NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI2025070202

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

June 2025

NSHC PTE. LTD.

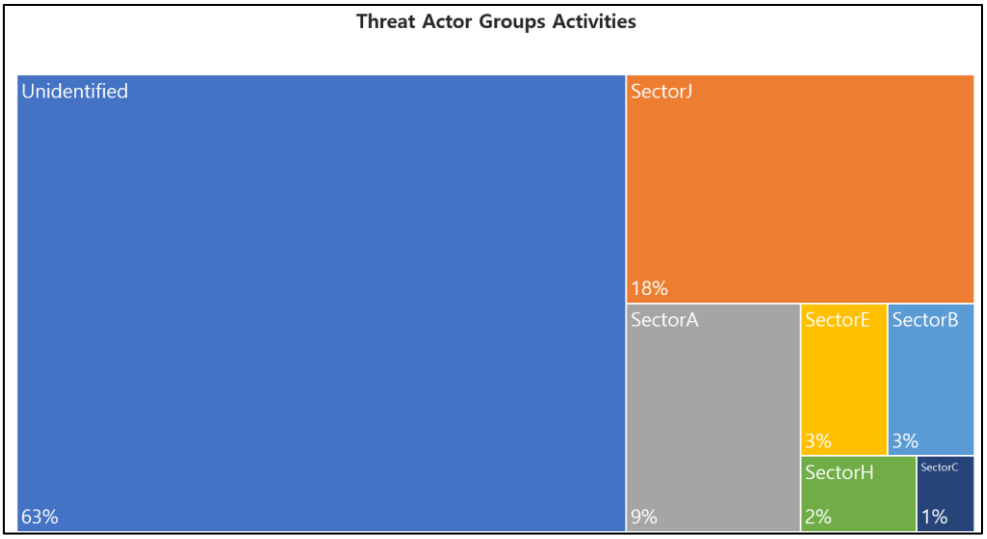
このレポートは 2025 年 5 月 21 日から 2025 年 6 月 20 日まで見つけた政府支援のハッキンググループ活動と関係あるイッシューを説明し、それに伴う侵害事故の情報と ThreatRecon Platform 内のイベント情報を含む。

Table of Contents

エグゼクティブサマリー

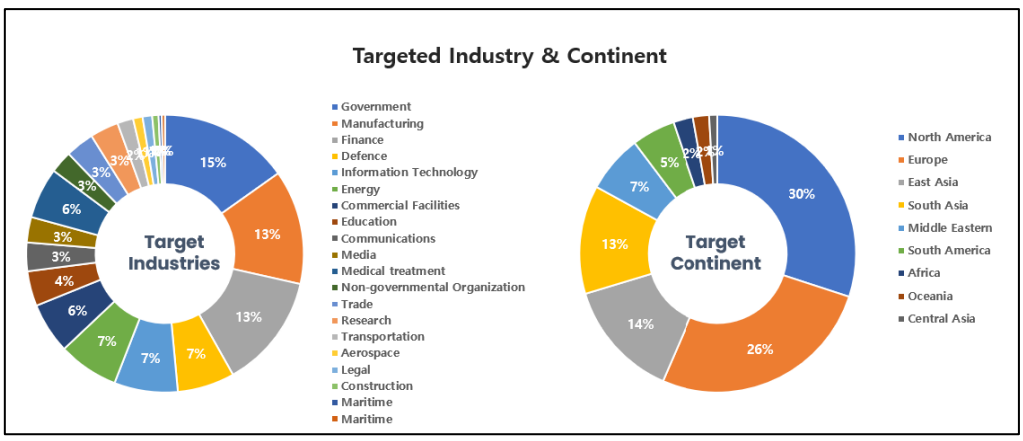
2025 年 5 月 21 日から 2025 年 6 月 20 日までの間に NSHC 脅威分析研究所（Threat Research Lab）が収集したデータと情報に基づいて分析したハッキンググループ（Threat Actor Group）の活動を要約した内容です。

今回の 6 月には、合計 79 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 63%で最も多く、次いで SectorJ、SectorA グループの活動が続きました。



[図 1: 2025 年 6 月に確認されたハッキンググループ別活動統計]

今年 6 月に発見されたハッキンググループのハッキング活動は、政府機関や製造業分野に従事する関係者またはシステムを対象に最も多くの攻撃を行い、地域別では北アメリカとヨーロッパに位置する国々を対象としたハッキング活動が最も多いことが確認されています。



[図 2: 2025 年 6 月に攻撃対象となった産業分野と国の統計]

SectorA グループは、開発環境と高リスクの社会分野の従事者を対象に活発な攻撃を行いました。GitHub、Supabase、ethers.js、NPM などの開発プラットフォームを悪用し、偽の NFT プロジェクトやフリーランスの提案書に偽装したサプライチェーン侵害を試み、macOS を含むマルチプラットフォームの Malware を通じて暗号通貨の秘密鍵と資格情報を盗みました。また、ジャーナリスト、教授、市民団体の活動家などを対象にフィッシングメールを送信し、PowerShell、LNK、AppleScript などを活用した悪意のあるペイロードを配布しました。正常なクラウドインフラを C2 チャネルとして使用する巧妙な検出回避戦術も確認されました。

SectorB グループは、サーバーベースのシステムおよびクラウド SaaS インフラを集中的に攻撃しました。MS SQL、RDP などの脆弱性を悪用して、Pemodifier、ESP（拡張ストアドプロシージャ）ベースのバックドアをインストールし、Ivanti EPMM および Commvault Metallic のゼロデイ脆弱性を利用して認証トークンを奪取し、ラテラルムーブメントを実行しました。Sliver フレームワークを利用した高度な C2 運用と認証システムの回避技術も併用されており、サプライチェーンおよび MSP 接続構造を媒介とした内部拡散戦略が特徴的です。

SectorC グループは、外交および政府機関を対象に巧妙なフィッシングとクライアント側の脆弱性攻撃を併用しました。Outlook の NTLM リレー脆弱性と Roundcube ウェブメールのスクリプト脆弱性を組み合わせて、ヨーロッパ・ウクライナ関連の組織に侵入し、国務省を装ったメールを通じてアプリケーション専用パスワード（ASP）を盗みました。ソーシャルエンジニアリングに基づく侵入戦略と、メールアカウントの長期的な制御を目的とした高度なアプローチが主な特徴として現れました。

SectorD グループはシステム管理者アカウントを対象に PowerShell ベースのマルウェアスクリプトを配布し、Google Drive リンクを通じてペイロードを配信しました。感染後は ScreenConnect を利用したリモート制御を通じて、継続的な情報収集と内部ネットワークの拡張を試みました。戦術の展開は単純ですが、合法的なリモート制御ツールを悪用することで検出を困難にする方法が特徴的です。

SectorE グループは、正常なオープンソースプロジェクトのリポジトリを偽装したり、ISO ファイルや LNK ファイルを利用したマルウェア感染シナリオを活用しました。初期侵入後には、Dropbox を通じた C2 通信と PowerShell スクリプトの実行を組み合わせ、ユーザーアカウント情報やキー入力を収集する戦略を展開しました。キャンペーンの展開速度は遅いものの、検出回避のための社会工学的設計が精巧に構成されていました。

SectorF グループは、macOS ユーザーを狙ったスクリプト型のマルウェアを配布しました。ダウンロードを誘導する PDF ドキュメントを通じて AppleScript を実行し、被害者の資格情報を収集したり、リモート C2 サーバーにコマンドを送信する方法が使用されました。過去より精密さは低いものの、特定の OS 環境に最適化された攻撃手法を維持していることが確認されました。

SectorH グループは、Android プラットフォームを利用したモバイルベースの情報収集作戦を実施しました。CapraRAT マルウェアを含む APK ファイルは、ビデオ通話アプリまたは政府案内アプリに

偽装され、アクセシビリティ権限を悪用して、ビデオ・音声の録音、位置追跡、メッセージ収集などの多様な監視機能を実行しました。南アジア地域を中心に、ソーシャルエンジニアリングに基づく持続的な脅威が続いています。

SectorK グループは、中東地域の政府機関を狙った高度なゼロデイ攻撃を実行しました。CVE-2025-33053（WebDAV）の脆弱性を利用して初期侵入に成功した後、ウェブシェルを挿入し、内部システムへの長期的なアクセスを確保しました。侵入後のラテラルムーブメントおよび管理者権限の奪取の流れは体系的に構成されており、組織内の重要システムを掌握するための戦略的行為と評価されます。

SectorS グループは南米地域の公共機関を対象に多段階 VBScript ベースの Malware を配布しました。感染後、リモートコマンドの実行とシステム情報の窃取が行われ、[Attack Flow]は単純ですが、現地の言語とターゲットに合わせた内容でフィッシング効果を最大化しました。長期的な侵入よりも短期的な情報窃取および偵察が目的であったと分析されています。

SectorT グループは ISO ファイルを利用したスクリプト型のマルウェア配布キャンペーンを実施し、感染後に Sliver フレームワークに基づくコマンド・コントロールの流れが検出されました。クラウドホスティングベースの C2 インフラと GitHub リポジトリを組み合わせて検出を回避し、内部アカウントの認証情報収集およびラテラルムーブメントに至る典型的な侵入シナリオが観察されました。

SectorJ グループは、最も活動量が多いグループの一つであり、企業環境やユーザーアカウント保護システムを回避する戦略的攻撃を集中的に展開しました。主に AnyDesk や ScreenConnect のようなリモート制御ツールを活用し、フィッシングメールやカレンダー招待リンクを通じて初期アクセスを確保しました。Calendly や Zoom リンクを悪用したり、OneNote および Windows Script Host ベースの Malware を通じてユーザーの相互作用を誘導する方法が確認されました。特に MFA 回避、資格情報の窃取、サプライチェーン汚染などの複合戦術が併用され、高い精密度を示しました。

詳細情報

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

1) SectorA01 used Fake NFT Projects to Deliver Malware Through GitHub (2025-05-30)

https://cti.nshc.net/events/view/15849

最近、SectorA01 グループのサイバー攻撃キャンペーンは、暗号通貨業界の従業員を対象とした精巧な攻撃を含んでいました。初期段階では、フィッシング手法を通じて攻撃対象システムに足場を築

きました。ある事例として、このグループは NFT マーケットプレイスのプロジェクトの潜在的な協力者を装い、「BitMEX」の従業員に「LinkedIn」を通じて接触しました。この従業員は、「Next.js/React」プロジェクト内にマルウェアが含まれた非公開の「GitHub」リポジトリに招待されました。分析の結果、このコードには JavaScript の eval 関数呼び出しが含まれており、特定のドメインに「HTTP」リクエストを送信し、難読化されたマルウェアの実行につながることが確認されました。この中の 1 つのコンポーネントは、以前に知られたマルウェアキャンペーンと関連する資格情報窃取ツールとして識別されました。攻撃はまた、「Supabase」データベースに接続し、感染したデバイスからの情報を記録する方法で進行しました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. "LinkedIn"を通じた協力者のなりすまし
   b. 非公開の"GitHub"リポジトリへの招待
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. "JavaScript 'eval'"関数の呼び出し
   b. 特定のドメインへの"HTTP"リクエスト送信
3. [資格情報アクセス] パスワードストアからの資格情報 (T1555)
   a. 資格情報窃取ツールの活用
   b. "Chrome"拡張機能 ID の参照
4. [収集] ローカルシステムからのデータ (T1005)
   a. 感染したデバイスの情報収集
   b. "Supabase"データベースへの情報送信
5. [流出] C2 チャネルを介したデータ流出 (T1041)
   a. 収集されたデータの外部送信
   b. "Supabase"データベースのオープン権限問題の利用
6. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 難読化されたマルウェアの使用
   b. "JavaScript"デオブフスケーションツールの活用

2) SectorA01 は偽の求人情報を使用して OtterCookie マルウェアを展開しました (2025-06-03)

https://cti.nshc.net/events/view/15922

攻撃対象産業群: 金融、IT

SectorA01 グループは最近、「OtterCookie」という新しいマルウェアを通じて、技術、金融、暗号通貨産業の専門家を対象に攻撃を実行しました。このマルウェアは、社会工学的な戦術を利用して偽

の求人広告やフリーランス契約を提案し、被害者に分散アプリケーション（DApp）の些細なバグを修正するよう誘導しました。コードはクリーンに見える「Node.js」を通じて配信され、実行過程で意図的なエラーを引き起こす「try/catch」ブロックを使用し、外部 API からペイロードを取得して実行するという創造的な方法を使用しました。「OtterCookie」の主な攻撃対象には、ブラウザの資格情報、「macOS」キーチェーン、「Solana」や「Exodus」などの暗号通貨ウォレットが含まれます。収集されたデータは、アメリカに位置する C2 サーバー（コマンド＆コントロールサーバー）に非標準ポート 1224 を通じて流出します。また、「OtterCookie」は暗号通貨とパスワードマネージャーに重点を置いたブラウザ拡張モジュールも使用します。この作戦は、「InvisibleFerret」など他のマルウェアを含むモジュール式多段階攻撃戦略の一環です。該当グループは以前にも「Beavertail」などの脅威を通じて類似の社会工学戦術を使用し、金融および暗号通貨産業を継続的にターゲットにしてきました。「OtterCookie」は「Node.js」ベースのクリーンに見えるコードで偽装し、初期実行時に意図的にエラーを発生させた後、外部 API からペイロードを受け取って実行する点で特に注目されます。

[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. 偽の求人広告を通じてアクセス
   b. フリーランス契約の提案で誘導
2. [実行] コマンドとスクリプトインタープリタ: JavaScript (T1059.007)
   a. "Node.js" コード内の "try/catch" ブロック使用
   b. エラー発生時に外部 API からペイロード実行
3. [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. "macOS" キーチェーンへのアクセス
4. [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データの収集
   b. ブラウザ拡張プログラムデータの収集
5. [データ流出] 代替プロトコルによるデータ流出 (T1048)
   a. 非標準ポート 1224 の使用
   b. 米国拠点の C2 サーバーへのデータ流出
6. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. "JavaScript" コードの難読化
   b. "Node.js" コードの巧妙な偽装

3) SectorA01 used Malware disguised as web3 library to steal keys (2025-06-12)

https://cti.nshc.net/events/view/16095

SectorA01 グループは暗号通貨開発者を標的に、ethers ライブラリに偽装したマルウェア NPM パッケージ web3-wrapper-ethers を作成し、秘密鍵の窃取を試みました。該当パッケージは kaufman0913 という名前で配布され、バージョン 6.14.5 から node-fetch を利用した外部送信機能が含まれ、悪意のある行為が本格化しました。核心となるマルウェアコードは src.ts/wallet/wallet.ts パスに挿入され、ビルド過程で lib.esm および lib.commonjs パスにも同様に反映されました。初期バージョンには誤った HTTP URL がハードコーディングされており、通信失敗が発生しましたが、該当エラーを修正しようとする者たちのリアルタイムデバッグの痕跡がコンソールログとコメントを通じて確認されました。その後に配布された最終バージョン（6.14.7）ではデバッグ関連のログが削除されましたが、URL エラーは依然として残っていました。分析の結果、パッケージが接続を試みた C2 サーバーは 74.119.194[.]244 と識別され、秘密鍵流出のためのトラフィック送信が目的であったと考えられます。

[Attack Flow]

1. [初期アクセス] 有効なアカウント (T1078)
   a. "web3-wrapper-ethers" パッケージを通じたアクセス
   b. "ethers" ライブラリを装ってユーザーを混乱させる
2. [実行] コマンドとスクリプトインタープリター (T1059)
   a. "src.ts/wallet/wallet.ts" ファイルの修正
   b. "node-fetch" を使用したコード実行
3. [認証情報アクセス] 入力キャプチャ (T1056)
   a. 個人キー収集のためのコード挿入
   b. "super()" 呼び出しの下にキー送信コードを追加
4. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. エンコードされたサーバーURL へのキー送信試行
   b. 74.119.194[.]244 へのデータ流出試行
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. コードのコメントおよびコンソールログの削除
   b. 不正な HTTP URL の問題未解決

4) SectorA01 used PylangGhost Malware in Fake Job Sites (2025-06-18)

https://cti.nshc.net/events/view/16240

2025 年 5 月、SectorA01 グループは暗号通貨およびブロックチェーンの専門家を狙ったサイバー脅威キャンペーンを開始しました。この攻撃は主にインドの少数のユーザーに影響を与え、

「PylangGhost」という Python ベースのリモートアクセス型トロイの木馬（RAT）を使用しました。このトロイの木馬は、以前に識別された Golang ベースの亜種と機能的に類似しています。彼らは実在の会社を装った偽の採用インタビューサイトを利用して被害者を誘引する欺瞞的な戦術を使用しました。これらのサイトは、ユーザーに悪意のあるドライバーをインストールさせ、RAT を配布します。該当グループは、ブラウザのフィンガープリンティングと適切なシェルコマンドを通じて、Windows と MacOS プラットフォームに対する個別の方法を展開しました。「PylangGhost」は 6 つの Python モジュールで構成され、データ窃盗やリモートシステム制御などのさまざまな機能を実行します。RC4 暗号化を使用して HTTP を介してコマンド＆コントロール（C2）サーバーと通信し、80 以上のブラウザ拡張機能から資格情報を盗むことができる機能を持っています。

[Attack Flow]

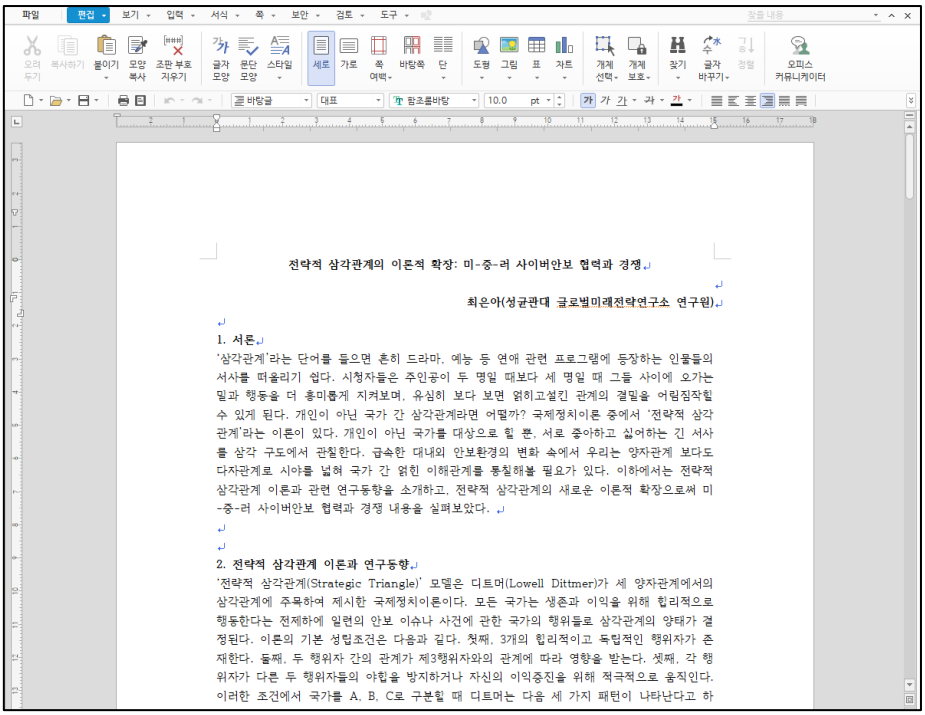
1. [初期アクセス] スピアフィッシングリンク (T1566.002)
   a. 偽の採用インタビューサイトのリンク送信
   b. ユーザーにクリックを促す
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. PowerShell またはコマンドシェルコマンドの実行
   b. ZIP ファイルのダウンロードと実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. レジストリ値の作成
   b. ユーザーログイン時にトロイの木馬を実行
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. RC4 暗号化の使用
   b. HTTP 通信を通じた暗号化パケットの送信
5. [資格情報アクセス] パスワードストアからの資格情報 (T1555)
   a. ブラウザ拡張機能からの資格情報の盗用
   b. パスワードマネージャーおよび暗号通貨ウォレットからの情報収集
6. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
   a. HTTP を通じた C2 サーバーとの通信
   b. コマンドループに従ったサーバーコマンドの実行
7. [収集] 情報リポジトリからのデータ (T1213)
   a. 保存されたブラウザ資格情報およびセッションクッキーの収集
   b. 様々なブラウザ拡張機能からのデータ収集

5) SectorA02 used LNK Malware disguised as a National Security Report (2025-06-09)

https://cti.nshc.net/events/view/16000

攻撃対象の産業群: ジャーナリスト、社会運動団体

SectorA02 グループは、「国家情報と防諜原稿.lnk」というマルウェアのショートカットファイルを利用して、韓国国内の対北関係者を対象に攻撃を行いました。この攻撃は、対北人権団体、北朝鮮関連の記者、脱北者、対北研究学者を主な対象としており、ファイルの容量は約 52MB です。このマルウェアは PowerShell を通じて分析され、.lnk ファイルから特定のオフセットのデータを抽出し、.hwp、.dat、.bat などの様々な形式で復元して悪意のある活動を行います。CMD スクリプトを含め、リバースシェルの実行やディレクトリ探索で実行ファイルを検索し、システム保護を回避するために%temp%ディレクトリで動作します。データ抽出過程では、.lnk ファイル内部で囮ファイルを生成し、これを静かに実行して ttf01.dat に偽装した二次ペイロードを配布します。このペイロードは XOR 暗号化、WinAPI 関数呼び出しを通じたメモリ操作、シェルコード実行を使用し、TLS 1.2 を活用して安全な通信を保証します。主に最小化された PowerShell ウィンドウを通じて 64 ビット Windows システムで 32 ビット実行パスとして運用されます。マルウェアはまた、成均館大学グローバル未来戦略研究所関連の研究員の名義で作成された文章をユーザーに表示する機能を含んでいます。



전략적 삼각관계의 이론적 확장: 미-중-러 사이버안보 협력과 경쟁

최은아(성균관대 글로벌미래전략연구소 연구원)

1. 서론

'삼각관계'라는 단어를 들으면 흔히 드라마, 예능 등 연애 관련 프로그램에 등장하는 인물들의 서사를 떠올리기 쉽다. 시청자들은 주인공이 두 명일 때보다 세 명일 때 그들 사이에 오가는 밀과 행동을 더 흥미롭게 지켜보며, 유심히 보다 보면 얽히고설킨 관계의 결말을 어림짐작할 수 있게 된다. 개인이 아닌 국가 간 삼각관계라면 어떨까? 국제정치이론 중에서 '전략적 삼각관계'라는 이론이 있다. 개인이 아닌 국가를 대상으로 할 뿐, 서로 좋아하고 싫어하는 긴 서사를 삼각 구도에서 관찰한다. 급속한 대내외 안보환경의 변화 속에서 우리는 양자관계 보다도 다자관계로 시야를 넓혀 국가 간 얽힌 이해관계를 통찰해볼 필요가 있다. 이하에서는 전략적 삼각관계 이론과 관련 연구동향을 소개하고, 전략적 삼각관계의 새로운 이론적 확장으로써 미-중-러 사이버안보 협력과 경쟁 내용을 살펴보았다.

2. 전략적 삼각관계 이론과 연구동향

'전략적 삼각관계(Strategic Triangle)' 모델은 디트머(Lowell Dittmer)가 세 양자관계에서의 삼각관계에 주목하여 제시한 국제정치이론이다. 모든 국가는 생존과 이익을 위해 합리적으로 행동한다는 전제하에 일련의 안보 이슈나 사건에 관한 국가의 행위들로 삼각관계의 양태가 결정된다. 이론의 기본 성립조건은 다음과 같다. 첫째, 3개의 합리적이고 독립적인 행위자가 존재한다. 둘째, 두 행위자 간의 관계가 제3행위자와의 관계에 따라 영향을 받는다. 셋째, 각 행위자가 다른 두 행위자들의 야합을 방지하거나 자신의 이익증진을 위해 적극적으로 움직인다. 이러한 조건에서 국가를 A, B, C로 구분할 때 디트머는 다음 세 가지 패턴이 나타난다고 하

[図 3: SectorA02 グループが使用したおとり文書]

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566)
   a. 「国家情報と防諜原稿.lnk」ファイル配布
   b. 特定の対北関係者を対象にカスタマイズされたフィッシングメール送信

2. [実行] コマンドとスクリプトインタープリター: PowerShell (T1059.001)
   a. PowerShell を通じた.lnk ファイルデータ抽出
   b. PowerShell スクリプトで様々なファイル(.hwp, .dat, .bat)復元
3. [持続性] ショートカット修正 (T1547.009)
   a. マルウェアのショートカットファイルで持続性維持
   b. システム再起動後も持続的に Malware 実行
4. [防御回避] 偽装 (T1036)
   a. ttf01.dat で二次ペイロード偽装
   b. .hwp ファイルに偽装してユーザーの混乱を誘導
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. メモリから認証情報収集
   b. WinAPI 関数呼び出しでシステム資格情報抽出
6. [探索] システム情報探索 (T1082)
   a. システムディレクトリ探索および情報収集
   b. 実行ファイル検索およびディレクトリ構造把握
7. [収集] ローカルシステムからのデータ (T1005)
   a. .lnk ファイル内部データ収集
   b. ユーザーファイルおよびシステム情報収集
8. [コマンドと制御] 暗号化チャネル (T1573)
   a. TLS 1.2 を活用した暗号化通信
   b. 外部サーバーとの安全なデータ送信
9. [流出] C2 チャネル経由の流出 (T1041)
   a. 収集されたデータを C2 サーバーに送信
   b. PowerShell スクリプトを通じてデータの窃取および送信完了

6) SectorA05 used Phishing Email Disguised as Tax Notification (2025-05-28)

https://cti.nshc.net/events/view/15868

SectorA05 グループは「国税庁」を装ったフィッシングメールを通じて、ユーザーが悪意のあるリンクをクリックするよう誘導しました。ユーザーがリンクをクリックすると、偽のログインポータルに接続され、このサイトはユーザーの資格情報を収集するために設計されています。悪意のあるサイトは韓国のドメインを使用して信頼性を高め、疑念を避けようとしました。これはソウルに位置する Vultr 仮想サーバーホスティングを利用して実行されました。メールヘッダーの分析結果、DKIM および SPF の通過の痕跡が発見され、メールセキュリティフィルターを回避するための技術的措置が取られたことを示唆しています。ハッカーは個人情報や暗号通貨の資格情報を盗み、取得した機密データに基づいて追加攻撃を行う可能性が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. 「国税庁」を装ったメール送信
   b. マルウェアリンクを含む
2. [実行] ユーザー実行 (T1204)
   a. ユーザーがリンクをクリック
   b. フィッシングサイトにリダイレクト
3. [資格情報アクセス] 入力キャプチャ (T1056)
   a. 偽のログインポータルで資格情報を収集
   b. ユーザー入力情報を保存
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. DKIM および SPF を通過
   b. メールセキュリティフィルターを回避
5. [コマンド＆コントロール] ウェブサービス (T1102)
   a. Vultr 仮想サーバーを使用
   b. ソウルに位置するサーバーを活用
6. [収集] 情報リポジトリからのデータ (T1213)
   a. ユーザー個人情報を収集
   b. 暗号通貨の資格情報を収集

7) SectorA05 used Multi-Channel Phishing to Deliver AppleSeed Malware (2025-06-09)

https://cti.nshc.net/events/view/15991

攻撃対象産業群: 防衛、軍事機関、社会運動団体

2025 年 3 月から 4 月の間に、韓国の「フェイスブック」、「メール」、「テレグラム」ユーザーを対象とした高度持続的脅威（Advanced Persistent Threat, APT）キャンペーンが確認されました。このキャンペーンは SectorA05 グループによって主導され、彼らは脱北者支援活動に関与した個人を欺くためにソーシャルエンジニアリング技術を活用した巧妙な侵入戦略を使用しました。該当グループは偽の「フェイスブック」アカウントを利用して宣教師や研究者を装い信頼を得て、パスワードで保護された「EGG」アーカイブを通じてマルウェアペイロードを配信しました。その後、「メール」と「テレグラム」を通じて追加の接触を試み、一貫したテーマを維持して攻撃対象に信頼を植え付けました。キャンペーンは合法的な「PDF」ドキュメントに偽装した悪性「JSE」スクリプトファイルを使用し、「VMProtect」でパックされた「DLL」を配信し、これにより持続的なシステムアクセスとデータ流出を可能にしました。この「DLL」は「regsvr32.exe」を通じて実行され、「RC4」と

「RSA」暗号化を使用して C2 サーバーと秘密裏に通信を行いました。彼らは多段階デコードプロセスと「XOR」および「Base64」エンコーディングを使用して悪性活動を隠蔽する高度な回避戦術を活用しました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. Facebook メッセージを通じた初期接触
   b. メールを通じたマルウェアファイル送信
2. [実行] コマンドとスクリプトインタープリター (T1059)
   a. JSE スクリプト実行
   b. PowerShell を通じた追加コマンド実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. レジストリ Run キー登録
   b. regsvr32.exe を通じた DLL 自動実行
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. Base64 でエンコードされたマルウェア
   b. XOR 暗号化を通じたコード隠蔽
5. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. システム情報収集
   b. 資格情報抽出
6. [コマンド＆コントロール] 暗号化チャネル (T1573)
   a. RC4 暗号化通信使用
   b. RSA でキー交換実行
7. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. C2 サーバーへのデータ送信
   b. PDF に偽装されたファイル送信

8) SectorA05 used Phishing Email with Malicious OLE Object Disguised as Academic Request (2025-06-12)

https://cti.nshc.net/events/view/16054

SectorA05 グループは最近、教授を対象に論文審査の依頼を装ったフィッシングメールキャンペーンを実施しました。このフィッシングメールには、悪性の OLE オブジェクトが挿入されたハングル文書ファイルが添付されており、メール本文に含まれるパスワードを入力しないと文書を開くことができません。文書が開かれると、%TEMP%パスに 6 つのファイルが自動生成されます。この中で重要なファイルは「peice.bat」で、文書内のハイパーリンクを使ってユーザーを騙し、実行を促しま

す。「peice.bat」ファイルが実行されると、元の悪性文書を削除し、生成されたファイルを特定のシステムパスにコピーして追加の実行を管理します。特に、「template.ps1」という PowerShell スクリプトは、システムのプロセスリストとインストールされたアンチウイルス情報を収集し、該当グループの Dropbox に送信します。このグループは AnyDesk のような正規のソフトウェアを利用して、承認されていないリモートアクセスを試み、クラウドベースの C2 通信を通じて精巧な攻撃を行っています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. メールを通じてフィッシングメール送信
   b. 論文審査の依頼を装い教授を対象とする
2. [実行] ユーザー実行 (T1204)
   a. ハングル文書ファイルを開くと OLE オブジェクトが実行される
   b. 文書内のハイパーリンクで「peice.bat」実行を誘導
3. [持続性] スケジュールされたタスク/ジョブ (T1053)
   a. 「GoogleTransltatorExtendeds」という名前でスケジューラー登録
   b. 12 分ごとに「cool.exe」実行設定
4. [防御回避] 偽装 (T1036)
   a. 正常な AnyDesk ファイルに偽装
   b. プロセスおよびウィンドウを隠す処理
5. [収集] ローカルシステムからのデータ (T1005)
   a. プロセスリストの収集
   b. インストールされたアンチウイルス情報の収集
6. [流出] C2 チャネル経由の流出 (T1041)
   a. 収集された情報を Dropbox に送信
   b. 追加ファイルのダウンロードおよび実行
7. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. クラウドベースの C2 通信を使用
   b. 正常なソフトウェアを利用して通信を偽装

9) SectorA05 used Phishing Page Disguised as Naver Login Webpage (2025-06-16)

https://cti.nshc.net/events/view/16172

SectorA05 グループは最近、フィッシングキャンペーンを通じて、著作権侵害を理由にコンテンツが一時的に削除されたという内容のメールを送信し、ユーザーに緊急措置を促しました。該当のメールは有名なオンラインサービスプロバイダーを装っており、「今すぐ確認」ボタンをクリックすると

、ユーザー情報を収集するためのフィッシングサイトにリダイレクトされました。このサイトは実際のログインページを精巧に模倣しており、ユーザーが資格情報を入力すると、その情報が該当グループに送信された後、異常なページに転送される仕組みでした。このキャンペーンは信頼できるブランドを利用した社会工学的手法に基づいており、資格情報の窃取を主な目的とした精巧なフィッシング戦略の一環と評価されています。

[Attack Flow]

1. [初期アクセス] スピアフィッシングリンク (T1566)
   a. メールを通じてフィッシングリンクを送信
   b. 著作権侵害を装う
2. [実行] ユーザー実行 (T1204)
   a. ユーザーが「今すぐ確認」ボタンをクリック
   b. 偽のログインページにリダイレクト
3. [資格情報アクセス] 入力キャプチャ (T1056)
   a. ユーザーの資格情報入力を誘導
   b. 入力された情報を収集
4. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. 収集された資格情報を送信
   b. 望ましくないページにリダイレクト

10) SectorA05 used KimJongRAT Stealer disguised as LNK File (2025-06-17)

https://cti.nshc.net/events/view/16216

「KimJongRAT」スティーラーの 2 つの新しい亜種が発見されました。このマルウェアは、攻撃対象のシステムに侵入し、個人情報やブラウザデータを含む暗号通貨ウォレット拡張機能を収集することを目的としています。2013 年に初めて観察されたこの亜種は、「Portable Executable（PE）」と「PowerShell」の実装を含んでいます。両方の亜種は、悪意のある「Windows」ショートカット（LNK）ファイルから始まり、グループの制御する「CDN」アカウントからドロッパーをダウンロードします。「PE」亜種のドロッパーは、追加の悪意のあるコンポーネントを配布し、ローダーとおとりの「PDF」を含みます。「PowerShell」亜種のドロッパーは、「ZIP」アーカイブを通じてキーロガーとスティーラーをインストールし、「PowerShell」スクリプトを実行します。両方の亜種は、システム、ブラウザ、「FTP」、メールクライアントのデータを C2 サーバーに漏洩させることを目的としています。このマルウェアは、プロセスインジェクションや暗号化された通信などの高度な技術を使用して検出を回避して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)
   a. マルウェアの "Windows" ショートカット (LNK) ファイル使用
   b. 攻撃者制御の "CDN" からドロッパーをダウンロード
2. [実行] コマンドとスクリプトインタープリタ: PowerShell (T1059.001)
   a. "PowerShell" スクリプト実行
   b. "ZIP" アーカイブでキーロガーとスティーラーをインストール
3. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. "PE" 変種のドロッパー実行
   b. 追加のマルウェア構成要素を配布
4. [防御回避] 偽装: 正当な名前または場所に一致 (T1036.005)
   a. 正当なサービスに偽装
   b. プロセスインジェクション使用
5. [資格情報アクセス] 入力キャプチャ: キーロギング (T1056.001)
   a. キーロガーインストール
   b. ユーザーの入力データ収集
6. [収集] 情報リポジトリからのデータ (T1213)
   a. システムおよびブラウザデータ収集
   b. 暗号通貨ウォレット拡張機能データを含む
7. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. "C2" サーバーへのデータ流出
   b. 暗号化された通信使用

11) SectorA06 used MacOS Malware Disguised as Zoom Extension (2025-06-18)

https://cti.nshc.net/events/view/16279https://cti.nshc.net/events/view/16279

SectorA06 グループは 2025 年 6 月、暗号通貨財団に所属するユーザーを対象に macOS 環境で巧妙なサイバー攻撃を実行しました。該当グループは Telegram メッセージを通じて被害者を偽の「Zoom」ミーティングリンクに誘導し、ディープフェイク技術を活用してユーザーがマルウェア Zoom 拡張プログラムをインストールするように仕向けました。該当拡張プログラムは AppleScript ベースのペイロードで、Rosetta 2 のインストール誘導、ユーザーパスワードの窃取、bash 履歴の削除などの機能を含んでいました。その後、キーロガー、情報窃取ツール、リモート制御ツールなど多数のペイロードが実行され、被害者のホストでは持続性の確保、コマンド実行、モジュールの復号、入力監視、暗号通貨情報の収集などの機能を実行する 8 種類のマルウェアバイナリが確認されました。本キャンペーンは macOS プラットフォームを狙った高度な社会工学に基づく攻撃と評価されています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. テレグラムを通じたフィッシングメッセージ送信
   b. "Calendly" リンクでユーザー誘導
2. [実行] AppleScript (T1059.002)
   a. "AppleScript" 実行でペイロードダウンロード
   b. "bash" 記録無効化
3. [持続性] Launch Daemon (T1543.001)
   a. "Telegram 2" を通じた持続性維持
   b. /Library/LaunchDaemons パス使用
4. [防御回避] プロセスインジェクション (T1055)
   a. "InjectWithDyld" を通じたプロセスインジェクション
   b. メモリ保護回避
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. ユーザーパスワード取得試行
   b. "sudo" を通じたパスワード検証
6. [収集] 入力キャプチャ (T1056)
   a. "XScreen" でキー入力モニタリング
   b. クリップボードと画面キャプチャ
7. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. C2 サーバーへのデータ送信
   b. "CryptoBot" を通じた暗号通貨情報窃取
8. [コマンド＆コントロール] ウェブサービス (T1102)
   a. ウェブソケットを通じたコマンド送信
   b. リモート "AppleScript" 実行

12) SectorB01 used LNK Malware disguised as PDF for Gov Entity Attack (2025-05-29)

https://cti.nshc.net/events/view/15738

攻撃対象産業群: 物流、政府・行政、海運、技術、自動車、娯楽、メディア・報道

SectorB01 グループは「TOUGHPROGRESS」マルウェアを利用して、世界中の政府機関や海運、メディア、技術、自動車産業を標的とした攻撃を行いました。彼らは損傷した政府のウェブサイトをマルウェアのホストとして利用し、スピアフィッシングメールを通じて ZIP ファイルを配布しました。この ZIP には PDF に偽装された LNK ファイルと、暗号化されたペイロードを含む画像ファイルが含まれており、実行時に悪意のある DLL をロードするように構成されていました。

TOUGHPROGRESS は「PLUSDROP」、「PLUSINJECT」、「TOUGHPROGRESS」の 3 つのモジュールで構成されており、暗号化、メモリ内ロード、プロセスホローイングなどの回避技術を活用しています。特に Google カレンダーを C2 チャンネルとして悪用し、イベントにコマンドを挿入し、結果を記録する方法で通信を行いました。マルウェアは.pdata 領域のシェルコードを XOR キーで復号化した後、LZNT1 圧縮 DLL をメモリ内でロードし、複雑なフロー難読化を通じて検出を回避しました。

[Attack Flow]

1. [初期アクセス] スピアフィッシングリンク (T1192)
   a. スピアフィッシングメール送信
   b. ZIP アーカイブリンクを含む
2. [実行] ユーザー実行 (T1204)
   a. "LNK"ファイル実行
   b. DLL ファイルロード
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 画像ファイル内の暗号化されたペイロード
   b. プロセスハロウィング技術の使用
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. Google カレンダーでの C2 通信
   b. カレンダーイベントに暗号化されたデータを記録
5. [持続性] スケジュールされたタスク/ジョブ (T1053)
   a. カレンダーイベントを通じたスケジュール実行
   b. 定期的なイベントポーリング
6. [収集] ローカルシステムからのデータ (T1005)
   a. 感染したホストデータの収集
   b. カレンダーイベントにデータを送信
7. [データ流出] 代替プロトコルによるデータ流出 (T1048)
   a. Google カレンダーを通じたデータ送信
   b. 暗号化されたデータ送信

13) SectorB61 used Maggie Backdoor Exploiting MS SQL Servers (2025-05-23)

https://cti.nshc.net/events/view/15589

攻撃対象産業群: IT、政府・行政、通信

SectorB61 グループは、MS SQL および RDP の脆弱性を悪用して初期侵入を行い、中国製ツールに基づくバックドアとマルウェアを使用します。主なツールには、SQL クエリを通じてコマンドを実

行する「Maggie」バックドア、改ざんされた DLL で動作する IRC ボット「Wgdrop」、および実行ファイルに悪性 DLL を挿入する「Pemodifier」があります。これらは信頼された証明書を悪用してセキュリティ検出を回避し、IRC ベースのボットネットおよび「WinEggDrop」製作者との関連性が指摘されています。該当グループは侵入後、悪性機能を統合した多機能（All-In-One）ツールを活用してシステムファイルを改ざんし、悪性 DLL をロードして持続的な制御権限を確保します。

[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. MS SQL および RDP ポートスキャニング
   b. ブルートフォースによるアクセス
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
   a. SQL クエリを通じた Malware 実行
   b. IRC コマンドを通じたリモート制御
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. 悪性 DLL ロードのための実行ファイルパッチ
   b. ユーザー信頼プログラムの改ざん
4. [権限昇格] プロセスインジェクション (T1055)
   a. Pemodifier を使用した実行ファイル改ざん
   b. 権限昇格ツールの使用
5. [防御回避] 有効なアカウント (T1078)
   a. 有効な証明書で Malware 署名
   b. セキュリティ検出回避のための証明書盗用
6. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. CredentialStealer を通じた資格情報流出
   b. Windows ログオンセッションマネージャからの情報収集
7. [探索] システム情報探索 (T1082)
   a. システム情報収集
   b. 仮想環境の有無確認
8. [横移動] リモートサービス: SMB/Windows 管理共有 (T1021.002)
   a. SMB/Admin Share を通じた内部移動
   b. SQL サーバーアクセスおよびアカウント追加
9. [収集] ローカルシステムからのデータ (T1005)
   a. ファイルダウンロードおよび実行
   b. プロセスおよびユーザーアカウント管理
10. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
    a. IRC サーバーを通じたコマンド制御

b. irc[.]itembuy[.]org サーバーへの接続

11. [影響] 影響のためのデータ暗号化 (T1486)

a. コインマイニングプログラムのインストール

b. システムリソース占有および悪性行為の実行

14) SectorB86 used RCE Exploit on Ivanti EPMM for Data Exfiltration (2025-05-21)

https://cti.nshc.net/events/view/15555

攻撃対象産業群: 金融、航空宇宙、健康、政府・行政、通信、防衛、自動車

SectorB86 グループは、2025 年 5 月 15 日に公開された Ivanti Endpoint Manager Mobile (EPMM)の脆弱性（CVE-2025-4427、CVE-2025-4428）を悪用して攻撃を行いました。この脆弱性は、認証されていないリモートコード実行（RCE）を可能にし、バージョン 12.5.0.0 およびそれ以前のバージョンに影響を与えます。攻撃はインターネットに公開された EPMM のデプロイメントを対象に同日から開始され、ヨーロッパ、北米、アジア太平洋の医療、通信、航空、政府、金融、防衛産業に影響を与えました。該当グループは「/mifs/rs/api/v2/」エンドポイントを狙い、Java ベースのコマンドを使用して悪性プロセスを実行しました。「KrustyLoader」という Malware が観察され、このコードは AWS S3 バケットを通じて配信されました。彼らはハードコーディングされた MySQL 資格情報を使用してデータの窃取を行い、窃取されたデータには機密性の高いデバイス情報と認証トークンが含まれていました。また、「Fast Reverse Proxy (FRP)」がネットワーク偵察および側面移動（Lateral Movement）に使用されました。

[Attack Flow]

1. [初期アクセス] 公開されたアプリケーションのエクスプロイト (T1190)

a. "Ivanti EPMM"の"/mifs/rs/api/v2/"エンドポイントに対する認証されていない RCE 脆弱性の悪用

b. Java ベースのコマンドを使用して悪性プロセスを実行

2. [実行] コマンドとスクリプトインタープリタ: JavaScript/JScript (T1059.007)

a. Java リフレクションを使用して"Runtime.getRuntime().exec()"を通じて任意のコマンドを実行

b. "Scanner"を使用して実行されたコマンドの出力をキャプチャ

3. [持続性] インプラントコンテナ (T1620)

a. "KrustyLoader"マルウェアのインストール

b. AWS S3 バケットを通じてペイロードを配信

4. [資格情報アクセス] 保護されていない資格情報 (T1552)

a. ハードコーディングされた MySQL 資格情報を使用してデータベースにアクセス

b. 敏感なデバイスデータと認証トークンの窃取

5. [探索] システムネットワーク構成の探索 (T1016)
   a. "FRP"を使用したネットワーク偵察
   b. "Nmap"を通じたネットワークスキャン
6. [横移動] 内部スピアフィッシング (T1534)
   a. 横移動のための認証トークンの使用
   b. "LDAP"サーバーおよびユーザー情報の窃取
7. [コマンドと制御] アプリケーション層プロトコル (T1071)
   a. サーバー側 Java インジェクションを通じたコマンド&コントロール(C2)メカニズムの構築
   b. "Sliver"バックドアを通じた持続的なリモートアクセスの確保
8. [データ流出] C2 チャネルを通じたデータ流出 (T1041)
   a. "Tomcat Java"プロセスのヒープメモリダンプ
   b. "dpaste[.]com"を通じた SQL クエリスクリプトのダウンロードと実行

15) SectorB108 used CVE-2025-3928 to compromise Commvault Metallic SaaS (2025-06-03)

https://cti.nshc.net/events/view/15820

SectorB108 グループは、「Commvault」の「Metallic」サービスとしてのソフトウェア（SaaS）プラットフォームのウェブサーバーで発見されたゼロデイ脆弱性（CVE-2025-3928）を悪用して攻撃を行いました。この脆弱性により、認証されたこのグループはウェブシェルを展開することができ、それを通じて「Commvault」に保存されたクライアントの秘密情報に不正アクセスし、顧客の「Microsoft 365」環境に侵入することができました。これは、過剰な権限を持つサービスプリンシパルとサードパーティ資格情報ストアのリスクを如実に示しました。これは、デフォルト設定と高い権限を持つ SaaS アプリケーションを対象とした広範なキャンペーンの一部として識別されており、このキャンペーンはアメリカの重要なインフラおよびクラウドソフトウェアプロバイダーを標的としていることで知られています。彼らはソフトウェアサプライチェーンの脆弱性を悪用して攻撃を拡大しました。

[Attack Flow]

1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. ゼロデイ脆弱性(CVE-2025-3928)の悪用
   b. ウェブサーバー攻撃
2. [実行] コマンドおよびスクリプトインタープリタ: Web シェル (T1059.001)
   a. Web シェルの配布
   b. "aspx", "default.aspx", "shell.aspx" ファイル名の使用
3. [資格情報アクセス] 資格情報アクセスのためのエクスプロイト (T1212)

a. クライアント秘密情報へのアクセス
b. "Commvault" ストレージ資格情報の抽出
4. [横移動] 内部スピアフィッシング (T1534)
a. "Microsoft 365" 環境への移動
b. サービスプリンシパル権限の悪用
5. [影響] データ操作 (T1565)
a. 顧客環境内のデータ操作
b. 無許可の変更およびアクセス試行

16) SectorB114 exploited SQL injection vulnerabilities for access (2025-05-27)

https://cti.nshc.net/events/view/15684

攻撃対象産業群: IT、物流、政府・行政、学界 - 大学、小売

SectorB114 グループは、Web アプリケーションの SQL インジェクション脆弱性を利用して攻撃対象システムの SQL サーバーに侵入し、Apache Struts2 の CVE-2017-9805 や GitLab の CVE-2021-22205 など、複数の既知の脆弱性を活用します。初期には金融サービス業界に集中していましたが、その後、物流、オンライン小売業、IT、学界、政府機関へと攻撃対象を広げました。彼らは「PULSEPACK」や DLL サイドローディングなどのカスタムオープンソースハッキングツールとバックドアを使用して検出を回避します。「PULSEPACK」はモジュラー型の.NET バックドアで、TCP を介した WebSocket を使用する新しいバージョンへと進化してきました。このグループは、権限昇格、資格情報のダンプ、横方向の移動、そしてスケジュールされたタスクを通じた持続性の維持など、さまざまな技術を使用します。

[Attack Flow]

1. [偵察] 脆弱性スキャン (T1595.002)
a. SQL インジェクション脆弱性スキャン
b. ウェブアプリケーション脆弱性の識別
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. SQL サーバー脆弱性の悪用
b. Apache Struts2 および GitLab 脆弱性の悪用
3. [実行] コマンドとスクリプトインタープリタ: PowerShell (T1059.001)
a. "powershell.exe"で追加ツールをダウンロード
b. システムシェルを開く
4. [持続性] スケジュールされたタスク/ジョブ: スケジュールされたタスク (T1053.005)
a. バックドア実行のためのタスクをスケジュール
b. システム再起動後の実行持続

5. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
    a. "GodPotato"および"JuicyPotato"で権限昇格
    b. 管理者グループにユーザーを追加
6. [防御回避] インジケータ除去: Windows イベントログのクリア (T1070.001)
    a. "wevtutil.exe"でイベントログを削除
    b. "VOIDMAW"でメモリスキャナーを回避
7. [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. LSASS メモリダンプ
    b. SAM および SYSTEM ハイブの抽出
8. [横移動] 横方向ツール転送 (T1570)
    a. ネットワークスキャンツールの転送
    b. "rakshasa"および"Stowaway"でプロキシトンネリング
9. [コマンド＆コントロール] 暗号化チャネル: 対称暗号 (T1573.001)
    a. AES 暗号化で C&C 通信
    b. "PULSEPACK"を使用した WebSocket 利用
10. [データ流出] C2 チャネル経由のデータ流出 (T1041)
    a. C&C チャネルを通じたデータの窃取
    b. バックドアを通じたデータ転送

17) SectorC01 exploited Microsoft Outlook and Roundcube vulnerabilities (2025-05-21)

https://cti.nshc.net/events/view/15543

攻撃対象産業群: 産業、物流、海上、政府・行政

SectorC01 グループは、2022 年から西部の物流および IT 企業を対象にサイバースパイ活動を行っています。この攻撃キャンペーンは、ウクライナへの支援を提供する企業を主なターゲットとしており、資格情報推測、スピアフィッシング、公共インフラの脆弱性悪用といった既知の戦術、技術、手順（TTPs）を活用しています。初期アクセスは、「Outlook NTLM」や「Roundcube」といった脆弱性、および「WinRAR」の任意コード実行脆弱性を通じて行われます。侵害後の活動には、重要な連絡先を特定するための偵察、「PsExec」や「Impacket」といったツールを用いた横方向の移動、そして「Exchange Web Services (EWS)」や「Internet Message Access Protocol (IMAP)」を通じたメールサーバーアクセスによるデータ窃取が含まれます。該当グループは、持続的なアクセスを維持するための高度な方法、メールボックス権限の調整、ウクライナへの支援物流に関する情報収集を行っています。また、国境付近のカメラをハッキングして移動経路を追跡することもあります。このキャンペーンは、ウクライナを支援する輸送および技術インフラを戦略的にターゲットにしていることを示しています。

[Attack Flow]

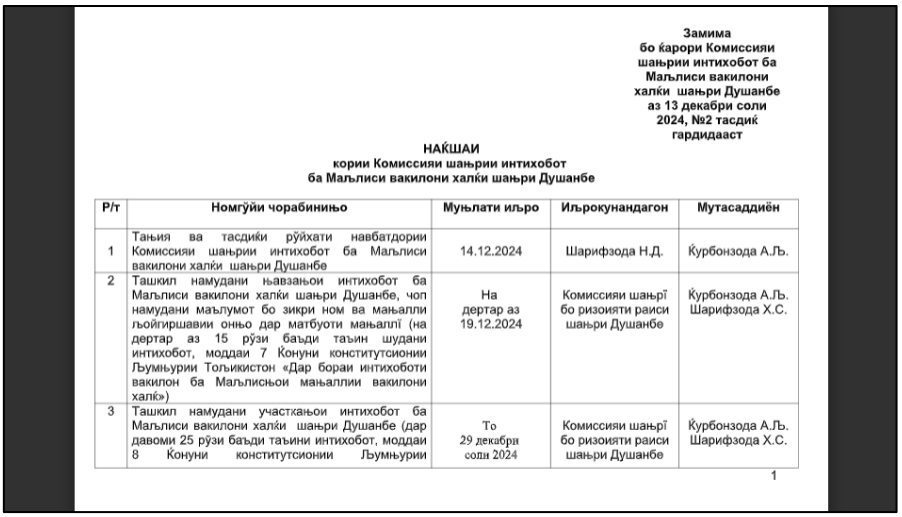
1. [初期アクセス] 資格情報推測 (T1110.001)
   a. 資格証明の推測
   b. ブルートフォース攻撃
2. [初期アクセス] スピアフィッシング (T1566)
   a. スピアフィッシングメールの送信
   b. マルウェアリンクおよび添付ファイルの使用
3. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. 公共インフラの脆弱性悪用
   b. SQL インジェクション攻撃
4. [実行] コマンドとスクリプトインタープリター (T1059)
   a. コマンドおよびスクリプトの実行
   b. マルウェアの実行
5. [持続性] アカウント操作 (T1098.002)
   a. メールボックス権限の調整
   b. MFA メカニズムの登録
6. [横移動] 横移動 (TA0008)
   a. PsExec および Impacket の使用
   b. RDP を通じたネットワーク移動
7. [収集] メール収集 (T1114)
   a. EWS および IMAP を通じたデータ収集
   b. メールサーバーへのアクセス
8. [データ流出] 自動収集 (T1119)
   a. 定期的な EWS クエリの使用
   b. 敏感データの長期収集
9. [防御回避] インジケーターの削除 (T1070.001)
   a. Windows イベントログの削除
   b. 隠されたインフラの使用
10. [偵察] 被害者組織情報の収集 (T1591)
    a. 企業組織情報の収集
    b. ビジネス関係の探索
11. [影響] データ破壊 (T1485)
    a. メールおよびデータの破壊試行
    b. 敏感情報の流出防止努力

18) SectorC01 used macro-enabled Word templates Malware (2025-05-22)

https://cti.nshc.net/events/view/15578

攻撃対象産業群: 政府・行政、教育、外交

SectorC01 グループは 2025 年 1 月から 2 月の間にタジキスタンを対象にフィッシングキャンペーンを実施しました。彼らは政府関連の文書を餌として使用し、主要な攻撃対象として政府機関、教育機関、研究機関を選びました。今回のキャンペーンでは、以前の HTA ベースのペイロードの代わりに、マクロが有効化された「Word」テンプレートファイルを活用する方法に戦術を変更しました。このマクロファイルは「Word STARTUP」ディレクトリに配置され、自動的に実行されるようにし、持続性を確保し、検出を困難にするための戦略的な転換を意味します。攻撃は VBA マクロを利用して文書の保護を解除し、属性を隠し、「STARTUP」ディレクトリに文書を複製して持続的な実行サイクルを開始しました。その後、マクロはシステム情報を収集し、実行時にコマンド＆コントロール（C2）サーバーとの通信を試みました。C2 通信プロトコルは、エンコードされたユーザーエージェントヘッダーを含む HTTP POST リクエストを使用し、サーバーが正しく応答した場合、追加の VBA コードを実行するように設計されていました。



Замима
бо қарори Комиссияи
шаҳрии интихобот ба
Маҷлиси вакилони
халқи шаҳри Душанбе
аз 13 декабри соли
2024, №2 тасдиқ
гардидааст

НАҚШАИ
кории Комиссияи шаҳрии интихобот
ба Маҷлиси вакилони халқи шаҳри Душанбе

Р/т	Номгӯйи чорабиниҳо	Муҳлати иҷро	Иҷрокунандагон	Мутасаддиён
1	Таҳия ва тасдиқи рӯйхати навбатдории Комиссияи шаҳрии интихобот ба Маҷлиси вакилони халқи шаҳри Душанбе	14.12.2024	Шарифзода Н.Д.	Қурбонзода А.Ҷ.
2	Ташкил намудани ҳавзаҳои интихобот ба Маҷлиси вакилони халқи шаҳри Душанбе, чоп намудани маълумот бо зикри ном ва маҳалли ҷойгиршавии онҳо дар матбуоти маҳаллӣ (на дертар аз 15 рӯзи баъди таъин шудани интихобот, моддаи 7 Қонуни конститутсионии Ҷумҳурии Тоҷикистон «Дар бораи интихоботи вакилон ба Маҷлисҳои маҳаллии вакилони халқӣ»)	На дертар аз 19.12.2024	Комиссияи шаҳрӣ бо ризоияти раиси шаҳри Душанбе	Қурбонзода А.Ҷ. Шарифзода Х.С.
3	Ташкил намудани участкаҳои интихобот ба Маҷлиси вакилони халқи шаҳри Душанбе (дар давоми 25 рӯзи баъди таъини интихобот, моддаи 8 Қонуни конститутсионии Ҷумҳурии	То 29 декабри соли 2024	Комиссияи шаҳрӣ бо ризоияти раиси шаҳри Душанбе	Қурбонзода А.Ҷ. Шарифзода Х.С.

1

[図 4: SectorC01 グループが悪用した餌文書]

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 政府関連文書を餌に使用
   b. 教育および研究機関を対象とした攻撃
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. マクロが有効化された「Word」テンプレートファイルを使用
   b. 「Word STARTUP」ディレクトリにファイルを配置
3. [持続性] Office アプリケーションのスタートアップ (T1137.004)

a. 「STARTUP」ディレクトリ内で自動実行設定
b. 持続的実行のためのサイクル開始
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. 文書の保護解除および属性の非表示
b. 検出回避のためのファイル複製
5. [収集] システム情報の発見 (T1082)
a. システム情報の収集
b. マクロ実行時点の情報収集
6. [コマンドと制御] アプリケーション層プロトコル (T1071)
a. HTTP POST リクエストで C2 サーバーと通信
b. エンコードされたユーザーエージェントヘッダーを使用
7. [実行] コマンドとスクリプトインタープリター: VBA (T1059.005)
a. サーバー応答時に追加の VBA コードを実行
b. 持続的な攻撃コマンドの実行

19) SectorC08 used VBS Malware disguised as Military Documents (2025-05-29)

https://cti.nshc.net/events/view/15782

攻撃対象産業群: 政府・行政、軍事機関

SectorC08 グループは 2013 年から政府および軍事機関を対象に高度な持続的脅威（APT）攻撃を行っています。彼らの主な目的は情報の窃取であり、セキュリティ企業によって何度も活動が露出されているにもかかわらず、その活動はさらに強化されています。最近、このグループの一連の VBS サンプルが検出されました。これはコードの断片化と Base64 エンコーディングを通じて高度に難読化されたスクリプトを使用し、ペイロードを段階的に配布する方法です。彼らは継続的に正常なファイルを感染させ、軍事情報をテーマにした Malware LNK ショートカットファイルを生成してユーザーの警戒を緩め、ソーシャルエンジニアリング技術を通じて実行を誘導します。主要な攻撃方法には、分析を妨害するためのスクリプト難読化、C2 通信のための代替メカニズム、制御維持のためのレジストリ修正などがあります。スクリプトはレジストリ操作とスケジュールされたタスクを通じて自己拡散し、戦術としては LNK ファイルを PDF や DOCX のような一般的な文書形式に偽装し、偽のティーザーを通じて悪意のある行動を開始することです。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
a. 軍事情報をテーマにした LNK ファイルに偽装
b. 偽のティーザーでユーザーのクリックを誘導
2. [実行] コマンドとスクリプトインタープリター: Visual Basic (T1059.005)

a. VBS スクリプトでペイロードを実行
b. Base64 エンコードされたスクリプトを段階的に実行
3. [持続性] レジストリの変更 (T1112)
a. レジストリキーを修正して持続性を確保
b. 定期的な実行を設定するために予約タスクを作成
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. コードの断片化と難読化技術を使用
b. Base64 エンコードで検出を回避
5. [認証情報アクセス] 入力キャプチャ (T1056)
a. 感染したシステムから情報を収集
b. キー入力の監視と保存
6. [探索] システム情報の探索 (T1082)
a. システムドライブとコンピュータ名を収集
b. レジストリに情報を保存
7. [コマンドと制御] アプリケーション層プロトコル: Web プロトコル (T1071.001)
a. HTTP/HTTPS を通じて C2 サーバーと通信
b. 代替 C2 アドレスをレジストリに保存
8. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. 収集したデータを C2 チャネルに流出
b. 正規表現を使用したデータの改ざんと送信

20) SectorC32 used AitM Phishing with Spoofed Microsoft Entra Login (2025-05-27)

https://cti.nshc.net/events/view/15706

攻撃対象産業群: 国防、教育、政府・行政、健康、IT、非政府組織(NGO)、メディア、輸送

2025 年 4 月、ロシア政府の利益と関連する組織を主要なターゲットとしたハッキンググループがサイバー諜報活動を行いました。彼らは主にヨーロッパと北米地域の政府、国防、交通、メディア、非政府組織（NGO）、ヘルスケアなど多様な産業群を攻撃対象としました。これらの活動は地政学的力学に関連する緊張状態が高まる時期に発生しました。ハッキンググループは主にオンライン市場で盗まれたログイン資格情報を購入し、攻撃対象システムへの不正アクセスを可能にしました。この作戦は、メールと重要なファイルの大規模な窃取を含んでいました。
サイバーセキュリティ対策の進展に対応して、このハッキンググループは 2025 年 4 月に資格情報を確保するための直接的な手法を強化しました。特に彼らは「スピアフィッシングキャンペーン」を通じて資格情報を窃取し、この過程で「中間者攻撃（Adversary-in-the-Middle, AitM）」戦術を使用しました。これは「タイポスクワッティング（typosquatting）」を通じて合法的な認証ポータルを模倣したものであり、オープンソースツールである「Evilginx」フレームワークを活用しました。

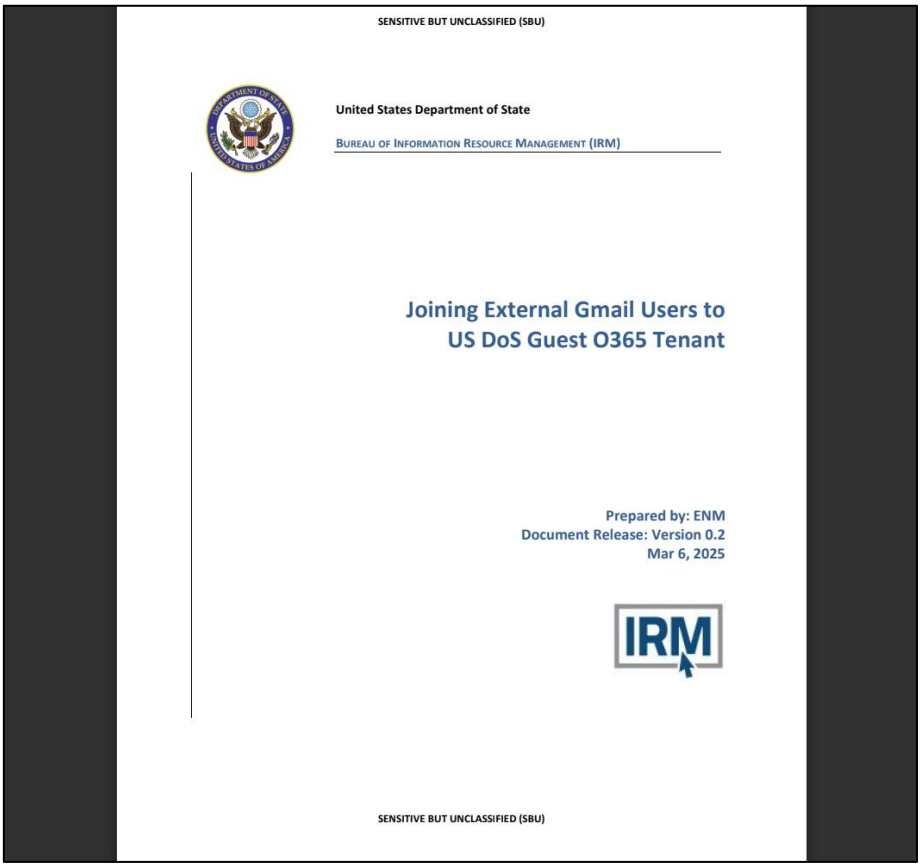
[Attack Flow]

1. [初期アクセス] 有効なアカウント (T1078)
   a. 盗まれたログイン資格情報の購入
   b. オンライン市場での資格情報の取得
2. [資格情報アクセス] スピアフィッシング (T1566.002)
   a. スピアフィッシングキャンペーンの使用
   b. 資格情報の窃取試行
3. [資格情報アクセス] 中間者攻撃 (T1557.002)
   a. Evilginx フレームワークの活用
   b. タイポスクワッティングによる認証ポータルの模倣
4. [収集] 情報リポジトリからのデータ (T1213)
   a. 大量のメールの窃取
   b. 重要なファイルの収集
5. [データ流出] ウェブサービスを介したデータ流出 (T1567)
   a. 窃取したデータの外部への送信
   b. ウェブサービスを通じたデータの流出

21) SectorC33 used Phishing Lures Disguised as State Dept Invitations (2025-06-18)

https://cti.nshc.net/events/view/16252

SectorC33 グループは、2025 年 4 月から 6 月にかけて、アメリカ国務省を装い、ロシアに批判的な著名な学者を対象にサイバー攻撃を実行しました。このハッキンググループは、ソーシャルエンジニアリング技術を使用してターゲットとの関係を構築し、カスタマイズされた餌を通じてターゲットにアプリケーション専用パスワード（ASPs）を設定させました。被害者はこれらの 16 文字のパスコードを共有するように騙され、これによりグループは被害者のメールボックスに継続的にアクセスする権限を得ました。キャンペーンでは、国務省のメールアドレスをスプーフィングし、会議招待状に偽装したフィッシングメールを送信して合法性を高めました。ターゲットは国務省をテーマにした無害な PDF の餌を受け取り、これは偽のクラウド環境にアクセスし、特定の名前で ASPs を生成する方法を含んでいました。2 つのキャンペーンはそれぞれ異なる ASP テーマを特徴としており、攻撃インフラでは住宅用プロキシが使用されました。彼らは ASPs を通じてメールクライアントを設定し、被害者のメールにアクセスして読み取るために使用し、長期的なアカウントアクセスを保証しました。


SENSITIVE BUT UNCLASSIFIED (SBU)

United States Department of State

BUREAU OF INFORMATION RESOURCE MANAGEMENT (IRM)

Joining External Gmail Users to
US DoS Guest O365 Tenant

Prepared by: ENM
Document Release: Version 0.2
Mar 6, 2025

IRM

SENSITIVE BUT UNCLASSIFIED (SBU)

[図 5: SectorC33 グループが悪用した餌文書]

[Attack Flow]

1. [偵察] 被害者情報の収集 (T1592)
   a. 著名な学者および批判的な人物のリスト収集
   b. 対象の社会的関係および関心事の調査
2. [リソース開発] インフラの取得 (T1583)
   a. 住宅用プロキシおよび VPS サーバーの確保
   b. スプーフィングされたメールアドレスの生成
3. [初期アクセス] フィッシング (T1566)
   a. 会議招待状に偽装したフィッシングメールの送信
   b. スプーフィングされた国務省メールアドレスの使用
4. [実行] ユーザー実行 (T1204)
   a. PDF ドキュメントを開くよう誘導
   b. 偽のクラウド環境へのアクセス指示
5. [資格情報アクセス] アプリケーションアクセス トークンの盗難 (T1550)
   a. アプリケーション専用パスワード（ASP）の生成誘導
   b. 16 文字のパスコード共有の誘導
6. [持続性] アカウントの作成 (T1136)

a. メールクライアントに ASP 設定
b. 継続的なメールボックスアクセスの保証
7. [防御回避] 代替認証素材の使用 (T1550.003)
a. ASP を通じた 2 段階認証の回避
8. [指揮統制] 非標準ポート (T1571)
a. 非標準ポートを通じたデータ転送
b. 検出回避のためのインフラ再利用
9. [収集] メール収集 (T1114)
a. 被害者のメール内容の収集
b. 長期的なメールアクセスの維持

22) SectorD38 used Whisper & PrimeCache backdoors for cyberespionage operations (2025-06-05)

https://cti.nshc.net/events/view/15947

攻撃対象産業群: 政府・行政、通信

SectorD38 グループは、2017 年から少なくとも活動しているサイバー諜報グループであり、クルディスタン地域政府（Kurdistan Regional Government, KRG）およびイラク政府の高官を対象に攻撃を行ってきました。このグループは「Shahmaran」バックドアを利用してクルドの外交関係者を攻撃した際に初めて発見されました。その後、「Whisper」バックドアと「PrimeCache」IIS モジュールを開発し、攻撃対象を拡大してきました。Shahmaran バックドアは、コマンド＆コントロール（C&C）サーバーを通じてリモートコマンドの実行を可能にし、Whisper バックドアはマイクロソフトエクスチェンジサーバーのウェブメールアカウントにログインして、メールの添付ファイルを通じて通信しました。PrimeCache は IIS サーバー内でバックドアとして動作し、HTTP リクエストをフィルタリングしてコマンドを実行してきました。この他にも、「Laret」と「Pinar」というリバーストンネルおよび様々な補助ツールが使用されました。

[Attack Flow]

1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
a. ウェブサーバーの脆弱性を利用した初期アクセス
b. Flog ウェブシェルを通じたリモートコマンド実行
2. [実行] コマンドとスクリプトインタープリター (T1059)
a. cmd.exe を通じたコマンド実行
b. PowerShell を通じたスクリプト実行
3. [持続性] システムプロセスの作成または変更 (T1543)
a. Whisper プロトコルドロッパーを通じた持続性維持

b. P.S. Olala サービス登録

4. [権限昇格] 権限昇格制御メカニズムの悪用 (T1548)
   a. 管理者権限でのシステムアクセス
   b. 権限昇格のための脆弱性悪用
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. コード難読化を通じた検出回避
   b. パラメータ暗号化を通じた情報隠蔽
6. [資格情報アクセス] ブルートフォース (T1110)
   a. ウェブメールアカウントの資格情報奪取
   b. Whisper バックドアを通じた資格情報アクセス
7. [探索] システム情報探索 (T1082)
   a. ファイルおよびディレクトリの属性要求
   b. システム情報収集
8. [横移動] リモートサービス (T1021)
   a. RDAT バックドアを通じたリモートサービスアクセス
   b. Laret および Pinar リバーストンネル使用
9. [収集] ローカルシステムからのデータ (T1005)
   a. ファイルのアップロードおよびダウンロード
   b. 特定ファイル属性要求
10. [コマンド&コントロール] アプリケーション層プロトコル (T1071)
   a. HTTP リクエストを通じた C&C 通信
   b. メール添付ファイルを通じたコマンド送信
11. [データ流出] C2 チャネルを通じたデータ流出 (T1041)
   a. ファイルを C&C サーバーに送信
   b. コマンド結果をメールで送信

23) SectorE05 used Phishing Email with CHM Malware Disguised as Docs (2025-05-22)

https://cti.nshc.net/events/view/15581

攻撃対象産業群: 政府・行政、国防、エネルギー

SectorE05 グループは「外交部文書」というテーマでフィッシングメールを利用し、中国とパキスタンの政府および産業部門を標的にしました。このメールには悪性の添付ファイルが含まれており、「CHM」と「PDF」形式で圧縮されていました。被害者が「CHM」ファイルを開くと、定期的に「PowerShell」コマンドを実行するタスクが設定され、持続性が確保されました。「PDF」ファイルには悪性スクリプトが挿入され、ユーザーがフィッシングサイトに誘導されました。攻撃に使用さ

れたトロイの木馬は「wmRAT」と「MiyaRAT」で、これらはデータ収集、ファイル操作、リモートコマンド実行などの作業を行い、特定の C2 サーバーと通信を行いました。「wmRAT」は画面キャプチャやファイル操作などのコマンドを実行し、「MiyaRAT」は主に政府および防衛システムを標的にしました。また、新しい C#ベースのリモートアクセス型トロイの木馬と Python ベースの資格情報窃取ツールが、機密データを抽出するために使用されました。このキャンペーンは、合法的な文書形式を悪用して悪性ペイロードを配信する高度なソーシャルエンジニアリング技術を強調し、このような巧妙な脅威に対する警戒が必要であることを示しています。該当グループは CHM ファイル内に悪性スクリプトを挿入し、「ChromeCrashReport」という名前のタスクを生成し、このタスクは 15 分ごとに実行されるように設定されていました。計画されたタスクで生成されたネットワークパケットはホスト情報を含んでおり、特定の C2 サーバーにリクエストを送り、コマンドを受信します。コマンドは「Public」ユーザードキュメントの下に保存され、「cmd」を通じて実行されます。「wmRAT」は情報収集、ファイルのアップロードおよびダウンロード、コマンド実行などの機能を果たし、「MiyaRAT」は政府および防衛システムを標的に画面キャプチャおよびファイル操作を行います。

[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. 「外交部文書」をテーマにしたフィッシングメールの送信
   b. 「CHM」および「PDF」形式のマルウェア添付ファイルを含む
2. [実行] ユーザー実行 (T1204)
   a. ユーザーが「CHM」ファイルを開く
   b. 「PDF」ファイルをクリックするとフィッシングサイトに誘導
3. [持続性] スケジュールされたタスク/ジョブ (T1053)
   a. 「PowerShell」コマンドを定期的に実行するタスクを作成
   b. 「ChromeCrashReport」計画タスクを設定
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 サーバーにホスト情報を送信
   b. C2 サーバーからコマンドを受信して実行
5. [資格情報アクセス] パスワードストアからの資格情報 (T1555)
   a. Python ベースの資格情報窃取ツールを使用したデータ抽出
6. [収集] 画面キャプチャ (T1113)
   a. 「wmRAT」を使用した画面キャプチャの実行
   b. 「MiyaRAT」を使用した政府および防衛システムのスクリーンショット収集
7. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. C2 サーバーを通じたデータ流出
   b. 暗号化されたデータの送信および受信

8. [影響] データ操作 (T1565)
   a. ファイルの操作および削除
   b. システム情報の変更および操作

24) SectorE05 used WmRAT, Disguised as Security Brief Report.iqy (2025-05-28)

https://cti.nshc.net/events/view/15742

攻撃対象産業群: 通信

SectorE05 グループは 2025 年 5 月 7 日、インドとパキスタン間の緊張状況を背景に、パキスタンの通信会社 PTCL の主要人員を対象にスピアフィッシング攻撃を実行しました。該当グループは StealC インフォスティーラーを利用してパキスタン CTD のメールアカウントを奪取した後、そのアカウントから IQY ファイルが含まれたフィッシングメールを送信しました。IQY ファイルは Excel マクロを通じてコマンドラインベースで WmRAT の亜種をダウンロードおよび実行し、PNG に偽装されたペイロードを活用して検出を回避しました。WmRAT はユーザー情報、ファイルリスト、スクリーンショット、位置情報などを収集し、コマンド実行およびファイル奪取機能を実行します。マルウェアはレジストリおよび Roaming ディレクトリを通じて持続性を確保し、rdata セクションに暗号化された形で C2 ドメインを隠します。復号化された C2 は tradesmarkets[.]greenadelhouse[.]com であり、HTTPS 443 ポートを通じた HTTP GET 方式で通信した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. 盗用された「CTD」メール資格情報の使用
   b. 「PTCL」人員を対象に「IQY」添付フィッシングメールを送信
2. [実行] ユーザー実行 (T1204)
   a. 「IQY」ファイルを実行して悪性「Excel」マクロを作動
   b. 「CMD」コマンドを通じて「WmRAT」亜種をダウンロードおよび実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 「PNG」画像に偽装されたペイロードをダウンロード
   b. 「XOR」暗号化された「C2」サーバー文字列を使用
4. [持続性] レジストリ実行キー/スタートアップフォルダー (T1547.001)
   a. Windows レジストリに持続性を確保するためのレジストリキーを追加
   b. 「C:¥ProgramData」に「vcswin.exe」実行を指定
5. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
   a. HTTPS を通じた「C2」サーバーとの暗号化通信
   b. 「vrocean」パラメーターに Base64 でエンコードされたデータを使用

6. [収集] スクリーンキャプチャ (T1113)
   a. デスクトップのスクリーンショットをキャプチャ
   b. ユーザーおよびホスト情報を収集
7. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. 「C2」チャネルを通じたデータの流出
   b. ファイルの流出およびリモートファイルストリーム書き込みをサポート

25) SectorE05 used ArtraDownloader disguised as software updater (2025-06-04)

https://cti.nshc.net/events/view/15929

SectorE05 グループは 2016 年以降、継続的にマルウェア戦略を発展させてきました。初期には基本的なダウンロードプログラムから始まり、現在では洗練されたリモートアクセス型トロイの木馬（RAT）へと進化しました。このグループは主にカスタムペイロードを特殊な感染チェーンを通じて配信し、ペイロード自体に高度な解析回避技術を使用することを避けています。彼らの武器庫は一貫したコーディングパターンを示し、システム情報の収集や文字列の難読化を含んでいます。これは共通の開発基盤を示唆しています。2025 年まで活発な開発が続いており、新しいバージョンは以前のキャンペーンから追跡可能です。特に、「MuuyDownloader」や「BDarkRAT」を含む複数のマルウェアファミリーの変種は、このグループの継続的な戦術改善を示しています。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. カスタマイズされたペイロード添付
   b. 感染チェーンを通じた配信
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. ShellExecuteA API の使用
   b. PowerShell コマンドの実行
3. [持続性] レジストリ実行キー / スタートアップフォルダ (T1547.001)
   a. "Run"レジストリキーへの登録
   b. ハードコーディングされたパスへのコピー
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 文字列の難読化
   b. 簡単なエンコーディングアルゴリズムの使用
5. [資格情報アクセス] 入力キャプチャ (T1056)
   a. キーボード入力フックの設定
   b. クリップボード内容のキャプチャ
6. [探索] システム情報探索 (T1082)

a. システム情報の収集
b. ユーザー名、コンピュータ名、オペレーティングシステム情報の収集
7. [収集] スクリーンキャプチャ (T1113)
a. スクリーンショットのキャプチャ
b. ファイルシステムの探索
8. [流出] C2 チャネル経由の流出 (T1041)
a. C2 サーバーへのシステム情報の送信
b. ペイロードファイル名の抽出と送信
9. [コマンド＆コントロール] 暗号化チャネル (T1573)
a. AES-256-CBC 暗号化の使用
b. ネットワークパケットの暗号化

26) SectorE05 used Spearphishing with CHM Files for Espionage Operations (2025-06-04)

https://cti.nshc.net/events/view/15926

攻撃対象産業群: 政府・行政、国防、外交

SectorE05 グループは、政府および防衛産業を主要な攻撃対象とする諜報活動に注力するハッキンググループです。このグループは主に「インド標準時（IST）」のタイムゾーンで活動し、アジアおよびヨーロッパ内の中国、パキスタンなど近隣地域に関連する機関を攻撃対象としています。該当グループは巧妙なスピアフィッシングメールを通じて初期アクセスを試み、しばしば外交文書や政府機関の書類に偽装した餌文書を使用して攻撃対象の信頼を誘導します。このグループは「163[.]com」や「ProtonMail」といったプラットフォームを活用し、外国政府機関を装ってフィッシング攻撃の信頼性を高めます。彼らの主な目的は、外交政策、防衛、貿易に関連する情報を収集することです。また、彼らは「Let's Encrypt」証明書を使用して特定のドメインにビーコンを生成する予約作業を通じて Malware を配布し、さまざまなファイル形式（MSC、LNK など）を活用して攻撃の戦術的柔軟性を示します。作戦の指紋には、被害者の情報を内蔵した固有の「PHP URL」パターンと、インド標準時の業務時間中の一貫したインフラ設定が含まれます。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
a. スピアフィッシングメール送信
b. 添付ファイルまたはリンクを通じた Malware ダウンロード
2. [実行] スケジュールされたタスク/ジョブ (T1053.005)
a. 予約タスクを作成して Malware 実行
b. PowerShell および cmd.exe 使用

3. [防御回避] 偽装 (T1036)
   a. 外国政府機関を装う
   b. 文書およびメールの件名を偽装
4. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. HTTP(S)プロトコル使用
   b. Let’s Encrypt 証明書使用
5. [収集] 情報リポジトリからのデータ (T1213)
   a. 被害者システム情報収集
   b. コンピュータ名およびユーザー名を含む
6. [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 C2 サーバーに送信
   b. PHP URL パターン利用
7. [リソース開発] インフラの侵害 (T1583)
   a. 多様なドメイン登録および使用
   b. インドの業務時間に合わせたインフラ設定

27) SectorF01 used Shortcut File disguised as PDF for DLL Side-loading (2025-05-29)
https://cti.nshc.net/events/view/15864

2025 年 5 月、台湾でアップロードされた疑わしい ISO イメージに関連して、精巧なサイバー攻撃が識別されました。この ISO イメージには、システムを損傷させるために設計された 3 つのファイルが含まれています。該当グループは PDF ファイルに偽装したショートカットファイルで、隠されたファイルである MSI インストーラーと MST 変換を実行させます。この方法は、コマンドライン引数で渡された非セキュアな変換を使用してインストールプロセスを修正する MST 変換を悪用します。攻撃には「tbs.dll」ファイルを通じた DLL サイドローディングが含まれ、レジストリ実行キーを通じて持続性を提供します。高度な技術としては、関数フック、DLL パッチ、シェルコード実行などが使用されます。シェルコードは AES-256 および XOR を使用して復号化され、LZMA 解凍を通じて追加のペイロードが明らかになります。最後に、Rust で作成されたこの Malware は、静的にリンクされた libcurl を使用してコマンド＆コントロールサーバーと通信を設定し、偽装されたユーザーエージェント文字列を通じてリモート制御機能を実行しました。

[Attack Flow]
1. [実行] ユーザー実行 (T1204)
   a. PDF に偽装されたショートカットファイルの実行
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. MSI インストーラの実行

b. MST 変換の適用

3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. レジストリ実行キーの作成
   b. "PCHealthCheck.exe" 実行の持続性設定
4. [防御回避] DLL サイドローディング (T1574.002)
   a. "tbs.dll" サイドローディング
   b. "PCHealthCheck.exe" を通じた DLL 実行
5. [実行] フック (T1179)
   a. "RtlUserThreadStart" 関数のフック
   b. Malware で実行フローを転換
6. [防御回避] ファイルまたは情報の難読化解除/デコード (T1140)
   a. AES-256 および XOR を使用したシェルコードの復号化
   b. LZMA 解凍を通じて追加ペイロードが明らかに
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. コマンドおよびコントロールサーバーとの通信設定
   b. 偽装されたユーザーエージェント文字列の使用

28) SectorH03 used Ares RAT disguised as legitimate Indian domains (2025-05-23)

https://cti.nshc.net/events/view/15588

攻撃対象産業群: 健康、政府・行政、通信、国防、教育、金融、軍事機関、メディア・報道

SectorH03 グループは、インドの主要産業である防衛、政府 IT、医療、通信、教育部門を標的にしました。この攻撃は 2025 年 5 月 7 日から始まり、精巧なスピアフィッシング、ウェブサイトの改ざん、データ漏洩など、さまざまな攻撃手法が使用されました。.ppam、.xlam、.lnk、.msi 形式のマルウェアファイルは、マクロおよびスクリプトを通じて秘密のコマンド＆コントロール（C2）通信を確立するために利用されました。攻撃者はソーシャルエンジニアリング技術を使用して最新の問題を悪用し、インド内の合法機関を装ったスプーフィングドメインを通じて初期侵入を行いました。今回のキャンペーンは、ペイロードの配信とアプリケーション層プロトコルに基づく C2 通信など、精巧な TTPs を活用した作戦と評価されています。

[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. マルウェアファイル添付
   b. スピアフィッシングメール送信
2. [実行] コマンドおよびスクリプトインタープリター: PowerShell (T1059.001)
   a. マクロ実行

b. PowerShell スクリプト実行

3. [永続性] システムプロセスの作成または変更: Windows サービス (T1543.003)
   a. サービス作成
   b. サービス修正
4. [防御回避] ファイルまたは情報の難読化 (T1027)
   a. ファイル難読化
   b. スクリプト難読化
5. [資格情報アクセス] パスワードストアからの資格情報 (T1555)
   a. 資格情報収集
   b. パスワードストアアクセス
6. [探索] システム情報探索 (T1082)
   a. システム情報収集
   b. ネットワーク構成探索
7. [横移動] リモートサービス: SMB/Windows 管理共有 (T1021.002)
   a. SMB を通じた移動
   b. 管理共有使用
8. [収集] 画面キャプチャ (T1113)
   a. 画面キャプチャ
   b. スクリーンショット保存
9. [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データ送信
10. [影響] データ破壊 (T1485)
    a. データ削除
    b. ファイル破壊

29) SectorH03 used Android RAT disguised as Viber App for Surveillance (2025-06-03)

https://cti.nshc.net/events/view/15862

攻撃対象産業群: 政府・行政、軍事機関

SectorH03 グループは、大規模な VPS プロバイダーである「Contabo」のホスティングサービスを利用して、改変された Android リモートアクセス型トロイの木馬（RAT）である「CapraRAT」と「Crimson RAT」を配布しました。このマルウェアは、Android ユーザーだけでなく、Windows ユーザーも標的にしました。該当グループは、「Crimson RAT」のコマンド＆コントロール（C2）用に特定の IP アドレスを使用しました。悪意のある APK が「com.moves.media.tubes」というパッ

ケージ名を持ち、これらの IP と通信していることが発見され、これらは 2023 年のより大きなキャンペーンと関連していました。この中の 1 つの APK は、有名な通信アプリを装い、オーディオ録音、SMS の傍受、連絡先へのアクセス、精密な位置追跡などの広範な権限を持っていることが判明しました。

[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. ソーシャルエンジニアリングを通じた悪性 APK 配布
   b. 人気のある VoIP および IM アプリケーションの偽装
2. [実行] コマンドおよびスクリプトインタープリタ: Android (T1059.007)
   a. 修正された「CapraRAT」および「Crimson RAT」の実行
   b. マルウェア実行のためのスクリプト使用
3. [持続性] ブートまたはログオン自動開始実行 (T1547.001)
   a. システム再起動時にマルウェア自動実行
   b. アプリインストール後の持続的な悪性活動維持
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. APK ファイルのコード難読化
   b. 検出を回避するための権限隠蔽
5. [認証情報アクセス] 入力キャプチャ (T1056)
   a. ユーザー入力データのキャプチャ
   b. ログイン情報および機密情報の収集
6. [発見] システム情報の発見 (T1082)
   a. デバイス状態および情報の収集
   b. 位置情報および連絡先リストへのアクセス
7. [収集] ローカルシステムからのデータ (T1005)
   a. マイクを通じたオーディオデータの収集
   b. SMS および連絡先データの収集
8. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. コマンド＆コントロールサーバーとの通信
   b. 「161.97.180[.]199」IP を通じたデータ送信
9. [流出] C2 チャネルを介した流出 (T1041)
   a. 収集されたデータの C2 チャネルを通じた外部送信
   b. ネットワークトラフィックを通じたデータ流出

30) SectorK01 used WebDAV Exploit of CVE-2025-33053 for Middle East Espionage (2025-06-11)

https://cti.nshc.net/events/view/16024

攻撃対象産業群: 政府・行政、国防

SectorK01 グループは、トルコ、カタール、エジプト、イエメンの政府および防衛産業を主な標的として、精巧なサイバー攻撃を実行しました。この攻撃は、CVE-2025-33053 というゼロデイ脆弱性を利用してリモートコード実行を可能にし、操作された作業ディレクトリを通じて実行されました。彼らは合法的な Windows ツールである"iediagcmd.exe"を悪用し、制御する WebDAV サーバーからマルウェア実行ファイルを実行しました。初期感染ベクターとしては、".url"ファイルを含むスピアフィッシングメールが使用され、これは多段階のマルウェア配布につながりました。攻撃の核心要素は、"Mythic C2"フレームワークに基づくカスタムインプラントである"Horus Agent"の配布でした。"Horus Agent"は、分析防止措置を導入し、暗号化されたチャネルを通じてコマンド＆コントロールサーバーと通信しました。補完ツールとしては、キーロガー、パッシブバックドア、資格情報ダンピングのための特殊モジュールが実装されました。この攻撃には、DLL ハイジャック、コード難読化を通じたカスタムローダーの使用、LOLBins の活用などの高度な技術も含まれていました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
    a. スピアフィッシングメール送信
    b. ".url" ファイル添付
2. [実行] ユーザー実行 (T1204)
    a. .url ファイル実行
    b. iediagcmd.exe を通じた Malware 実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
    a. Malware 実行のための自動開始設定
    b. 持続的な感染維持
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
    a. コード難読化適用
    b. 分析防止措置導入
5. [資格情報アクセス] 資格情報ダンピング (T1003)
    a. 資格情報ダンパー使用
    b. ドメインコントローラーから資格情報抽出
6. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
    a. 暗号化されたチャネルを通じた C2 通信
    b. RC4 および AES 暗号化使用
7. [データ流出] 代替プロトコルを通じたデータ流出 (T1048)

a. 代替プロトコルを通じたデータ流出
b. ウェブベースのプロトコル活用

31) SectorS01 used VBS Malware for Multi-Stage RAT Deployment (2025-06-10)
https://cti.nshc.net/events/view/16099

SectorS01 グループのサイバー脅威活動が確認されました。彼らは難読化された Visual Basic Script ファイルを含む 16 のオープンディレクトリクラスターを運営し、これを通じて「Remcos」、「LimeRAT」、「DCRat」、「AsyncRAT」などのリモートアクセス型トロイの木馬（RAT）を配布する 3 段階のマルウェアインストールプロセスを実行します。初期段階では、難読化された VBScript が実行され、base64 でエンコードされたペイロードをデコードし、PowerShell ベースのステージャーを生成します。このスクリプトはインターネットアーカイブなどから画像またはテキストファイルに偽装されたコンポーネントをダウンロードし、メモリインジェクターを通じて最終的な RAT をロードします。C2 インフラストラクチャは duckdns[.]org などの動的 DNS サービスを活用して IP アドレスを定期的に変更していると分析されています。全体の[Attack Flow]は、メモリ内ロードとインターネットベースのコンテンツ隠蔽を通じて検出を回避し、さまざまな RAT ツールを活用して感染システムに持続的なリモート制御権限を確保することに重点を置いています。

[Attack Flow]
1. [初期アクセス] フィッシング (T1566)
   a. マルウェア VBS ファイルをフィッシングメールで配布
   b. ステージ 1 ドロッパーとして VBS スクリプトを実行
2. [実行] コマンドとスクリプトインタープリター (T1059)
   a. 難読化された VBScript を実行
   b. PowerShell スクリプトを生成および実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. PowerShell スクリプトで持続性を確保
   b. システム再起動時に自動実行を設定
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. VBS スクリプトの難読化
   b. base64 エンコードでファイルを隠す
5. [資格情報アクセス] 入力キャプチャ (T1056)
   a. RAT を通じたキーロギング
   b. スクリーンショットのキャプチャ
6. [探索] システム情報探索 (T1082)
   a. システム情報の収集

b. ネットワーク設定の把握
7. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
a. C2 通信のための動的 DNS の使用
b. duckdns[.]org で IP アドレスを回転
8. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. 収集された情報を C2 に送信
b. 継続的なデータ流出の管理

32) SectorT01 used spear phishing to exploit Roundcube vulnerability (2025-06-05)
https://cti.nshc.net/events/view/15946

SectorT01 グループのスピアフィッシングキャンペーンは、ポーランドの攻撃対象を狙い、「Roundcube」の脆弱性「CVE-2024-42009」を悪用しました。この脆弱性は、メールを開いたときに JavaScript の実行を許可し、ユーザーの資格情報を盗むことを目的としています。該当グループは、「[!IMPORTANT] Invoice to reservation number: S2500650676」といった件名のメールを送信し、ユーザーが迅速に行動するよう促しました。ユーザーがメールを開くと、悪性 JavaScript がブラウザに「サービスワーカー（Service Worker）」をインストールし、ユーザーがウェブメールにアクセスする際にログイン資格情報をキャプチャします。これらの資格情報は、彼らが制御するサーバーに送信されます。マルウェアはサービスワーカーを利用してバックグラウンドで実行され、持続性を維持し、ウェブメールのログイン要求を傍受します。「CVE-2025-49113」という新しい脆弱性が悪用された証拠はありませんが、他の攻撃と組み合わされると効果的な攻撃チェーンになるリスクがあります。攻撃は古いバージョンの「Roundcube」のインストールを必要とし、これはアップデートの重要性を強調しています。

[Attack Flow]
1. [偵察] スピアフィッシング添付ファイル (T1566.001)
a. ポーランドの攻撃対象にフィッシングメールを送信
b. "CVE-2024-42009" 脆弱性を悪用するためのメール作成
2. [実行] ユーザー実行: 悪意のあるリンク (T1204.001)
a. メールを開くと JavaScript が実行される
b. ユーザーがメールを開くとマルウェアが活性化
3. [持続性] サービスワーカーのインプラント (T1505.003)
a. ブラウザにサービスワーカーをインストール
b. サービスワーカーを通じて持続性を維持
4. [資格情報アクセス] 入力キャプチャ: 資格情報収集 (T1056.001)
a. Web メールのログイン試行時に資格情報をキャプチャ

b. キャプチャされた資格情報を攻撃者のサーバーに送信
5. [収集] 情報リポジトリからのデータ (T1213)
a. メールボックスの内容を分析
b. アドレス帳をダウンロードし、フィッシングメッセージを追加送信
6. [流出] 代替プロトコルによるデータ流出 (T1048)
a. キャプチャされた資格情報および追加データを攻撃者のサーバーに送信

2. サイバー犯罪（Cyber Crime）ハッキンググループの活動

1) SectorJ01 used Fake Browser Updates for NetSupport RAT Delivery (2025-06-13)

https://cti.nshc.net/events/view/16097

攻撃対象産業群: 金融、小売、観光・宿泊

SectorJ01 グループは最近、新しいインフラを活用して攻撃を展開しました。このインフラには、ペイロード配布用のドメインと関連 IP が含まれています。主要なツールとしては、PowerShell ベースのカスタムローダー「PowerNet」と難読化された FakeBat の亜種「MaskBat」が特定されました。グループのサブキャンペーン「GrayAlpha」は、偽のブラウザ更新ページ、悪性 7-Zip ダウンロードサイト、TDS TAG-124 トラフィック誘導ネットワークの 3 つの主要な感染ベクターを活用しており、この中で TDS TAG-124 は新たに観察された手段です。活性化されたインフラは主にバレットプルーフホスティングに基づいており、2025 年 4 月まで登録された偽の 7-Zip 配布サイトが使用された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. フィッシングメール送信
b. マルウェアリンク含む
2. [実行] PowerShell (T1059.001)
a. "PowerNet" ローダー使用
b. "NetSupport RAT" 実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
a. システム起動時自動実行設定
b. レジストリキー修正
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. "MaskBat" 難読化

b. コードストリング隠蔽

5. [コマンド＆コントロール] ウェブサービス (T1102)
   a. ペイロードダウンロード
   b. C2 サーバーと通信
6. [影響] データ破壊 (T1485)
   a. システムファイル削除
   b. ログデータ損傷

2) SectorJ02 used more_eggs Backdoor disguised as Resumes on AWS (2025-06-10)
https://cti.nshc.net/events/view/16043

SectorJ02 グループは、経済的利益を目的として活動するサイバー犯罪グループであり、時間の経過とともに戦術を進化させてきました。初期には「POS（Point-of-Sale）」システムの侵害や大規模な決済カードの盗難で悪名を馳せましたが、現在は企業を対象とした高度なソーシャルエンジニアリングキャンペーンに転換しています。彼らは「LinkedIn」や「Indeed」といった求人プラットフォームを悪用し、求職者を装って人事担当者との信頼を築いた後、フィッシングメールを送信します。フィッシングメールにはクリック可能なリンクは含まれておらず、受信者が URL を手動で入力するよう誘導してセキュリティフィルターを回避します。使用されるドメインはしばしば実際の応募者の名前を模倣し、「GoDaddy」を通じて匿名で登録されます。このグループは「AWS」などのクラウドサービスを利用してフィッシングサイトをホスティングし、「CloudFront」を通じて出所を隠蔽し、インフラを維持します。被害者が家庭用 IP や一般的なブラウザを使用するなど特定の条件を満たす場合、CAPTCHA を通じて悪性「ZIP」ファイルをダウンロードするよう誘導されます。この ZIP ファイルには偽装された「.LNK」ファイルが含まれており、これは「JavaScript」を実行して「More_eggs」バックドアを配布します。攻撃チェーンは「PowerShell」の実行とスケジュールされたタスクを通じた持続性と回避技術を使用し、信頼できるインフラに支えられた階層的フィッシング戦術の効果を強調します。

[Attack Flow]

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
   a. 求職者を装ったメール
   b. 手動入力 URL を含む
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. ZIP ファイル内の.LNK ファイルを実行
   b. wscript.exe で隠された JavaScript を実行
3. [持続性] スケジュールされたタスク/ジョブ (T1053)
   a. スケジュールされたタスクを作成

b. レジストリ実行キーを追加
4. [防御回避] 偽装 (T1036)
a. 信頼できるクラウドサービスを使用
b. CloudFront で出所を隠蔽
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: ウェブプロトコル (T1071.001)
a. HTTPS プロトコルを使用
b. スプーフィングされた User-Agent ヘッダー
6. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. HTTPS を通じたデータの外部送信
b. コマンド＆コントロール（C2）チャネルを利用

3) SectorJ25 used RAT Malware and exploited Vulnerability (2025-06-04)

https://cti.nshc.net/events/view/15941

Chaos RAT は、Golang で作成されたオープンソースのリモートアクセスツールであり、ハッカーが Linux と Windows システムを侵害して悪意のある活動を行うために使用しました。本来は合法的なリモート管理ツールとして意図されていましたが、Chaos RAT のクロスプラットフォームサポート機能と簡単なアクセス性のため、サイバー犯罪者に好まれました。このマルウェアは 2022 年 11 月に実際の攻撃で初めて発見されました。主に暗号通貨マイニングキャンペーンで使用され、主にフィッシングメールを通じて被害者に配信され、悪意のあるスクリプトを展開してクローンタブ(crontab)ファイルを変更することで持続性を維持します。「Chaos RAT」の管理パネルは、該当グループがペイロードを生成し、セッションを管理し、コンピュータを制御できるようにします。この RAT の主な機能には、ファイル管理、リバースシェルアクセス、スクリーンショットキャプチャ、システム再起動、ターミナルコマンドとリモートコード実行などが含まれます。このマルウェアは、コマンド＆コントロールサーバーとの通信に JWT を認証手段として使用し、オペレーティングシステムに特化した実行パスに基づいて作業を行います。重要な脆弱性である「CVE-2024-30850」は、サーバー側のコマンドインジェクションを許可し、スクリプティング攻撃を通じた追加の悪用を可能にします。オープンソースの特性により、出所の追跡が難しく、さまざまなサイバー脅威に容易に適応できるため、オープンソースソフトウェアの二重使用問題を強調します。

[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試行
b. マルウェアリンクまたは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. スクリプトを通じて crontab ファイルを変更

b. サーバー側のコマンド実行

3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. crontab ファイルを使用した持続性維持
   b. リモートペイロードの更新可能
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. アカウント権限昇格のための脆弱性悪用
   b. システム制御権限の確保
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. Base64 エンコードを通じたデータ隠蔽
   b. ランダムなフィールド名の使用による検出回避
6. [資格情報アクセス] 安全でない資格情報 (T1552)
   a. 管理パネルのデフォルト資格情報使用
   b. 認証トークンの利用
7. [探索] システム情報探索 (T1082)
   a. システムメタデータおよびネットワーク情報の収集
   b. OS および使用環境のプロファイリング
8. [収集] ローカルシステムからのデータ (T1005)
   a. スクリーンショットのキャプチャおよびサーバー送信
   b. ファイルの探索およびダウンロード
9. [コマンドと制御] アプリケーション層プロトコル (T1071)
   a. C2 サーバーとの通信に JWT を使用
   b. コマンドおよび制御サーバーとの持続的接続維持
10. [影響] システムシャットダウン/再起動 (T1529)
    a. システム再起動および終了コマンドの実行
    b. ユーザーログアウトおよびロック機能の使用
11. [流出] C2 チャネルを通じた流出 (T1041)
    a. C2 チャネルを通じたデータ送信
    b. Base64 エンコードされた結果の送信

4) SectorJ109 used Malware disguised as Todesk Installer for Control (2025-06-06)

https://cti.nshc.net/events/view/15952

攻撃対象産業群: 製造、IT

SectorJ109 グループは、リモートコントロール、暗号通貨のマイニング、DDoS 攻撃などを含む様々な悪意のある行為を行っています。最近、このグループはウォータリングホールウェブサイトを悪用して被害者のデバイスに Malware を拡散しており、これは SEO 最適化を通じて合法的に見える偽

のソフトウェアダウンロードサイトからトロイの木馬を配布する方法で行われました。攻撃の過程で、被害者を誘導して悪意のあるインストールパッケージをダウンロードさせ、その中には実行時に「Winos4.0」リモートコントロールツールを仕込む「Todesk」パッケージが含まれていました。攻撃は「Silverfox」トロイの木馬、シェルコードバックドア、アンチウイルス回避技術などを活用しました。感染したシステムは特定のポートを使用してコマンド&コントロールサーバーと通信しました。また、この Malware は Windows Defender の除外設定を修正し、定期的なタスクの実行を通じて持続性を維持しました。

[図 6: SectorJ109 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] ドライブバイ妥協 (T1189)
    a. ウォータリングホールウェブサイトの活用
    b. SEO 最適化された偽ソフトウェアダウンロードサイトの使用
2. [実行] コマンドとスクリプトインタープリタ (T1059)
    a. PowerShell を通じたコマンド実行
    b. cmd.exe を利用した regsvr32 の呼び出し
3. [持続性] レジストリの変更 (T1112)
    a. Windows Defender の除外設定の修正
    b. 定期的なタスク実行のためのレジストリエントリの追加
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
    a. シェルコードバックドアのインストール

b. システム権限での実行

5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 正常なコード内に Malware を隠す
   b. アンチウイルス検出回避技術の使用
6. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. システム情報の収集
   b. 資格情報の奪取試行
7. [探索] システム情報の探索 (T1082)
   a. システムプロセスのモニタリング
   b. ローカルシステム情報の収集
8. [横移動] リモートサービス (T1021)
   a. リモートコントロールツールの配布
   b. ネットワーク内の他のシステムへの移動
9. [収集] ローカルシステムからのデータ (T1005)
   a. ローカルファイルシステムからのデータ収集
   b. 収集した情報の C2 サーバーへの送信
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 サーバーとの特定ポート通信
    b. 悪性トラフィック隠蔽のためのプロトコル使用
11. [流出] C2 チャネルを介した流出 (T1041)
    a. 収集されたデータの C2 サーバーへの送信
    b. 継続的な C2 通信を通じたコマンド受信
12. [影響] データ破壊 (T1485)
    a. システムファイルまたはログの削除
    b. 感染痕跡の除去試行

5) SectorJ222 distributed Loader Malware via phishing emails (2025-05-27)

https://cti.nshc.net/events/view/15694

攻撃対象産業群: 航空宇宙、エネルギー、工学、社会基盤施設

SectorJ222 グループは 2025 年 3 月、ロシアとモルドバのエネルギー、核、航空機、機械工学などの主要産業を対象に 2 件のサイバー攻撃キャンペーンを実施しました。攻撃者はフィッシングメールを通じて信頼される機関を装い、悪意のある ZIP ファイルを配布しました。この ZIP ファイルには C#ベースの難読化されたローダーが含まれていました。ローダーは C2 サーバーと通信して追加のペイロードをダウンロードするよう設計されており、このペイロードは合法的な実行ファイルおよび PDF に偽装されていました。悪意のあるロジックは、複雑な難読化、DLL サイドローディング、

XOR ベースの文字列暗号化、エンコードされた命令シーケンスを含んでおり、これにより検出を回避しました。攻撃チェーンの初期には、対象環境を事前評価する手順が含まれており、条件が満たされない場合、サンドボックス回避のために非悪意のペイロードを代替送信する方法が適用されました。両キャンペーンともに巧妙な検出回避技術を活用して攻撃成功率を最大化し、フィッシングメールを基にした侵入とローダー中心の階層的ペイロード展開方式が特徴です。

[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. マルウェアを含む「ZIP」ファイル
2. [戦術] 実行 (T1204)
   a. 「LNK」ファイル実行
   b. 「JScript.NET」コードコンパイル
3. [戦術] 防御回避 (T1140)
   a. 難読化された「C#」ローダー使用
   b. 「XOR」暗号化で文字列難読化
4. [戦術] 永続化 (T1547)
   a. 「startapp.bat」バッチスクリプト生成
   b. スタートフォルダにペイロード保存
5. [戦術] コマンド＆コントロール (T1105)
   a. 「C2」サーバーからペイロードダウンロード
   b. 「User-Agent」ヘッダー使用
6. [戦術] 発見 (T1083)
   a. システム環境確認
   b. 特定条件未満時に代替ファイルダウンロード
7. [戦術] 実行 (T1059)
   a. 「cmd.exe」でコマンド実行
   b. 「MSBuild」を通じて「C#」コンパイルおよび実行

6) SectorJ223 used Fake AI Tool Websites to distribute Malware (2025-05-27)

https://cti.nshc.net/events/view/15702

SectorJ223 グループは 2024 年 11 月から人工知能（AI）ツールへの一般の関心を悪用し、Malware を配布するキャンペーンを展開しています。彼らは偽の「AI ビデオジェネレーター」ウェブサイトを通じて Malware を拡散し、ソーシャルメディア広告を使用してユーザーをこれらの悪意のあるサイトに誘導しています。これらの広告は Facebook や LinkedIn のようなプラットフォーム

で広く拡散され、数百万のユーザーに露出しました。主に Python ベースの情報窃取およびバックドア Malware が AI 生成コンテンツに偽装されたダウンロード可能な ZIP ファイルを通じて配布されます。これらの偽サイトにアクセスすると、多段階のペイロードが実行され、STARKVEIL ドロッパーを通じて XWORM や FROSTRIFT のようなモジュラーMalware ファミリーが配布されます。これらの Malware の亜種は、DLL サイドローディングやプロセスインジェクションのような高度な技法を使用し、Tor や Telegram のような通信チャネルを活用して C2 活動を行い、ログイン資格情報や機密データを標的としています。このキャンペーンは世界中のさまざまな産業に影響を与えており、ドメインローテーションのような持続的な戦術を使用して検出を回避しています。

[図 7: 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広告でユーザーを誘引
   b. 偽の AI ツールウェブサイトにリダイレクト
2. [実行] ユーザー実行 (T1204)
   a. ZIP ファイルをダウンロードして実行
   b. STARKVEIL ドロッパーを実行
3. [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を通じた Malware 実行
   b. DLL サイドローディング技術を使用
4. [持続性] ブートまたはログオン自動開始実行 (T1547)

a. AutoRun レジストリキーを使用
b. 持続的実行のためのバックドアをインストール
5. [コマンド＆コントロール] 暗号化チャネル (T1573)
a. Tor ネットワークを通じた C2 サーバー接続
b. Telegram を通じた情報送信
6. [収集] 入力キャプチャ (T1056)
a. キーロギングを通じた入力情報収集
b. ブラウザー拡張プログラムを通じた情報窃取
7. [データ流出] 代替プロトコルを通じたデータ流出 (T1048)
a. Telegram API を通じたデータ流出
b. Malware ネットワークを通じた機密データ送信

7) SectorJ224 exploited CVE-2025-32432 for RCE in Craft CMS (2025-05-27)
https://cti.nshc.net/events/view/15683

SectorJ224 グループは、Craft コンテンツ管理システム（CMS）を標的にして、リモートコード実行（RCE）脆弱性 CVE-2025-32432 を悪用しました。この脆弱性は 2025 年 2 月中旬から 5 月初旬まで活発に悪用され、CMS バージョン 3.0.0-RC1 から 5.6.17 までに影響を与えました。該当グループはウェブシェルを注入してコマンド実行を可能にすることで、非認可の初期アクセスを獲得し、その後、マルウェアシェルスクリプトをダウンロードして実行しました。感染チェーンは、「4l4md4r」という大型 ELF および「IPRoyal」という住宅用プロキシウェアを含む複数のペイロードを実行するローダーの配布につながりました。ローダーはまた、特定のモネロウォレットに設定された「XMRig」という暗号通貨マイナーをインストールしました。追加の分析結果、この脅威活動はトルコに位置するプロファイルと関連付けられ、これは IP アドレスの使用および PoC エクスプロイトを共有する TikTok 活動を通じて証明されました。彼らは動的リンカーハイジャックおよびランサムウェア配布などの技術を使用して、オペレーションを隠蔽しようとしたと分析されています。

[Attack Flow]
1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
a. CVE-2025-32432 脆弱性の悪用
b. Web シェルの注入
2. [実行] コマンドとスクリプトインタープリタ (T1059)
a. コマンド実行のための Web シェル使用
b. 4l4md4r.sh スクリプトのダウンロードと実行
3. [持続性] 内部プロキシのインプラント (T1090.002)
a. IPRoyal プロキシウェアのインストール

b. レジデンシャルプロキシの設定
4. [防御回避] 実行フローのハイジャック (T1574.005)
a. 動的リンカのハイジャック
b. /etc/ld.so.preload の修正
5. [実行] ネイティブ API (T1106)
a. ELF バイナリ 4l4md4r の実行
b. 알람다르.so ライブラリの実行
6. [実行] スケジュールされたタスク/ジョブ (T1053)
a. XMRig マイナーの設定と実行
b. モネロウォレットへの接続
7. [発見] ファイルとディレクトリの発見 (T1083)
a. 書き込み可能なディレクトリの検索
b. ペイロードのドロップと実行
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. データ暗号化の試み

8) SectorJ225 used Tycoon2FA PhaaS to Bypass MFA and Phish Credentials (2025-05-28)

https://cti.nshc.net/events/view/15736

SectorJ225 グループは、2023 年 9 月からサービス型フィッシング（PhaaS）プラットフォームである「Dadsec」と「Tycoon2FA」を利用した大規模なフィッシングキャンペーンを継続的に実施しています。攻撃者は、メールリンクまたは QR コードを通じて被害者をフィッシングページに誘導し、主にマイクロソフトのログインページを装って資格情報を盗み、多要素認証（MFA）を回避します。彼らは、固有の URL 構造や res444.php などの特定の PHP リソースを活用し、AES ベースの復号化技術とコード難読化で分析を妨害します。収集された資格情報とセッションクッキーは攻撃者のサーバーに送信され、MFA を回避してアカウントに継続的にアクセスできるようにします。
Tycoon2FA は、ユーザーフレンドリーなインターフェース、カスタマイズ可能なフィッシングテンプレート、自動化機能を統合したキットを提供し、最新のキャンペーンでは HTML ボディハッシュとページタイトルが一致するフィッシングウェブページが使用されました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
a. メールリンクまたは QR コードでフィッシングページを配布
b. フィッシングページが Microsoft ログインページを装い、資格情報を収集

2. [資格情報アクセス] 中間者攻撃 (T1557)
   a. 攻撃者制御サーバーで資格情報の中間者攻撃を実行
   b. セッションクッキーを収集して MFA を回避
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. AES 復号化でコードを隠蔽
   b. 高度な難読化および分析妨害機能を使用
4. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. 収集された資格情報を攻撃者制御サーバーに送信
   b. セッションクッキーを送信し、継続的なアカウントアクセスを維持
5. [コマンド＆コントロール] 暗号化チャネル (T1573)
   a. 暗号化されたチャネルを通じて C2 通信
   b. 被害者情報の安全な送信および処理

9) SectorJ231 used CHAINVERB Malware disguised as Signed Documents (2025-06-04)

https://cti.nshc.net/events/view/16048

攻撃対象産業群: 金融

2024 年 2 月 13 日、ConnectWise ScreenConnect バージョン 23.9.7 以下に脆弱性が公開され、2025 年 5 月からその脆弱性を悪用した攻撃が急増しています。特にグローバルな金融機関を狙ったフィッシングキャンペーンで脅威が集中的に観察されており、該当グループは「CHAINVERB」ダウンローダーに関連したデジタル署名のマルウェアドロッパーを活用しました。このドロッパーは「.top」または「dns.net」TLD を使用する eCrime ベースのインフラと接続されており、署名の偽造または悪用された「ConnectWise LLC」署名を含んでいます。「CHAINVERB」はデジタル証明書に埋め込まれた C2 URL を通じて二次ペイロードをダウンロードし、感染したシステムに ConnectWise Control リモートアクセスツールをインストールします。これにより、彼らはスクリーンショットのキャプチャ、内部ネットワークの偵察などの情報収集を行うことができます。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 請求書テーマのフィッシングメール送信
   b. メール内にマルウェア URL を含む
2. [実行] ユーザー実行 (T1204)
   a. ユーザーがマルウェアファイルを実行
   b. "CHAINVERB" ダウンローダーを実行
3. [持続性] 有効なアカウント (T1078)

a. "ConnectWise Control" リモートアクセスツールをインストール
b. 定期的なリモート接続を維持
4. [防御回避] コード署名 (T1553.002)
a. デジタル署名の悪用
b. "ConnectWise LLC" で偽の署名
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. デジタル証明書内蔵のコマンド＆コントロール URL を活用
b. 追加ペイロードのダウンロードと実行
6. [収集] スクリーンキャプチャ (T1113)
a. 内部システムのスクリーンショットをキャプチャ
b. 偵察情報を収集

10) SectorJ234 used ClickOnce for Windows Malware Disguised as Updates (2025-06-19)

https://cti.nshc.net/events/view/16255

SectorJ234 グループは 2023 年から活動を開始し、2025 年 4 月に再び活動を再開しました。このグループは主に暗号通貨の窃取を目的として情報窃取型 Malware（Infostealer）を配布する技術を採用しました。彼らは偽のオンラインプロジェクトを通じて被害者を誘引しています。現在の彼らの運営方法は、合法的なプロジェクトを模倣した複製ウェブサイトを生成し、Windows および macOS ユーザーにダウンロードを提供することです。Windows プラットフォームでは、Microsoft の「ClickOnce」アプリケーション配布を悪用し、DLL マニフェストリダイレクションを通じて SmartScreen セキュリティを回避し、Malware ペイロードを目立たないように実行します。これらのペイロードには主に「StealC」や「Rhadamanthys」といった情報窃取型 Malware が含まれており、機密データや暗号通貨ウォレット情報の収集に重点を置いています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
a. 偽のオンラインプロジェクトの使用
b. フィッシングによる誘引
2. [実行] ユーザー実行 (T1204)
a. ClickOnce アプリケーションの実行
b. DLL マニフェストリダイレクション
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
a. XWorm を通じた持続性の確保
b. 追加の Malware 配布準備

4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 自己署名証明書の使用
   b. SmartScreen 回避
5. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. StealC を通じた資格情報の収集
   b. Rhadamanthys を通じた暗号通貨ウォレット情報の収集
6. [収集] ローカルシステムからのデータ (T1005)
   a. 敏感なデータの収集
   b. 暗号通貨ウォレットデータの収集
7. [流出] C2 チャネルを通じた流出 (T1041)
   a. C2 チャネルを通じたデータ流出
   b. ログおよび収集データの送信
8. [コマンド＆コントロール] 暗号化チャネル (T1573)
   a. 暗号化されたチャネルの使用
   b. 通信の隠密性の維持

今月のサイバー脅威の特徴

2025 年 6 月の 1 か月間に観測された脅威イベントは、多数の APT グループが多様な戦術を駆使して、政治的・金銭的目的を同時に追求する複合的な様相を呈していました。ハッキンググループは特にソーシャルエンジニアリングと脆弱性の悪用を巧みに組み合わせ、正規のサービスやソフトウェアインフラを攻撃ベクターとして活用することで、検出回避能力を一層強化しました。このような傾向は、暗号通貨産業、学界、政府機関、軍事組織、SaaS ベースのインフラなど、攻撃対象の拡大とも連動しています。

最も顕著な特徴は、暗号通貨関連の従事者および開発環境をターゲットにした攻撃の高度化です。攻撃者は、NFT プロジェクト、Web3 ライブラリ、フリーランスの提案書など、実在する可能性が高い資料に偽装した文書またはリポジトリを通じて被害者のシステムにアクセスしました。特に、Node.js、React、Supabase、GitHub など、開発者に馴染みのある技術環境が集中的に悪用され、被害者のデバイスに個人キー、API トークン、GitHub 認証情報を盗む悪性ペイロードを挿入する方法が主流となりました。これに加えて、macOS をターゲットにした Malware の配布も並行して行われ、プラットフォームの観点でも従来の Windows 中心からの拡張が確認されました。

また、学界、社会運動団体、軍事機関などを対象としたフィッシングベースの攻撃も広範囲に観察されました。攻撃者は、メールフィルタリングを回避するために SPF/DKIM 認証を通過する方法でフィッシングメールを送信し、AppleSeed、KimJongRAT、PowerShell スクリプトなどを活用した多段階の Malware 感染を試みました。彼らは、正規のソフトウェアである AnyDesk、Zoom、

Dropbox、GoogleDrive などをコマンド＆コントロール（C2）チャネルとして悪用し、被害者の相互作用を誘導する社会工学技法は、受信者の職種と活動領域に合わせてカスタマイズされました。
6 月の脅威イベントでは、サーバー側の脆弱性の悪用が依然として主要な侵入ベクターとして利用されました。MS SQL サーバー、RDP、WebDAV などの旧式システム環境はもちろん、Ivanti EPMM、Commvault Metallic などのエンタープライズソリューションのゼロデイ脆弱性が積極的に悪用されました。攻撃者は侵入後、拡張ストアドプロシージャ形式のバックドアをインストールしたり、ウェブシェルの挿入、資格情報の収集、認証トークンの窃取、ラテラルムーブメントなどを行いました。これらの攻撃は主にアジアおよびヨーロッパ地域の公共機関および民間企業を対象に行われ、一部のキャンペーンでは Sliver フレームワーク、KrustyLoader などの高度な攻撃フレームワークも活用されました。
社会工学に基づく戦術は、国・言語・職業に応じてさらに精巧化されており、Roundcube、Outlook NTLM、ウェブメールスクリプトの脆弱性など、メールクライアントの脆弱性を直接利用する事例も登場しました。アメリカ国務省、国税庁、国内の大学など権威ある機関を装ったフィッシングメールは、ASP の奪取、MFA の回避、長期的なメールアクセス権の確保などにつながり、ユーザーが疑うことなく添付ファイルやリンクをクリックするよう誘導する方法がほとんどでした。
Android を基盤とした攻撃も多数確認されました。CapraRAT などのモバイル用 RAT を活用したキャンペーンでは、ビデオ通話、テキストメッセージ、位置情報の窃取、通話録音など、デジタル監視レベルのマルウェア機能が搭載されており、Google アカウントを窃取するためにアクセシビリティ権限を誘導する戦術が活用されました。このように、攻撃者は単一のプラットフォームに依存せず、Windows、macOS、Android までを包括するマルチプラットフォーム戦略を策定していました。
攻撃の展開方法も進化しました。従来のように単純にマルウェアを配布したり、単一の C2 チャネルを運営するのではなく、Zoom や Calendly のようなスケジュール管理ツールに C2 URL を挿入したり、Supabase のようなサーバーレスバックエンドを通じてコマンドを送信するなど、検出を困難にする方法が多く活用されました。これらの方法は特にクラウドベースのセキュリティシステムの限界を狙ったものと判断されます。

今月のサイバー脅威の示唆点

2025 年 6 月の脅威イベントは、技術的侵入に限定されず、情報収集・サプライチェーン侵害・アカウント奪取・インフラ破壊までを含む長期的なサイバー作戦の性格を強く示しました。特に注目すべき点は、攻撃者が高リスクの脆弱性を迅速に武器化し、セキュリティ対応のゴールデンタイムを事実上無力化していることです。CVE-2025-4427、CVE-2025-3928、CVE-2025-32432 などは公開直後に短期間で実際の攻撃に利用され、一部はすでにゼロデイとして長期間にわたり密かに悪用されていた状況も捉えられました。これは「情報公開 → 武器化 → 攻撃」までの転換サイクルが急激に

短くなっていることを意味し、従来の受動的なセキュリティ運用方式では脅威に追いつくのが難しいという現実を示しています。

今月の脅威で特に目立ったもう一つの動きは、セキュリティの盲点を狙う攻撃戦略です。ハッキンググループは、伝統的な企業や政府機関を超えて、ジャーナリスト、教授、市民団体の活動家など、従来の脅威モデルから外れた人的資産を精密に狙いました。国税庁を装ったメール、論文依頼を偽装したメッセージ、特定の海外機関からの送信を装ったリンクファイルなどは、受信者の職務に関連した文脈を反映したソーシャルエンジニアリングで構成されており、単純な添付ファイル感染を超えて権限の確保や長期的なアクセスを目指した精巧な侵入が行われました。このような動きは、セキュリティの範囲を技術的資産から人的資産にまで拡大する必要性を強く示唆しています。

開発者と SaaS プラットフォームをターゲットにした攻撃も今月の主要な軸でした。ハッキンググループは ethers.js、Supabase、GitHub、NPM などの開発環境を狙い、偽のプロジェクトや Malware が挿入されたリポジトリを通じてサプライチェーンへの侵入を試みました。これは開発段階から Malware が含まれて製品化されたり、開発者アカウントが奪取されて外部からの完全性検証が難しくなる状況につながる可能性があります。既存のセキュリティモデルはこのような「開発者自体を標的とする」攻撃に対応するには非常に脆弱であり、MFA の適用、依存性の検証、CI/CD 上のセキュリティポリシーの再設計などが必要であることが明らかになりました。

技術的戦術の観点から見ると、今月の脅威は EDR やシグネチャベースの検出を回避する戦術が目立ちました。PowerShell、JavaScript、AppleScript などの様々なスクリプト言語が交差して使用され、コマンド＆コントロール（C2）チャネルは特定の IP や URL に限定されなくなりました。Dropbox、Google Drive、Zoom、Calendly、Supabase などの正規のクラウドサービスを悪用する方法が一般化し、セキュリティ検出装置の観点からは「正常な行為」と誤認される可能性が高まっています。C2 とユーザー間の通信フローを単純に識別する方法はすでに無力化されており、今では行動ベースの検出とシナリオ中心の脅威分析が重要な対応戦略となっています。

一方、企業の内部インフラ、特に SaaS 環境と統合された ID システムを狙った攻撃も戦略的に進化しています。攻撃者は認証回避、トークンの窃取、MFA 回避技術を組み合わせて、Microsoft 365、Commvault、Ivanti などのクラウドベースのソリューション内部に侵入しました。その後、ラテラルムーブメント（側面移動）を通じて組織内部全体に拡散する方法が繰り返され、この過程でサプライチェーンや MSP を媒介に間接的に侵入する場合も観察されました。これは、従来の境界ベースのセキュリティモデルが SaaS 中心の構造に転換された環境では限界を露呈せざるを得ないという事実を再確認させます。ユーザー権限の最小化、統合認証構造の再設計、内部行動の検出強化など、全般的な ID ベースのセキュリティ再整備が切実に求められています。

総合的に見ると、6 月の脅威イベントは攻撃者が従来のセキュリティシステムを解体し、新しい経路を絶えず開拓していることを示しています。セキュリティ脆弱性への対応時間の短縮、人材資産の保護範囲の拡大、開発者エコシステムのセキュリティ強化、クラウドサービスベースの検出戦略への転換、SaaS ID システムの再構築がすべて並行して議論されるべき時期です。これらの脅威は互いに有機的に結びついており、断片的な防御措置では長期的な対応が不可能な構造的問題へと進化してい

ます。今必要なのは、攻撃者の視点から「全体構造を見た」防御戦略、そして技術ではなく意図と文脈を検知するセキュリティ思考の転換です。

Recommendation

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

1. 脆弱性保護 (Exploit Protection)

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

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

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

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

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

3. セキュリティ認識教育 (User Training)

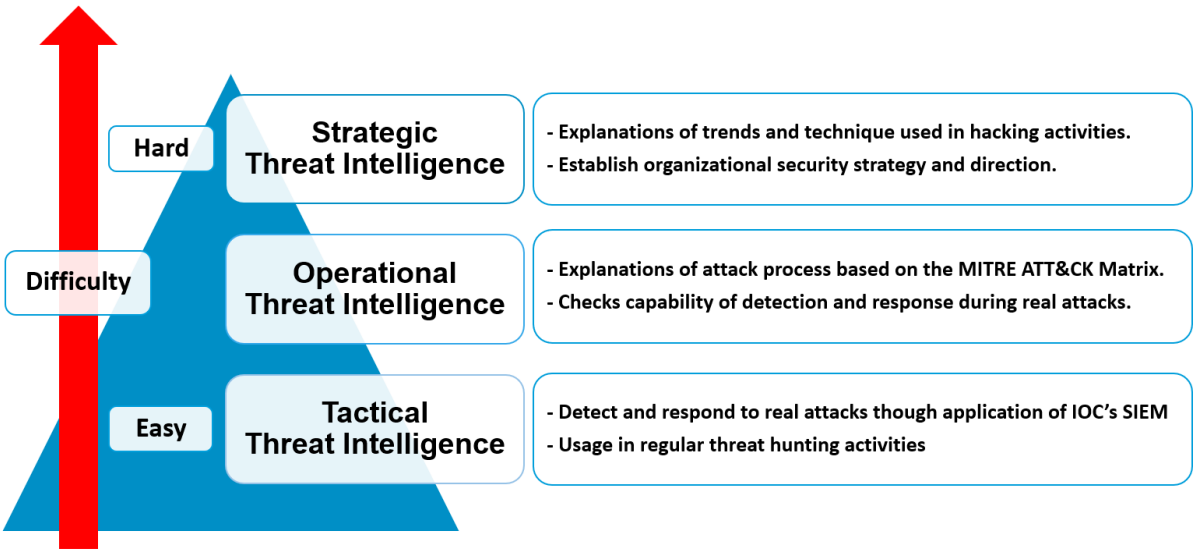
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

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

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

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

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



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

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

5. ネットワークにおける脅威緩和

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

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

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

2) ネットワーク細分化 (Network Segmentation)

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

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

6. ユーザーアカウントの脅威緩和

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

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

2) アカウント使用政策 (Account Use Policies)

アカウントのセキュリティ設定に関した政策設定の検討が必要

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

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

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

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

7. エンドポイントの脅威緩和

1) ソフトウェアアップデート(Update Software)

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

2) OSの構成 (Operating System Configuration)

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

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

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

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

4) 実行防止 (Execution Prevention)

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

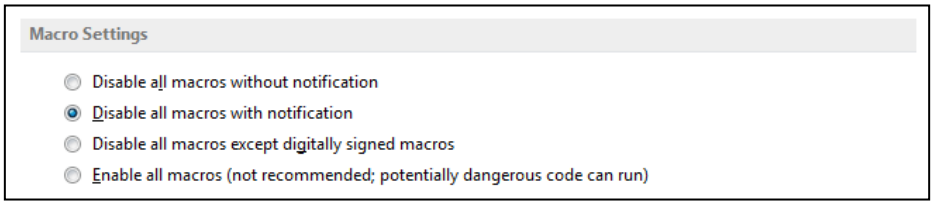
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

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

Program)

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

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



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

6) コード署名 (Code Signing)

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

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

7) アンチウイルス (Antivirus)

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

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

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

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

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

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

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

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

10) 企業モバイル政策 (Enterprise Policy)

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

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

LEGAL DISCLAIMER

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

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

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

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

NSHC.

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