文書をメールで送信し、攻撃を行いました。この文書は「CVE-2017-11882」脆弱性を悪用して「FormBook」マルウェアの亜種を配布します。攻撃は販売注文を装ったメールから始まり、受信者が添付ファイルを開くように誘導します。添付された Word 文書「order0087.docx」は「OOXML」形式で、内部に細工された「RTF」ファイル「Algeria.rtf」を含んでいます。この「RTF」ファイルは「Microsoft Equation Editor」の脆弱性を悪用してバッファオーバーフローを引き起こし、マルウェア「DLL」ファイル「AdobeID.pdf」に偽装されたファイルを実行します。この「DLL」ファイルはシステムの

NSHC©2025 All rights reserved.

一時ディレクトリに抽出され、「FormBook」ペイロードを「PNG」画像ファイルに偽装してダウンロードします。検出を避けるため、ペイロードはプロセスホローイング技法を使用して「Windows フォトビューアー」プロセス（「ImagingDevices.exe」）内で実行されます。マルウェアはレジストリ設定を変更してシステム起動時に自動実行されるように持続性を維持します。この過程で保存されたパスワードやキー入力を含む機密データを窃取し、プロセスインジェクションとファイルレス実行技法の巧妙な使用が際立っています。


Re: purchase order

A Anne <info@odziz.com>
받는 사람 sales@woodsmiths.co.nz
2025-02-4

order0004.docx
248 KB

Dear sales,

please find the attached orders .

Class & Country Homes
Anne n.145
00186 Rome
Tel +39.06.68.80.76.42
Fax +39.06.68.80.69.78
info@cchroma.it
www.cchroma.it
www.facebook.com/cchroma

Privacy Notice:
Any unauthorized use of this message or any attachments is prohibited and may constitute a crime. If you have received it in error, we would be grateful if you would notify us by email of receipt and immediately destroy it and any attachments.

Confidentiality notices:
Any unauthorized use of this e-mail or any of its attachments is prohibited and could constitute an offence. If you are not the intended address, please immediately advise the sender by e-mail and destroy the message and its attachments.

[Figure 7: SectorJ172 グループが利用したフィッシングメール]

[Attack Flow]

1. [実行] メールを介したフィッシング (T1566.001)
   a. ユーザーを欺くための販売注文に偽装したメールを送信
   b. マルウェア「Word」文書「order0087.docx」を添付してメール送信
2. [実行] クライアント実行のためのエクスプロイト (T1203)
   a. 「CVE-2017-11882」脆弱性を含む「RTF」ファイルを実行
   b. バッファオーバーフローを通じて「DLL」ファイル「AdobeID.pdf」を実行
3. [防御回避] プロセスホローイング (T1055.012)
   a. 「FormBook」ペイロードを「ImagingDevices.exe」プロセスに注入
   b. ファイルレス方式でメモリ内のみで実行
4. [持続性] レジストリ実行キー/スタートアップフォルダ (T1547.001)
   a. レジストリキー「HKCU¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run」を修正
   b. 「AdobeID.pdf」の自動実行を通じて持続性を確保
5. [資格情報アクセス] 入力キャプチャ (T1056)

NSHC©2025 All rights reserved.

a. キー入力記録を通じて機密情報を収集
b. 保存されたパスワードなどの資格情報を窃取
6. [収集] ローカルシステムからのデータ (T1005)
a. システムクリップボードおよびスクリーンショットデータを収集
b. 様々なソフトウェアから保存された資格情報を収集
7. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
a. 暗号化された通信チャネルを通じて C2 サーバーと通信
b. 「FormBook」ペイロードの暗号化および復号化過程を実行

11) SectorJ173 used Malware to mine cryptocurrency (2025-04-29)

https://cti.nshc.net/events/view/14719

最近、SectorJ173 グループが Linux 環境を対象に Perl ベースの暗号通貨マイニングボットネットを利用した攻撃活動を行っています。該当グループは脆弱に設定された SSH 資格情報を悪用して不正アクセスを試み、疑わしいアカウントと関連付けられた不正な SSH キーを利用して初期侵入を開始します。その後、「tddwrt7s.sh」スクリプトをダウンロードして実行し、「dota.tar.gz」ファイルをダウンロードして解凍し、「XMRig」の修正版を配布して Monero 暗号通貨をマイニングする方法です。この過程で CPU リソースを過度に使用し、隠蔽技術を使用して隠しディレクトリを通じて持続性を維持します。また、IRC ベースのボットネットクライアントを通じて DDoS 攻撃やデータ漏洩などの追加コマンドを実行することができます。

[Attack Flow]

1. [実行] コマンドとスクリプトインタープリター: Unix シェル (T1059.004)
a. "wget" または "curl" を使用してスクリプトをダウンロード
b. "dota.tar.gz" ファイルをダウンロードして解凍
2. [持続性] アカウント操作: SSH 認証キー (T1098.004)
a. 既存の SSH 設定を削除し、新しい公開鍵を追加
b. SSH アクセス権限の設定とディレクトリ権限の設定
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. Base64 エンコードと Perl スクリプトの難読化
b. 隠しディレクトリの作成と使用
4. [コマンドと制御] アプリケーション層プロトコル (T1071)
a. ハードコーディングされた IRC サーバーに接続
b. ランダムに生成されたニックネームでチャンネルに参加
5. [影響] リソースハイジャック (T1496)
a. Monero 暗号通貨のマイニング

NSHC©2025 All rights reserved.

b. 高い CPU 使用率の設定

6. [発見] システム情報の発見 (T1082)

a. 実行中のプロセスの監視

b. 40%以上の CPU を使用するプロセスの検出と管理

12) SectorJ175 used DragonForce Ransomware (2025-05-02)

https://cti.nshc.net/events/view/14941

攻撃対象産業群: 健康、政府・行政、小売、弁護士

SectorJ175 グループは最近、イギリスの主要小売業者を対象にランサムウェア攻撃を行い、「Harrods」、「Marks and Spencer」、そして「Co-Op」を含む複数の大企業に深刻なサービス中断を引き起こしました。これにより、決済システム、在庫管理、給与などの主要なビジネス機能に影響を与えました。このグループは 2023 年 8 月にマレーシアで始まり、当初は政治的動機から出発しましたが、次第に金融的動機に変化しました。攻撃対象システムへの初期アクセスは主にフィッシングメールと「Apache Log4j」および「Ivanti Connect Secure」の既知の脆弱性を悪用して行われます。ハッキンググループは「Cobalt Strike」と「mimikatz」などのツールを活用し、資格情報詐取攻撃と「RDP」サービスの脆弱性に重点を置いています。このグループのランサムウェアは「LockBit」コードから始まり、「Conti v3」ベースの独自の変種に発展し、「AES」と「ChaCha8」暗号化を特徴としています。また、さまざまなプラットフォームでカスタムペイロード管理のためのアフィリエイトパネルを提供し、「Windows」と「Linux」を含む複数の環境で運用されています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)

a. フィッシングメールを通じた初期アクセス

b. 資格情報の窃取試行

2. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)

a. "Apache Log4j" の脆弱性利用

b. "Ivanti Connect Secure" の脆弱性悪用

3. [実行] コマンドおよびスクリプトインタープリタ (T1059)

a. "Cobalt Strike" を通じたコマンド実行

b. "mimikatz" を使用した資格情報の窃取

4. [持続性] ブートまたはログオン自動開始実行 (T1547)

a. 持続性のための "SystemBC" バックドア配布

b. リモート管理ツールの設定

5. [資格情報アクセス] 資格情報ダンピング (T1003)

a. "mimikatz" を使用した資格情報のダンプ

NSHC©2025 All rights reserved.

b. "Advanced IP Scanner" でのネットワーク探索
6. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. ペイロードの暗号化および偽装
b. 'ホワイトラベル' サービスでのランサムウェア偽装
7. [影響] 影響のためのデータ暗号化 (T1486)
a. "AES" および "ChaCha8" 暗号化の使用
b. ファイルシステムおよび "ESXi" 環境のデータ暗号化
8. [データ流出] Web サービスを介したデータ流出 (T1567)
a. "MEGA" を通じたデータ窃取
b. "WebDAV" および "SFTP" 転送の使用
9. [コマンド＆コントロール] Web サービス (T1102)
a. "SOCKS5" トンネリングのための "SystemBC" 使用
b. リモートサーバーとの通信設定

13) SectorJ197 used new Domains for NodeJS Backdoor (2025-04-29)

https://cti.nshc.net/events/view/14723

SectorJ197 グループは、「KongTuke」、「Fake CAPTCHA」、「Mispadu」、「Lumma stealers」キャンペーンで偽の CAPTCHA 確認を悪用した悪性キャンペーンを実行しました。これらのキャンペーンは、ユーザーを「NodeJS」ベースのバックドアを実行するよう誘導し、従来の PE 構造のレガシーリモートアクセス型トロイの木馬（RAT）に似た高度な「NodeJS」RAT を展開しました。侵入は、悪性「NodeJS」スクリプトがハッキンググループが制御するインフラと接続を確立することから始まり、追加コンポーネントの配布命令を待ちながら待機状態を維持します。
「SOCKS5」プロキシと XOR 暗号化を使用する「NodeJS」RAT の亜種も発見されました。初期アクセスベクターとしては、改ざんされたウェブサイトが使用され、ソーシャルメディアリンクを通じてユーザーを悪性サイトにリダイレクトし、このサイトには悪性「JavaScript」コードが注入されます。コードは、モジュールのロード、データ収集（オペレーティングシステム、IP、ブラウザ情報）、およびその後の偽 CAPTCHA の実行を含みます。「NodeJS」スクリプトは、複数の回避戦術と VM 防止措置を含み、システム偵察と RAT 機能を備えた「NodeJS」バックドアを展開します。RAT は、隠密な通信のために「SOCKS5」プロキシを使用し、レジストリの修正によって持続性を維持するメカニズムを含みます。コマンド＆コントロール（C2）活動は、持続性、実行、ペイロード配信、XOR 暗号化メカニズムを使用したステルスをサポートし、これらのキャンペーンの技術的洗練と進化する戦術を強調します。

[Attack Flow]

NSHC©2025 All rights reserved.

1. [初期アクセス] コンテンツ注入 (T1659)
   a. 注入されたマルウェアの JavaScript コード
   b. ソーシャルメディアリンクを通じたリダイレクト
2. [実行] コマンドおよびスクリプトインタープリター (T1059)
   a. "PowerShell" コマンドの実行
   b. "NodeJS" ベースのバックドアの実行
3. [持続性] システムプロセスの作成または変更 (T1543)
   a. レジストリエントリの追加
   b. 持続性のためのスケジューリング
4. [防御回避] 仮想化/サンドボックス回避 (T1497)
   a. 準仮想化技術の検出
   b. 低メモリ環境の検出
5. [探索] システム情報の探索 (T1082)
   a. オペレーティングシステム情報の収集
   b. ネットワーク構成情報の収集
6. [コマンド＆コントロール] 暗号化チャネル (T1573)
   a. XOR 暗号化の使用
   b. "SOCKS5" プロキシを通じた通信
7. [データ流出] ツールの転送 (T1105)
   a. C2 サーバーへのデータ送信
   b. 追加ペイロードのダウンロードと実行

14) SectorJ197 used Phishing Email Leading to MintsLoader Infection (2025-05-13)
https://cti.nshc.net/events/view/15297

SectorJ197 グループの今回のフィッシングキャンペーンは、「certificado de titularidad bancaria.msg」という件名のフィッシングメールを通じて「MintsLoader」マルウェア感染を誘導しました。メールには「certificado_titularidad_bancaria」という名前の ZIP ファイルが添付されており、複数の JavaScript ファイルと関連付けられていました。これらの JS ファイルは「/1.php?s=[campaign]」形式の URL でネットワーク行動パターンを示し、キャンペーン識別子として「flibabc12」が使用されました。ドメイン「glmhhdcmgcfddbk[.]top」は IP アドレス 185[.]250.151.155 に解決され、これは以前に使用された脅威インジケーターと関連する複数のマルウェアファイルと結びついています。5 月に分析されたマルウェア JS ファイルのうち、少なくとも 21 個が同じ IP に関連付けられ、識別されたインフラを継続的に悪用していると分析されています。

NSHC©2025 All rights reserved.

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. "certificado de titularidad bancaria.msg" フィッシングメール送信
   b. "certificado_titularidad_bancaria" ZIP ファイル添付
2. [実行] ユーザー実行 (T1204)
   a. ZIP ファイルのダウンロードと解凍
   b. JavaScript ファイルの実行
3. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. "/1.php?s=[campaign]" 形式の URL に接続
   b. "flibabc12" キャンペーン識別子の使用
4. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. 持続的な接続のためのインフラ再利用
   b. IP アドレス 185[.]250.151.155 への持続的接続
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. JavaScript ファイルの難読化
   b. フィッシングメールおよび添付ファイルの偽装

15) SectorJ206 used AWS Access Key to Create 'Persistence-as-a-Service' (2025-05-13)

https://cti.nshc.net/events/view/15308

SectorJ206 グループは、漏洩した長期 AWS アクセスキーを利用して、150 分間にわたり 5 つの IP アドレスを通じて攻撃対象システムに悪意のある活動を行いました。この攻撃は、一般的かつ革新的な戦術を両方活用しました。注目すべき技術としては、「API ゲートウェイ」と「ラムダ(Lambda)関数」を使用して「サービスとしての持続性(persistence-as-a-service)」を作成し、資格情報が撤回された後でも IAM ユーザーを動的に生成できる機能が含まれていました。ハッキンググループの行動は、テレグラム IP アドレスでの異常な「コンソールログイン(ConsoleLogin)」イベントを通じて、テレグラムボットを介した自動化を示唆しました。該当グループは、組織レベルのサービス統合を無効化してセキュリティ制御を回避する目的で信頼できるアクセスを妨害しました。AWS Identity Center を悪用して MFA を回避し、セッション持続時間を延長するための設定を構成しました。日常的な活動としては、SES API の列挙、「We Are There But Not Visible」という説明を持つ EC2 セキュリティグループの作成試行、過剰な管理権限を IAM ユーザーに付与することが含まれていました。この攻撃は、AWS 環境内で持続性を維持し、意図を隠蔽するための洗練されたアプローチを反映しています。

[Attack Flow]

NSHC©2025 All rights reserved.

1. [永続性] 「persistence-as-a-service」を作成
   a. API ゲートウェイの作成
   b. ラムダ関数「buckets555」の作成とトリガー設定
2. [資格情報アクセス] AWS Identity Center を悪用
   a. MFA 設定の回避
   b. セッション持続時間を 90 日に延長
3. [防御回避] 信頼されたサービスアクセスを無効化
   a. DisableAWSServiceAccess API の呼び出し
   b. 組織サービス統合の無効化
4. [探索] AWS SES 設定を列挙
   a. GetAccount API の呼び出し
   b. ListIdentities API の呼び出し
5. [権限昇格] 管理者権限を付与
   a. IAM ユーザーに「AdministratorAccess」ポリシーを付与
   b. IAM ユーザーのログインプロファイル作成を試みる
6. [実行] 自動化された ConsoleLogin に Telegram を使用
   a. テレグラム IP（149.154.161[.]235）からのコンソールログインイベントの発生
   b. テレグラムボットを通じた自動ログイン URL の生成
7. [影響] EC2 セキュリティグループの作成を試みる
   a. 「We Are There But Not Visible」の説明のセキュリティグループ作成を試みる
   b. EC2 セキュリティグループ「Administratorsz」の作成を試みる

16) SectorJ213 new Domains for Lumma Stealer Malware (2025-04-22)

https://cti.nshc.net/events/view/14588

攻撃対象産業群: 政府・行政

SectorJ213 グループは、2024 年 8 月から政治的企業を対象に高度なファイルレス侵入戦略を使用して機密データを窃取しました。彼らは Chrome のゼロデイ脆弱性を悪用し、ダウンロードしたシェルコードをシステムメモリに直接注入し、「Lumma stealer」トロイの木馬をディスクにファイルを残さずに配布しました。各オペレーションは固有の使い捨て「コマンド・アンド・コントロール（C2）」ドメインを使用し、約 1,600 のドメインが 1 年以内に識別され、グループのインフラへのかなりの投資を示しています。侵入は通常 3〜5 分間続き、長期的な制御を避け、ゴートラフィック広告ドメインを通じて提供される CAPTCHA に偽装されたスクリプトを使用しました。攻撃は主に政府および企業組織の古い Chrome がインストールされた Windows 7 システムに影響を与え、ブラウザクッキー、メール資格情報、その他の機密ファイルを窃取した後、持続性を設定せずに終了しました。

NSHC©2025 All rights reserved.

[Attack Flow]

1. [初期アクセス] ドライブバイ妥協 (T1189)
   a. 広告ドメインを通じたマルウェアスクリプトの配布
   b. CAPTCHA に偽装されたスクリプトの実行
2. [実行] クライアント実行のためのエクスプロイト (T1203)
   a. "Chrome" ゼロデイ脆弱性の悪用
   b. ダウンロードしたシェルコードをメモリに注入
3. [持続性] なし
   a. ファイルレスアクセスで持続性を設定せず
4. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. "Lumma stealer"でメール資格情報を窃取
   b. ブラウザクッキーの窃取
5. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. 各オペレーションごとに固有の C2 ドメインを使用
   b. Cloudflare CDN を通じて C2 ドメインを隠蔽
6. [データ抽出] C2 チャネルを介したデータ抽出 (T1041)
   a. 窃取されたデータを C2 に送信
   b. データ送信後にクリーンに終了

17) SectorJ214 used Metasploit for Cactus Ransomware (2025-04-24)

https://cti.nshc.net/events/view/14645

SectorJ214 グループは「LAGTOY」バックドアを使用して重要なインフラ組織に侵入しました。その後、このブローカーは「Cactus」というランサムウェアグループにアクセス権を提供しました。この攻撃は金銭的利益を目的としており、資格情報の窃取、ネットワークの損傷、ランサムウェアの配布につながり、最終的には二重恐喝戦略に帰結しました。主な手法としては、カスタムインプラントおよびリモート管理ツールが活用されました。脅威行為者は最初に偵察を行った後、取得したアクセス情報をランサムウェアグループに販売し、さらなる悪用を試みました。この作戦の深刻度は、データ漏洩を含む影響により高く評価されました。キャンペーンで使用された技術には、オペレーティングシステムの資格情報ダンピング、リモートシステムの発見、代替プロトコルを通じたデータ漏洩、ホスト指標の削除、システム情報の発見およびアカウント作成などが含まれます。これらの方法は、ネットワーク情報を利用した攻撃準備および悪用において高度な能力を示しています。

[Attack Flow]

NSHC©2025 All rights reserved.

1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. "LAGTOY" バックドア使用
   b. 主要インフラ組織への侵入
2. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. 資格情報の窃取
   b. オペレーティングシステムからの情報抽出
3. [探索] リモートシステム探索 (T1018)
   a. リモートシステム情報の収集
   b. ネットワーク内部構造の把握
4. [持続性] システムプロセスの作成または変更 (T1543)
   a. システムプロセスの生成
   b. 持続的なアクセスの確保
5. [防御回避] ホスト上のインジケーターの削除 (T1070)
   a. ホストインジケーターの削除
   b. 検知回避
6. [収集] ローカルシステムからのデータ (T1005)
   a. ローカルシステムからのデータ収集
   b. 情報の蓄積
7. [流出] 代替プロトコルを使用した流出 (T1048)
   a. 代替プロトコルを使用したデータ流出
   b. ネットワーク外部への情報送信
8. [影響] 影響のためのデータ暗号化 (T1486)
   a. ランサムウェアの配布
   b. データの暗号化および二重窃取の試み

18) SectorJ216 used Malware for Password Spray Attack and cryptomining (2025-04-23)

https://cti.nshc.net/events/view/14629

SectorJ216 グループは、コンテナ環境のセキュリティ脆弱性を悪用して攻撃を行っています。彼らは特に「Kubernetes」クラスターをターゲットにしており、主に侵害されたクラウド資格情報、脆弱または誤って構成されたイメージ、露出した管理インターフェースを通じて攻撃を開始します。攻撃手法としては、悪性コンテナのデプロイ、アプリケーションレベルのエクスプロイト、クラウドコントロールプレーンを通じた不正アクセスがあります。最近の事例では、該当グループは教育産業を対象にクラウド環境で巧妙な資格情報攻撃を行いました。彼らは Microsoft Azure ベースのインフラ内で AzureChecker.exe ツールを活用し、大規模なパスワードスプレー（Password Spraying）手

NSHC©2025 All rights reserved.

法を実行し、それによって有効な資格情報を特定し、認証回避に成功したと分析されています。その後、取得したアクセス権を基に暗号通貨の採掘を目的としたリソースグループを作成し、クラウドリソースを不正に活用しました。このキャンペーンは Kubernetes 環境でも拡張され、アプリケーションレベルの SQL インジェクション攻撃、ノードレベルの脆弱性エクスプロイト、そして誤った環境構成（misconfiguration）などを通じて多様な攻撃ベクターが活用される可能性を示唆しました。特に、クラスター内に存在する不安定なネットワーク設定を悪用して内部トラフィックの流れを不正に操作または再ルーティングする活動が観察され、これは権限昇格および内部システム間のラテラルムーブメント（Lateral Movement）を可能にします。

[Attack Flow]

1. [初期アクセス] 有効なアカウント (T1078)
   a. 侵害されたクラウド資格情報の使用
   b. ゲストアカウントを通じたリソースグループの作成
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
   a. "AzureChecker.exe" ツールの使用
   b. 暗号通貨マイニング作業のためのコンテナ作成
3. [持続性] アカウント操作 (T1098)
   a. アカウントとパスワードの組み合わせ使用
   b. クラウド資格情報の検証
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. 脆弱なイメージの悪用
   b. 誤った環境設定の活用
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. AES 暗号化されたデータのダウンロード
   b. "accounts.txt" ファイルの使用
6. [発見] クラウドサービスの発見 (T1526)
   a. クラウド制御プレーンの探索
   b. クラスター管理層へのアクセス
7. [影響] リソースの乗っ取り (T1496)
   a. 暗号通貨マイニングのためのコンテナ使用
   b. 200 以上のコンテナの作成

19) SectorJ221 used Hijacked Domains for Scam and Malicious URLs (2025-05-20)

https://cti.nshc.net/events/view/15515

攻撃対象産業群: 健康、政府・行政、高等教育

NSHC©2025 All rights reserved.

SectorJ221 グループは、DNS 設定のエラーを悪用して S3 バケットや Azure エンドポイントなどの放置されたクラウドリソースを奪取します。2023 年 12 月以降に活動を開始し、商業的なパッシブ DNS（PassiveDNS）サービスを通じて脆弱性を特定し、「CNAME」レコードの脆弱性を悪用してドメインを奪取します。2025 年 2 月には、「アメリカ疾病予防管理センター」（「CDC」）のサブドメインを侵害し、そのドメインの信頼性を利用して「トラフィック分配システム」（TDS）を通じてスキャムとマルウェアを配布しました。彼らの方法は、「DNS」設定のエラーを利用してクラウドリソースに無断でアクセスし、悪意のある「URL」を通じてユーザーをリダイレクトすることです。これらの「URL」は合法的なウェブサイトのコンテンツを悪用して悪意を隠し、広告技術サービスを通じて被害者をスキャムに誘導します。「Hazy Hawk」は、継続的に被害者をターゲットにするためにプッシュ通知を統合します。

[Attack Flow]

1. [偵察] 被害者ネットワーク情報の収集 (T1590)
   a. パッシブ DNS サービスへのアクセス
   b. DNS 記録の分析
2. [リソース開発] インフラの取得 (T1583)
   a. 放置されたクラウドリソースの識別
   b. Azure アカウントの作成
3. [初期アクセス] 公開アプリケーションの悪用 (T1190)
   a. CNAME レコードの奪取
   b. ドメインハイジャック
4. [実行] コマンドとスクリプトインタプリタ (T1059)
   a. マルウェア URL の生成
   b. トラフィック分配システムの活用
5. [持続性] システムプロセスの作成または変更 (T1543)
   a. プッシュ通知の統合
   b. ブラウザ通知の継続的送信
6. [防御回避] ファイルまたは情報の難読化 (T1027)
   a. URL リダイレクトと難読化
   b. 正当なウェブサイトコンテンツの盗用
7. [影響] ユーザー実行 (T1204)
   a. 被害者をスキャムに誘導
   b. マルウェアの配布

20) SectorJ223 used Stealer Malware via Fake AI Video Generation Platforms (2025-05-08)

NSHC©2025 All rights reserved.

https://cti.nshc.net/events/view/15125

SectorJ223 グループは AI テーマの詐欺プラットフォームを作成しました。彼らは Facebook のようなソーシャルメディアを利用して攻撃対象を引き寄せ、無料の AI コンテンツ作成ツールを提供すると主張していますが、この過程でユーザーは悪意のあるウェブサイトに誘導され、AI 生成コンテンツに偽装された Malware をダウンロードしてしまいます。この Malware は主に「Noodlophile Stealer」で構成されており、ブラウザの資格情報、暗号通貨ウォレット情報、その他の機密データを盗むように設計されています。さらに、システムへのリモートアクセス型トロイの木馬を配布し、より深い制御を確保することができます。攻撃戦略はソーシャルエンジニアリングに基づいており、AI の進展に対する信頼を悪用して、クリエイターや小規模ビジネスなどの新しいターゲットグループを攻撃対象としています。Malware のインストールは巧妙に設計されており、合法的な AI コンテンツに偽装されたファイルのダウンロードを含む多段階のインストールチェーンを実行します。この過程には、「CapCut.exe」のような C++バイナリをビデオファイルに偽装し、コマンド実行のための動的リンクライブラリ「AICore.dll」などが使用されます。

[図 8: SectorJ223 グループが利用したフィッシングサイト]

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. ソーシャルメディアを通じた AI ツール提供広告
   b. 偽の AI プラットフォームへユーザーを誘導
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. CapCut.exe の実行を通じた Malware のロード

NSHC©2025 All rights reserved.

   b. AICore.dll でコマンドを実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. Windows レジストリの Run キーにスクリプトを登録
   b. Explorer.bat スクリプトを通じた持続性の確保
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. Document.docx に偽装されたバッチファイル
   b. Base64 エンコードおよびパスワード保護されたアーカイブ
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. ブラウザ資格情報の窃取
   b. 暗号通貨ウォレット情報の収集
6. [コマンドと制御] アプリケーション層プロトコル (T1071)
   a. Telegram ボットを通じた情報漏洩
   b. リモートサーバーとの通信
7. [データ流出] C2 チャネルを通じた流出 (T1041)
   a. Noodlophile Stealer を通じたデータ送信
   b. Telegram API を通じたデータ漏洩
8. [影響] データ破壊 (T1485)
   a. 一時ファイル削除によるフォレンジック痕跡の除去
   b. 自己破壊機能による証拠の除去

今月のサイバー脅威の特徴

2025年5月の1か月間、APTグループとサイバー犯罪グループの活動は、前例のないほど精巧で多様化した戦術的な様相を示しました。彼らは単発的な侵入や単純な情報窃取を超えて、明確な目的を持った長期的かつ組織的な攻撃作戦を遂行し、各攻撃段階で高度な技術と偽装戦術が複合的に活用されました。

APTグループの場合、政治、外交、国防、先端技術、暗号通貨産業などの国家戦略資産または高付加価値産業群を主要な標的とし、巧妙に操作されたソーシャルエンジニアリングに基づく餌文書や、通常の業務フローを装ったメール、協力機関または内部人員を装ったメッセンジャーメッセージを通じて初期侵入の足場を築きました。このようにユーザーの信頼を巧みに悪用したアプローチは、既存のセキュリティ検出システムを効果的に回避する手段として機能しました。

初期侵入後には、LNK、PowerShell、HTA、悪性文書（DOC、XLS）、MSIファイルなど様々なフォーマットのマルウェアペイロードを活用して段階的に追加モジュールをロードする手法が多数観察され、WindowsおよびMacOSなどのオペレーティングシステムを問わず、Bashスクリプトや

NSHC©2025 All rights reserved.

AppleScriptなどOS特化技術が動員されました。特にファイルレス(fileless)方式でメモリ上でのみ実行される悪性スクリプトの活用は、痕跡を最小化し、検出を困難にしました。また、UACバイパス、DLLサイドローディング、プロセスインジェクション、タスクスケジューラの登録、Plistファイルの修正などを通じて感染の持続性と権限の維持を確保しました。

また、攻撃者は感染後、対象システムからブラウザのクッキー、資格情報、キー入力、クリップボードデータ、ファイルシステム構造などの機密情報を収集し、これをDropbox、MEGA、Yandex、pCloudのような正式なクラウドプラットフォームを通じて外部に送信しました。この過程では、HTTPSベースの暗号化チャネル、Cloudflare Tunnel、Ngrok、Fastly、Amazon CloudFrontなどのCDN、または動的DNS（DynDNS、No-IP）ベースの技術を組み合わせてC2インフラの可視性を最小限に抑えました。

主要な使用マルウェアとしては、RoKRAT、BeaverTail、SparkRAT、DslogdRAT、InvisibleFerretなどが識別されており、これらはRAT（Remote Access Trojan）ベースのリモート制御機能に加えて、モジュール化されたプラグイン構造を通じて収集対象データを柔軟に設定できるように設計されていました。一部のケースでは、攻撃者が対象システムで仮想化検出、サンドボックス回避、地域言語ベースの環境認識機能まで搭載した事例も観察されており、これは攻撃対象が特定の地域や機関に限定されていたことを示唆しています。

一方、サイバー犯罪グループはAPTグループとは異なる目的の下、金銭的利益を得るためにランサムウェアおよび情報窃取型のマルウェアの拡散に集中していました。彼らはRaaS（Ransomware-as-a-Service）またはMaaS（Malware-as-a-Service）のエコシステムを基盤に、匿名性の保証と機能の多様性を掲げた攻撃プラットフォームを活用しており、攻撃実行者、インフラ提供者、収益分配者が分離された構造でキャンペーンを展開しています。

最近活動が活発なランサムウェアであるQilin、RA Lord、Interlockなどは、メールフィッシング、マルウェアMSIインストールファイル、マルウェアChrome拡張プログラム、偽の採用サイト、偽造されたウォレットアプリなどを通じて拡散されており、感染後にはシステムの暗号化、バックアップの破壊、機密情報の流出および脅迫サイトの運営へとつながる典型的な二重恐喝モデルが適用されました。

情報窃取を目的としたマルウェアには、Amethyst Stealer、TerraStealer、Tycoon 2FAキット、NetSupport Managerなどが使用され、これらはブラウザに保存された情報、パスワード管理プログラム、OTP認証トークン、クリップボード内の暗号通貨アドレスなどを収集し、Telegram、TOX、Discordなどの非公式チャネルを通じて攻撃者のサーバーに送信しました。特に一部のキャンペーンでは、ポッドキャストプラットフォーム、YouTube動画の説明欄、SNS投稿に隠されたリンクを通じてマルウェアペイロードを配布する非伝統的な戦術も観察されました。

全体的に、APTとサイバー犯罪グループの両方が、検出を回避しつつ長期的な制御権を維持するという目標の下、高度な侵入方法と通信インフラ運用戦略を継続的に発展させています。これらの攻撃は特定の地域に限定されず、アジア、ヨーロッパ、中南米などに拡散しており、キャンペーンの規模と頻度、技術の複雑さ、インフラの隠蔽性の観点から徐々にグローバル化しています。特に攻撃者間の

NSHC©2025 All rights reserved.

インフラ共有、マルウェアの再利用、偽装戦術の一致などにより、攻撃間の区別がさらに難しくなっており、これは防御の観点でも大きな挑戦課題となっています。このような様相は、今後の脅威インテリジェンス収集と対応戦略の策定において、多層監視、行動基盤の検出、インフラ分析の重要性がさらに浮き彫りになることを示唆しています。

今月のサイバー脅威の示唆点

2025年5月の1ヶ月間に観察されたAPTおよびサイバー犯罪グループの活動は、戦術的な精密さと侵入方法の多様化に基づき、既存の防御システムを回避し、長期的な侵入を試みる脅威行為者の戦略的変化が一層具体化していることを示しています。彼らはもはや単一のベクトルに依存せず、複数のオペレーティングシステム（macOS、Windows）を同時に狙ったり、クラウドベースのインフラ、正式なIT管理ツール、正規の証明書などの合法的手段を巧妙に悪用することで、脅威の検出可能性を最小限に抑えています。

初期侵入段階では、SPF/DKIMの整合性が保たれたフィッシングメール、実際の企業の採用ページを精巧に複製したスミッシングリンク、有効なコード署名を含むMalware配布など、ユーザーが信頼できる要素を意図的に活用することで、技術的・心理的防御線の両方を無力化するソーシャルエンジニアリングに基づく戦略が全面的に拡大しています。これは単純な技術的対応だけでは脅威を遮断するのが難しく、ユーザーの認識および組織レベルのポリシーに基づく防御が並行して行われる必要があることを強く示唆しています。

APTグループの活動を見てみると、単に初期侵入を成功させるだけでなく、その後のコマンド実行、内部偵察、資格情報の窃取、感染の持続性確保など、一連の攻撃段階を綿密に設計していることが明らかです。特に、Living off Trusted Sites（LoTS）技法を通じて、Google Drive、Dropbox、OneDrive、GitHubなどのクラウドサービスインフラを通信チャネルおよびデータ流出経路として積極的に活用しており、これはネットワークベースの検出システムを無力化させています。さらに、ファイルレス攻撃、インメモリーローディング技法、スクリプトベースの即時実行ペイロードなどは、定型化されたルールベースの検出システムを回避するのに効果的に作用しており、これは署名ベースの脅威検出方式の限界を露呈させています。

このように、APTグループが駆使する戦術は、短期的な成果よりも長期的な情報収集、内部権限の拡大、戦略資産へのアクセスを目指しており、Attack Flow全体を理解し対応するための脅威インテリジェンスに基づく分析の必要性が日増しに高まっています。

NSHC©2025 All rights reserved.

サイバー犯罪グループの場合、2025年5月にも収益化中心の戦略がさらに精巧になった様子が観察されました。彼らはRaaSおよびMaaSモデルに基づく犯罪エコシステムを積極的に活用しており、攻撃ツールの開発、配布、運用がそれぞれ独立してサービス化される傾向が顕著になっています。Qilin、Interlock、RA Lordなどの主要なランサムウェアグループは、ファイルの暗号化にとどまらず、機密データの流出、脅迫サイトの開設、バックアップシステムの破壊、被害企業のメディア露出を通じた社会的圧力など、多層的な恐喝戦略を併用しています。これに加えて、Amethyst Stealer、Tycoon 2FAキット、NetSupport Managerなどの多様な情報窃取型Malwareが組み合わされて使用され、攻撃対象の認証情報、ブラウザセッション、OTPトークンなどを窃取し、後続の攻撃や追加の収益化に活用されています。特にこれらのキャンペーンは、ソーシャルメディア、モバイルアプリ、音声ベースのチャンネル（例：ポッドキャスト）、悪質なウェブ広告を通じて広範囲に拡散されており、技術的手段よりも心理的弱点を狙う高度に精巧なソーシャルエンジニアリング手法が併用されています。また、Telegram、TOX、Discordなど匿名性と暗号化が保証される非公式チャンネルを通じた攻撃ツールの流通およびリアルタイムの被害情報の送信が日常化しており、クレデンシャル窃取自動化ツールおよびC2フレームワークのアクセス性が拡大するにつれて、技術熟練度が低い行為者でも高度なレベルの攻撃を実行できる環境が整っています。このように攻撃インフラの分業化・自動化は、攻撃範囲を全地理的・産業的範囲に拡大することに寄与しており、これは既存の防御体系に対する全面的な再考を要求しています。

結論として、2025年5月の攻撃トレンドは、単一の技術的脆弱性の悪用ではなく、戦術・技術・ソーシャルエンジニアリング・インフラ運用戦略が巧妙に結合された複合型攻撃の拡散が特徴です。それに伴い、組織の防御戦略もルールベースの検出や単一のセキュリティ機器中心の受動的アプローチから脱却し、異常行動の検出、コンテキストベースの脅威分析、インフラ間の関連性分析を含む多層的な脅威中心の防御システムへの転換が求められています。さらに、クラウドサービス、オープンソースソフトウェア、外部ストレージなどの濫用を監視し制御できる政策的基準と技術的な可視性の確保が、セキュリティガバナンスの重要な要素として位置づけられるべき時期です。

NSHC©2025 All rights reserved.

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

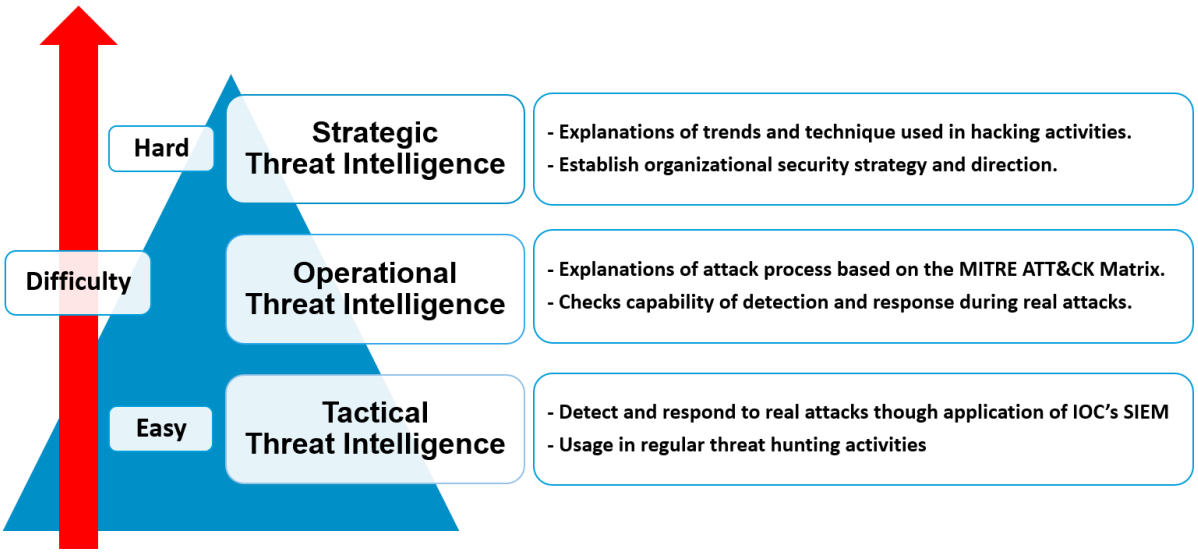
- ソーシャルエンジニアリング(Social Engineering)技法とスピアフィッシング(Spear Phishing)E-Mail を識別できる教育の検討が必要

NSHC©2025 All rights reserved.

- 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

NSHC©2025 All rights reserved.

- 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

NSHC©2025 All rights reserved.

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

NSHC©2025 All rights reserved.

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

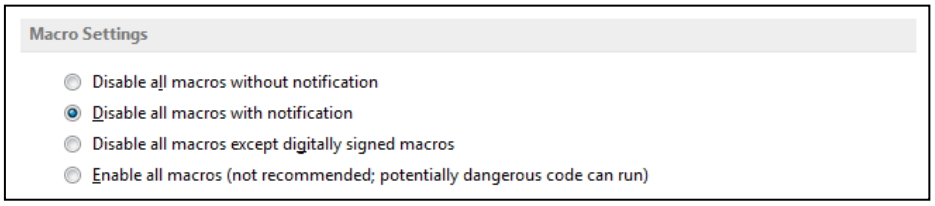
5) 機能の無効化及びプログラムの削除 (Disable or Remove Feature or

NSHC©2025 All rights reserved.

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

NSHC©2025 All rights reserved.

- 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

NSHC©2025 All rights reserved.

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.

NSHC©2025 All rights reserved.