NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI2025110602

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

Oct 2025

NSHC PTE. LTD.

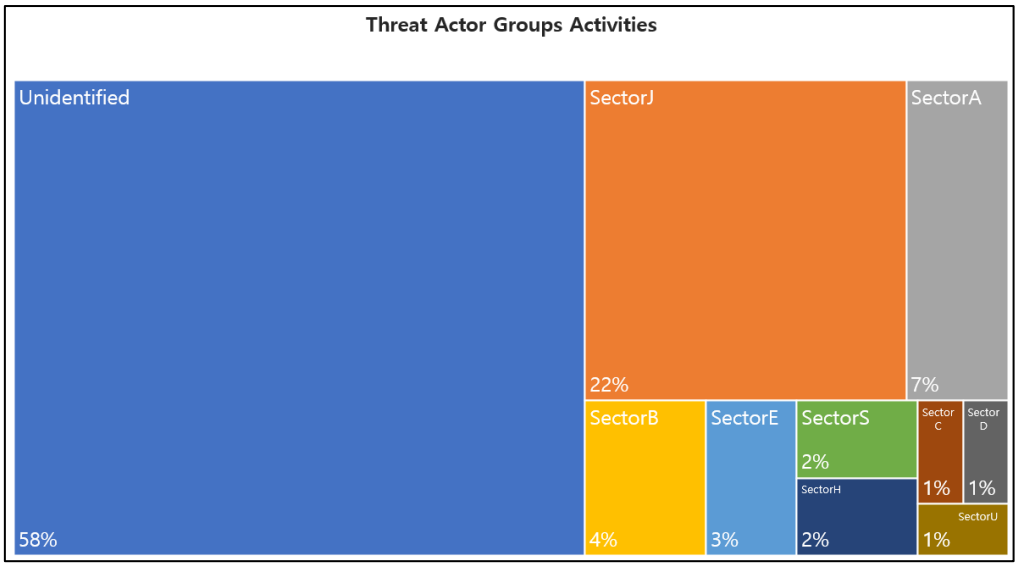
このレポートは 2025 年 9 月 21 日から 2025 年 10 月 20 日まで見つけた政府支援のハッキンググループ活動と関係あるイッシューを説明し、それに伴う侵害事故の情報と ThreatRecon Platform 内のイベント情報を含む。

Table of Contents

エグゼクティブサマリー

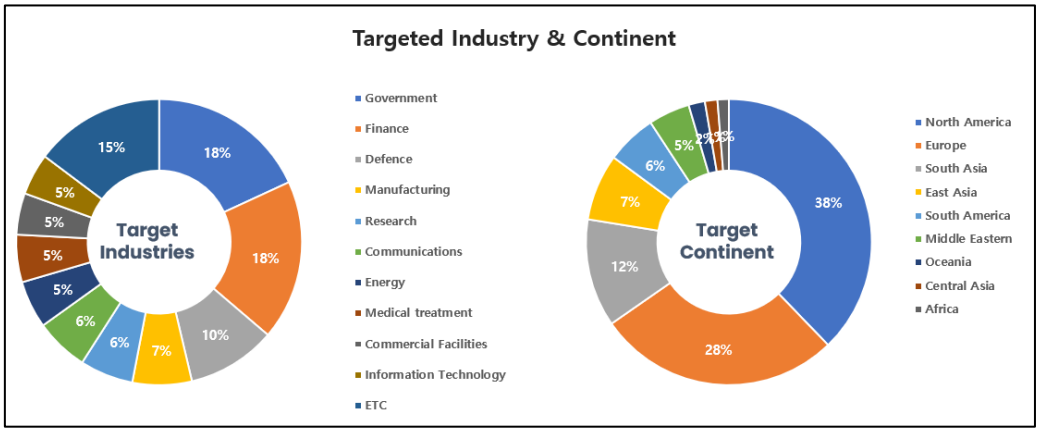
2025 年 9 月 21 日から 2025 年 10 月 20 日まで NSHC Threat Research Lab で収集したデータと情報に基づいて分析したハッキンググループ(Threat Actor Group)の活動を要約整理した内容である。

今回 10 月には、合計 83 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 58%で最も多く、SectorJ、SectorA グループの活動がそれに続いた。



[図 1: 2025 年 10 月に確認されたハッキンググループ別活動統計]

今回 10 月に発見されたハッキンググループのハッキング活動は、政府機関および金融業分野に従事する関係者またはシステムを対象に最も多くの攻撃を実行しており、地域別では北アメリカ(North America)とヨーロッパ(Europe)に位置する国家を対象としたハッキング活動が最も多いことが確認される。



[図 2: 2025 年 10 月攻撃対象となった産業分野と国家統計]

SectorA グループのサイバー攻撃活動を分析してみると、彼らは主に精巧な社会工学技法と高度な技術を活用して、複数のオペレーティングシステムを対象とした多段階攻撃を展開する。このグループは Windows、macOS、Linux システムをすべて標的にしており、主にソフトウェア開発者のような技術専門家を狙う。攻撃は主に偽のソフトウェアアップデートや就職提案を通じて行われ、これを通じて被害者のデバイスにアクセスした後、様々な Malware を配布してシステムを持続的に感染させる。特に彼らは Node.js ベースの Malware を活用してシステム情報を収集し、クレデンシャル窃取、データ流出、そして暗号通貨や Web3 プロジェクトを狙った金融犯罪を行う。このグループは BeaverTail、OtterCookie、そして新しい OtterCandy のような Malware を活用し、これらのコードは情報窃取およびリモートコマンド実行を可能にする機能を果たす。攻撃者はまた、高度な難読化技術と多段階 C2 インフラを構築して Malware 検出を回避し、持続的なシステム掌握を保証する。特に GitHub のような合法的なプラットフォームを利用して悪性ペイロードを配布し、スケジューラーを活用した持続性確保と PowerShell を通じたコマンド実行などで攻撃をさらに隠密に進行する。彼らは精巧な身元盗用戦術を使用してソーシャルメディアプラットフォームで偽のプロフィールを運営し、これを通じてフィッシング攻撃や就職詐欺などを行う。これを通じて確保した情報は金融犯罪およびデータ流出に使用され、これらの複合的な攻撃戦略はサイバー犯罪とスパイ活動が結合した形態を示す。したがって彼らの活動は持続的な監視と対応が必要である。

SectorB グループのハッキング活動は、複数の地域で多様な産業を対象とした複雑で精巧なサイバー攻撃を特徴とする。このグループは主にサイバースパイ活動を通じて情報収集とデータ窃取に集中し、主に合法的なツールとクラウドサービスを活用して検出を回避し、持続性を維持する戦略を使用する。例えば、ロシアの IT サービスプロバイダーに長期間アクセスし、ソフトウェアビルドシステムを潜在的に悪用し、Yandex クラウドを通じてデータを窃取する方法は、彼らがどのように合法的なチャネルを悪用するかを示している。また、様々な Malware と技術を継続的に開発し、新しいバックドアを配布し、Microsoft Graph API のような現代的な技術を活用してコマンド＆コントロールを実行し、DLL サイドローディング、SMBExec、スケジュールされたタスクを利用した側面移動と持続性を維持する。これらの技術は特に台湾のソフトウェア会社ネットワーク侵害事件で顕著であり、ShadowPad と BYOVD 技法を活用して防御システムを無力化するなど、精巧な攻撃技法を頻繁に使用する。さらに、このグループは Pantegana と Cobalt Strike のようなツールを活用して政府、防衛および民間部門の高位組織を対象とした世界的なサイバースパイ攻撃を実行し、SonicWall、F5 BIG-IP、Fortinet FortiGate のようなデバイスの脆弱性を利用した初期アクセスを通じて多様な組織を狙う。彼らの攻撃はしばしば地理的および政治的事件と連動して発生し、特に VPN およびその他のセキュリティ製品の既知の脆弱性を悪用して大規模攻撃を実行し、オープンソースツールを使用して攻撃経路とインフラの出所を隠す。また、このグループは偽の人物を装ったスピアフィッシングキャンペーンを通じて北米、アジア、ヨーロッパの複数の機関を攻撃し、様々なペルソナと言語を使用してフィッシングメールを作成し、信頼関係構築フィッシング戦略を通じて悪性ペイロードを配信する。この過程で LLM を活用してフィッシングメールと Malware を開発したと分析される。一方、こ

のグループは複雑なランサムウェア攻撃を通じて VMware ESXi 仮想マシンと Windows サーバーをターゲットにし、様々なランサムウェア変種を配布し、「Velociraptor」のようなオープンソースツールを活用して持続的なアクセスを維持し、PowerShell スクリプトを使用してデータを窃取し暗号化する。最後に、このグループは PlugX 変種を活用して中央および南アジアの通信および製造産業群を攻撃し、DLL 検索順序ハイジャックのような精巧な技術を使用して検出を回避し Malware を実行する。これらの事件は、SectorB グループが継続的に攻撃技法と Malware を発展させ、合法的なシステムとツールを悪用して検出を回避するサイバースパイ活動を続けていることを示している。SectorC グループのハッキング活動の様相は、2 つの主要な攻撃キャンペーンを通じて明らかになる。最初のキャンペーンでは、ClickFix という多段階攻撃チェーンを利用してロシアの市民社会関連の個人および組織を対象とする。攻撃は、被害者が市民活動家のためのリソースを装った損傷したウェブページを訪問することで始まり、このページは訪問者に Cloudflare Turnstile チェックボックスを装った悪性コマンドを実行するよう誘導する。実行されたコマンドは「machinerie.dll」という悪性 DLL をダウンロードし、Windows の「rundll32.exe」ユーティリティを使用して実行する。BAITSWITCH として知られるこの DLL は持続性を確保した後、制御されたドメインから SIMPLEFIX という PowerShell ベースのバックドアをダウンロードする。検出を避けるために難読化とレジストリに保存されたペイロードを使用し、特定のユーザーエージェント文字列でエンコードされたコマンドおよびコントロール（C2）チャネルを通じて独占的な通信を保証する。SIMPLEFIX は情報収集、追加スクリプトの実行、C2 サーバーとの通信など複数のタスクを実行する。このキャンペーンは、クリップボード操作、プロセス持続性、洗練されたデータ窃取技術などの高度な方法を明らかにする。2 番目のキャンペーンは、2025 年 9 月後半にウクライナの複数の地域にある防衛軍と地方政府機関を対象とした一連の標的サイバー攻撃として現れ、ロシアのサボタージュおよび偵察グループに対抗する内容のコミュニケーションを装って進行する。主要な配信方法は、Ukr.net および Gmail のようなサービスを通じて送信されたメールで、VHD ファイルをダウンロードできるリンクを含むか、直接これらのファイルを添付する。このファイルは主に PDF 形式の文書と実行ファイルを含み、攻撃者は GitHub で利用可能な多機能ツール OrcaC2 と Go でコーディングされたファイルスティーラーFILEMESS を利用する。FILEMESS は再帰ファイル検索を実行し、Telegram API を通じてファイルを窃取し、レジストリエントリを生成して持続性を確保し、認証トークンを暗号化して複数のインスタンスを防ぐ。OrcaC2 はコマンド実行、ファイル転送、トラフィックトンネリングなどの機能を提供する。 SectorC グループの攻撃者は、洗練された多段階攻撃手法と多様なマルウェアを活用して標的を達成しており、持続性と検出回避戦略を通じて長期的な浸透を図っている。SectorD ユ畠のハッキング活動は高度に組織化されたサイバースパイ作戦として際立っており、主要攻撃対象は中東の政府、法律、学界、航空およびエネルギー分野とアメリカ、アジアの金融分野に及びます。これらの攻撃は CVE-2024-1709 脆弱性とルーターの DNS 操作を利用したカスタムリモートアクセスツールで構成されており、EDR システムを回避するための回避技術と社会工学を通じたインフラ損傷およびデータ窃取に重点を置いています。このグループはプロセスインジェクション、EDR 回避、サプライチェーンピボット、複雑なフィッシングインフラを活用して高い技術力を示

しており、これはサプライチェーンと国家安全保障に重要な脅威を提起します。最近のサイバーキャンペーンでは生成型 AI ツールを使用してアメリカの非営利研究機関の文書を装った悪性 PDF 文書を作成し、これは'PowerLess'というマルウェアと共に配布されました。これらの PDF は DLL ファイルである'sin.dll', 'sst.dll', 'ssts.dll'と結合され、追加の悪性行為を促進しました。AI 生成コンテンツを活用した精巧なスピアフィッシング餌の作成は、AI が攻撃戦術、技術、手順を強化するために使用される進化する脅威環境を強調します。別のキャンペーンでは少なくとも 2025 年 7 月から複数のドメインを対象としたフィッシング攻撃が識別され、'online' TLD を使用して Google Meet のような合法的なビデオ会議サービスを装ったフィッシング攻撃を実行しました。このキャンペーンは'viliam'で始まるサブドメインパターンを使用して悪性コンテンツを配布し、イスラエルのユーザーを狙った可能性があります。キャンペーンの継続的な活動はビデオ会議サービスが標的となるサイバースパイ活動の継続的な脅威を強調します。また、ヨーロッパの航空宇宙、防衛、通信分野を対象とする精巧なサイバー脅威キャンペーンが識別され、HR 採用担当者を装ったスピアフィッシング戦術を使用して偽の求職プラットフォームを構築しました。この攻撃は以前に文書化されていない API を悪用して合法的なプロセスに悪性 DLL を挿入する複雑な多段階 DLL サイドローディング技術を使用し、MiniJunk バックドアと MiniBrowse スティーラーを含むツールセットはコンパイラレベルの技術で強力に難読化されています。これらは有効なデジタル証明書とサイズ拡張技術を活用してセキュリティシステムを回避し、複数の冗長サーバーとエンコードされた通信プロトコルを通じてコマンド＆コントロールを実行します。これらの活動は戦略的情報目標と一致し、ヨーロッパの対象まで焦点を拡大しています。SectorD 그룹의 攻撃戦術とマルウェア使用は高度な技術と組織力に基づく継続的な脅威を示しています。

SectorE グループのハッキング活動は一貫したスパイ活動を中心に展開され、主に外注人材を活用して低コストの基礎的な技術方法を使用しますが、国家の戦略的目標を狙っているという特徴があります。彼らはフィッシングフレームワークを利用した攻撃を実行し、核心的には"DeliveryBoy"というドロッパーを使用して持続性のための"MadBoy"のようなローダーを配布し、"Win"という CMD コマンド実行インプラントを活用します。特にローダーは動的ペイロードローディングおよびプロセスインジェクションのような高度な技術を活用します。GitHub の偽プロジェクトを通じて配布されるマルウェアマクロは.xlsm ファイルなどで資格情報を収集し、コマンド-コントロールサーバーと接続して持続性を維持します。彼らはクラウドストレージをペイロード配信に使用し、匿名性のために Tor ノードを使用します。Windows プラットフォームを主に標的とし、政府、軍事、防衛および重要な産業分野、特に南アジア地域を狙います。フィッシングメールとマルウェア文書を初期アクセスベクターとして使用し、最近では WooperStealer で Python ベースのバックドアと AnonDoor に進化したツールを使用することで技術的適応力を示しています。攻撃は OLE オブジェクトトリガー感染を通じて開始され、リモート URL に接続してさまざまなマルウェアコンポーネントをダウンロードします。これらのコンポーネントには、システムプロファイリングおよび情報窃取のための構造化されたコマンドを使用してさまざまなファイルタイプをリモートサーバーに送信できる WooperStealer が含まれます。マルウェアは DLL サイドローディングおよび Python ベースのバッ

クドアを使用して長期的なアクセスを目指し、持続性のために DLL サイドローディングおよびスケジュールされたタスクを利用し、エンコードされたコンポーネントを活用して可視性を減らします。"Operation SouthNet"というキャンペーンでは無料ホスティングプラットフォームを利用して資格情報収集ポータルと海洋および政府テーマを扱った文書を配布します。50 以上のマルウェアドメインが確認されており、これらのドメインは現地ドメインに合わせた Outlook および Zimbra ウェブメールポータルなどに偽装します。攻撃者はレガシーC2 資産を再利用し、インフラストラクチャの重複を活用して持続的で適応力のある技術を示しています。南アジア諸国を対象としたこのキャンペーンは、重要な国家部門を侵入しようとする意図を強調し、迅速なドメイン切り替えと洗練された社会工学技法を活用してスパイ活動の目標を維持します。最近のキャンペーンはスピアフィッシングとカスタマイズされたメールを使用して標的を侵入し、BabShell および MemLoader のようなカスタムおよびオープンソースツールを活用して高度な PowerShell スクリプトおよびリバースシェル機能を使用した持続性とコマンド実行を行います。彼らは WhatsApp を通信チャネルとして活用し、ChromeStealer Exfiltrator など特定のモジュールを活用してファイルとブラウザストレージの機密データを収集および流出させます。グループのインフラはワイルドカード DNS、VPS およびクラウドサービスを使用して運用弾力性を維持します。これらのキャンペーンはグループの技術的精巧さと地域サイバーセキュリティに対する持続的な脅威レベルを強調します。

SectorH グループのハッキング活動は主に Windows と Linux システムを対象とした精巧なサイバー脅威キャンペーンとして現れる。このグループは各プラットフォームにカスタマイズされた戦術を使用してデータを奪取し、システムに持続的にアクセスすることに重点を置いている。Windows 環境では.ppam ファイルフォーマットを利用してマルウェアマクロを仕込み、多段階攻撃チェーンを実行し、最終的にデータ流出を目標とする。この過程で使用された.ppam ファイルは"Jammu Kashmir Police Letter"のような名前で偽装され、ユーザーを欺く戦略が使用された。マクロスクリプトは静的検出を避けるために暗号化された ZIP ファイルをダウンロードし、ハードコーディングされたパスワードでこれを解読してリモート制御実行ファイルを配布する。一方、Linux では.desktop ファイルを使用して PDF に偽装し、ユーザーが実行するよう誘導し、ELF 実行ファイルをダウンロードする方式で攻撃を進行する。ここで使用された ELF ペイロードは Golang で開発された新しい RAT で、“systemd"設定を通じて持続性を確保し、リモートコマンド実行およびデータ奪取を行うことができるよう設計されている。両プラットフォームとも共通ドメインを通じてペイロードを配布し、これはクロスプラットフォーム戦略を使用していることを示唆する。StealthServer と呼ばれるマルウェアはフィッシングメールを通じて配布され、政治および軍事会議に関連するテーマを活用してユーザーを欺く。このマルウェアは Windows では PPT ファイルのマルウェアマクロを、Linux では PDF に偽装された.desktop ショートカットを使用して実行時に正当な文書を開きつつ同時にマルウェアを配布する。StealthServer は Go で開発されており、クロスプラットフォーム機能をサポートし、ファイル流出とリモートコマンド実行を C2 サーバーを通じて行う。このマルウェアは精巧なリバースエンジニアリング防止技術を使用して分析を困難にし、Windows 変種は TCP または WebSocket を、Linux 変種は HTTP または WebSocket を利用した通信を行う。C2 サーバー

との通信は公式政府ドメインに似たドメイン名を使用し、ペイロード難読化が観察され、分析をさらに複雑にする。システムに持続性を確保するためにシステムサービス登録、開始スクリプト修正、予約タスク生成などの技術を活用し、C2 サーバーとのデータ交換には JSON 形式を使用する。特に、ファイル流出は AES 暗号化を通じてセキュリティ回避を試みる。全体として、このキャンペーンは Windows と Linux 環境の両方で隠密に活動し、持続的にシステムを制御しようとする高度な脅威戦術を示している。

SectorT グループのハッキング活動は非常に精巧で戦略的に進行される。2025 年初めに発生した事件では、攻撃者がリビア海軍の儀典室を装い、ブラジル軍を狙った攻撃を実行した。この攻撃は Zimbra Collaboration Suite のゼロデイ脆弱性(CVE-2025-27915)を利用して行われ、特に Zimbra と類似したオープンソースのコラボレーションツールで発見される脆弱性を狙ったものであった。使用された方法は、メールを通じた悪性.ICS ファイルを活用したもので、これは一般的でない攻撃方式として確認される。該当スクリプトは広範なデータ窃取を目的とする情報収集型 Malware で、Zimbra ウェブメールから資格情報、メール、連絡先、共有フォルダなどを含む多様なデータをコマンド＆コントロールサーバー(ffrk[.]net/apache2_config_default_51_2_1)に流出させた。Malware は検出を避けるためにいくつかの回避技法を使用し、特定時間後に実行されるよう遅延を設け、実行頻度を 3 日に一度に制限し、ユーザーインターフェース要素を隠すなどの技法を使用した。また、ユーザー活動をモニタリングし、非アクティブ状態が検出されるとデータを窃取する方法を選択した。資格情報およびメール窃取は非同期 JavaScript 関数を利用して実装され、メールを ProtonMail アカウントにリダイレクトするための悪意のあるメールフィルタルールを追加した。これらの TTPs は、攻撃者が高いレベルの技術的専門性を有し、目標を長期的に観察し、精巧な技法でデータを窃取するための計画を立てて実行していることを示唆する。SectorT グループは目標対象の機密情報を持続的かつ隠密に収集することに大きな重点を置いているように見える。

SectorJ グループのハッキング活動を分析すると、彼らは主にゼロデイ脆弱性と社会工学技法を活用して多様な産業群を狙った攻撃を行っていることが確認できる。彼らは Oracle E-Business Suite の CVE-2025-61882 脆弱性を悪用して認証を回避し、リモートコード実行を通じてデータを奪取しようと試み、Web シェルの配布を通じて持続的なアクセスを維持する。このような攻撃は Telegram を通じた PoC 共有により、多数の脅威グループが参加した可能性を示唆する。また、過去には悪性 JavaScript ファイルを税金フォームに偽装して“Brute Ratel”ペイロードを実行し、様々な Malware を配布してデータを奪取した。この過程でコマンド＆コントロール技術としてプロセスインジェクション、予約タスク、レジストリ実行キーを活用し、BackConnect VNC を通じて断続的に通信を維持した。最近ではゲームパッチに Malware を注入してユーザーデータを奪取するなど、ユーザーを狙った攻撃も行った。特に、SVG ファイルを通じたフィッシングキャンペーンではリバースシェルをダウンロードして持続的なアクセスを確保し、被害者システムのデータを収集する方法を使用した。金融的動機を持つグループは AI を活用した音声フィッシングとサプライチェーンシステムを悪用して高位エンジニアアカウントにアクセスし、企業ネットワークに侵入して Salesforce アプリケーションから顧客データを奪取して金銭的利益を得ようとした。彼らはまた、政府機関を装ったメールキ

ャンペーンを通じて金融情報を奪取し、信頼性を利用した社会工学技法を活用した。IIS サーバーを狙った SEO 詐欺および資格情報奪取攻撃では Web シェルをアップロードして持続的なアクセスを維持し、RDP および VPN を活用した精巧な防御メカニズムを構築した。彼らは MonsterV2 Malware のような様々な Malware を配布してリモートアクセスおよびデータ奪取を行い、Web インジェクションキャンペーンを通じてユーザーに悪性 PowerShell コマンドを実行させた。AWS クラウド環境を狙った攻撃では TruffleHog ツールを使用して漏洩した資格情報を検索し、API 呼び出しを通じて新しいユーザー生成および権限昇格を通じてデータ収集および奪取を試みた。全般的に SectorJ グループの活動はゼロデイ脆弱性悪用、社会工学技法、Malware 配布およびデータ奪取を中心にし、様々な技法とツールを活用して持続的なアクセスを維持し、被害を最大化しようとする様相を見せる。

詳細情報

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

1) SectorA01 used Social Engineering for Trojanized Code Delivery (2025-09-25)

https://cti.nshc.net/events/view/18902

攻撃対象産業群: IT

攻撃者は 2023 年から活動を開始しており、特定の国の IT 労働者キャンペーンと緊密な連携を示している。このグループは Windows、Linux、macOS システム全般のソフトウェア開発者を対象としており、暗号通貨および Web3 プロジェクトを通じて財政的利益を追求している。初期アクセス戦略は社会工学技法に大きく依存しており、LinkedIn や Upwork のようなプラットフォームで偽の採用担当者プロフィールを活用し、段階的なインタビューを通じてトロイの木馬化されたコードベースを配布する。このような技法は被害者が非公開リポジトリからプロジェクトをダウンロードするように仕向け、これらのプロジェクトには主に BeaverTail と OtterCookie 情報窃取型 Malware が隠されている。初期アクセスが行われると、BeaverTail は情報窃取型 Malware およびダウンローダーとして機能し、InvisibleFerret および TsunamiKit という新しいコンポーネントの感染につながる。TsunamiKit はデータおよび暗号通貨窃取のための精巧なツールで、TsunamiInjector と TsunamiClient のようなコンポーネントを含んでいる。このグループはまた Tropidoor Malware を使用する。さらに攻撃者は偽の身元およびソーシャルエンジニアリング技法を駆使して内部アクセス権を確保し、これを通じてデータ漏洩と金銭窃取を実行する。このようなハイブリッド方式はサイバー犯罪と諜報技術の融合を示している。

[Attack Flow]

1. [Reconnaissance] Gather Victim Identity Information (T1589)
   a. 被害者の資格情報を収集する
   b. 社会工学に活用する
2. [Resource Development] Establish Accounts: Social Media Accounts (T1585.001)
   a. 偽の採用担当者アカウントを生成する
   b. ソーシャルメディアプラットフォームを活用する
3. [Resource Development] Compromise Accounts (T1586)
   a. アカウントの奪取（乗っ取り）
   b. マルウェアを配布する
4. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. マルウェアを含むプロジェクトを含むメールを送信する
   b. 添付ファイルのダウンロードを誘導する
5. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. ClickFix 技法を活用する
   b. 偽の問題解決リンクを提供する
6. [Execution] User Execution: Malicious Link (T1204.001)
   a. 偽のインタビューサイトでマルウェアをダウンロードさせる
   b. ClickFix 技法で実行を誘導する
7. [Execution] User Execution: Malicious File (T1204.002)
   a. トロイの木馬化したファイルを実行する
   b. BeaverTail 亜種を含む
8. [Execution] Command and Scripting Interpreter (T1059)
   a. VBS、Python、JavaScript を使用する
   b. シェルコマンドを実行する
9. [Defense Evasion] Valid Accounts (T1078)
   a. 盗用された資格情報を使用する
   b. 偽アカウントを維持する
10. [Defense Evasion] Obfuscated Files or Information (T1027)
    a. 難読化された悪性スクリプト
11. [Defense Evasion] Masquerading (T1036)
    a. 正常なソフトウェアに偽装する
    b. NVIDIA インストーラ等に偽装する
12. [Defense Evasion] Virtualization/Sandbox Evasion (T1497)
    a. 環境検査を実行する
    b. 分析回避手法を活用する

13. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
    a. HTTP/S を通じたコマンドおよび制御通信
    b. AkdoorTea、BeaverTail、Tropidoor を使用する
14. [Command and Control] Ingress Tool Transfer (T1105)
    a. BeaverTail を通じた追加ペイロードのダウンロード
    b. InvisibleFerret、TsunamiKit、Tropidoor を配布する

2) SectorA01 used Typosquatted npm Packages to Deploy BeaverTail Malware (2025-10-10)

https://cti.nshc.net/events/view/19285

攻撃対象産業群: IT

「Contagious Interview」キャンペーンは、Web3、暗号通貨、ブロックチェーン開発者および求職者を標的に、npm レジストリを介して攻撃を実行したものである。2025 年 7 月以降、338 個以上の悪性パッケージが 50,000 回以上ダウンロードされ、そのうち 25 個は依然として活動中である。北朝鮮と関連が疑われる脅威行為者は 180 個以上の偽のペルソナと複数の C2 エンドポイントを用いて攻撃を遂行した。作戦はタイポスクワッティングと難読化された JavaScript パッケージを含み、BeaverTail ペイロードや InvisibleFerret バックドアのような二段階のマルウェアを継続的に取得する手法を採用している。本キャンペーンは LinkedIn 上で採用担当者を装い、偽の採用課題を用いて開発者を誘引するソーシャルエンジニアリングを核心としている。日常的な npm 作業中に悪性パッケージをインストールすると、多段階の侵害に繋がり、最終的に金銭的損失を招くおそれがある。脅威の主要目的は開発者エンドポイントへのアクセス確保および暗号通貨の窃取であり、別名アカウント、ローダー変種、VPS の IP アドレスおよび合法的なホスティングサービスを悪用した C2 技術を通じて持続的に運用されている。

[Attack Flow]

1. [Reconnaissance] Gather Victim Identity Information (T1589)
    a. ソーシャルメディアで Web/ブロックチェーン開発者プロファイル収集
    b. メール、Github、Telegram など連絡先情報収集
2. [Resource Development] Acquire Infrastructure: Domains (T1583.001)
    a. タイポスクワッティングドメイン登録
    b. 合法的ホスティングサービス基盤 C2 インフラ構築
3. [Resource Development] Stage Capabilities (T1608.002)

a. 悪性 npm パッケージ制作およびアップロード
    b. BeaverTail ローダーおよび InvisibleFerret バックドア準備
4. [Initial Access] Phishing: Spearphishing Link (T1566.002)

a. LinkedIn で採用担当者を装い、偽の採用課題を提供
b. 悪性 npm パッケージインストール誘導
5. [Execution] User Execution: Malicious File (T1204.002)
a. 開発者が悪性パッケージをダウンロードおよび実行
6. [Execution] Command and Scripting Interpreter (T1059.007)
a. Node.js 環境で難読化された JavaScript 実行
7. [Defense Evasion] Obfuscated Files or Information (T1027.013)
a. 難読化されたファイル使用
b. 暗号化されたファイル保存および復号化
8. [Persistence] Event Triggered Execution (T1546.016)
a. インストールパッケージで実行
b. 持続的実行環境構築
9. [Credential Access] Credentials from Password Stores (T1555.003)
a. ウェブブラウザから資格情報抽出
b. キーチェーンから資格情報抽出
10. [Discovery] System Information Discovery (T1082)
a. システム情報探索
b. ファイルおよびディレクトリ発見
11. [Exfiltration] Exfiltration Over C2 Channel (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送信
12. [Command and Control] Ingress Tool Transfer (T1105)
a. C2 コマンド送信
b. Malware ダウンロードおよび実行
13. [Impact] Financial Theft (T1657)
a. 暗号通貨窃取

3) SectorA01 used Malware disguised as Nvidia and macOS patches (2025-10-13)

https://cti.nshc.net/events/view/19334

攻撃対象産業群: IT、政府・行政、国防

攻撃者は 2025 年 9 月、Windows および macOS システムを標的とした精巧なサイバーキャンペーンを実行しました。攻撃者は合法的なソフトウェアアップデートに偽装し、偽の Nvidia アップデート、macOS カメラドライバーおよびその他のソフトウェアパッチを圧縮ファイルとシェルスクリプトを通じて配布しました。実行時に、これらのダウンロードは node.js のインストールを開始し、main.js を実行し、これは追加の動作のためにコマンド＆コントロール（C2）サーバーと通信しま

した。このキャンペーンはリモートコマンド実行とデータ窃取を含んでいました。macOS では、さまざまな偽装の下でシェルスクリプトがさらに暗号化されたリソースをダウンロードし、システムデータとブラウザ資格情報を収集する Python ペイロードを実行して C2 サーバーに送信しました。Windows 攻撃は類似のベクターを使用し、システム再起動時に Malware 実行を保証するためにレジストリ持続性を追加しました。また、両システムともオペレーティングシステムの詳細、地理的位置、ブラウザ資格情報およびクレジットカードデータを収集する Malware によって悪用されました。暗号化されたペイロードは、文字列反転、Base64 デコードおよび zlib 解凍を含む多段階の暗号解除ルーチンを経ました。高度な難読化技術と Windows 11 以上で実行される特定の条件は、攻撃の複雑さを示しました。さまざまなドメイン名と IP アドレスを持つサーバーとの通信が設定され、追加のコマンドを伝達し実行して持続的なシステム損傷を保証する多段階 C2 インフラとして機能しました。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 偽のソフトウェアアップデートに偽装
   b. Nvidia アップデートおよび macOS カメラドライバ配布
2. [Execution] Command and Scripting Interpreter (T1059)
   a. node.js インストールおよび main.js 実行
   b. シェルスクリプトおよびバッチファイル使用
3. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. Windows レジストリ持続性追加
   b. システム再起動時に Malware 実行
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. 文字列反転、Base64 デコード、zlib 解凍
   b. 高度な難読化技法使用
5. [Credential Access] Credentials from Web Browsers (T1555)
   a. ブラウザ資格情報収集
   b. クレジットカードデータ収集
6. [Discovery] System Information Discovery (T1082)
   a. オペレーティングシステム詳細情報収集
   b. 地理的位置情報収集
7. [Collection] Data from Local System (T1005)
   a. システムデータ収集
8. [Command and Control] Non-Standard Port (T1571)
   a. 多段階 C2 インフラ使用
   b. サーバーとの持続的通信設定

9. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. 収集されたデータを C2 サーバーへ送信
    b. リモートコマンド実行および追加コマンド受信

4) SectorA01 used OtterCandy Malware disguised as Job Interviews (2025-10-15)
https://cti.nshc.net/events/view/19501

攻撃キャンペーンは OtterCandy という Malware を使用して多重オペレーティングシステムである Windows、macOS、Linux を対象とする。このキャンペーンは ClickFake Interview という大規模作戦に関与している。GolangGhost と FrostyFerret のようなツールを使用して資格情報および資産の窃取を目指す持続的なキャンペーンを含む。OtterCandy は Node.js で実装され、RAT とデータ窃取機能を実行し、Socket.IO を活用して C2 サーバーと接続し、コマンドを実行する。この Malware はブラウザ資格情報、暗号通貨ウォレット、機密ファイルを窃取することができる。“process.on”を使用して自己複製を通じて持続性を維持し、2025 年 8 月にユーザー識別を強化する“client_id”の追加、窃取データ範囲を追加のブラウザ拡張プログラムで拡張、削除過程中のアーティファクト除去機能の実装という主要なアップデートが観察された。これらの詳細は進化する脅威に対する持続的な注意とモニタリングが必要であることを示唆している。

[Attack Flow]
1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
    a. ClickFix のウェブページへ誘導する
    b. ユーザークリック誘導
2. [Execution] Command and Scripting Interpreter: Node.js (T1059.007)
    a. Node.js 로 Malware 実行
    b. OtterCandy の命令受信および実行
3. [Persistence] Boot or Logon Autostart Execution (T1547.001)
    a. SIGINT イベント受信時フォーク
    b. DiggingBeaver による持続性確保
4. [Credential Access] Credentials from Web Browsers (T1555.003)
    a. ブラウザ資格情報脱取
    b. 暗号通貨ウォレット脱取
5. [Collection] Data from Information Repositories (T1213)
    a. 敏感なファイル収集
    b. ブラウザ拡張プログラムデータ収集
6. [Command and Control] Encrypted Channel (T1573)
    a. Socket.IO を通じた C2 サーバーとの暗号化通信

b. C2 命令受信および応答

7. [Defense Evasion] Indicator Removal on Host (T1070)
   a. レジストリキー削除
   b. ファイルおよびディレクトリ削除

5) SectorA01 used Node.js Malware disguised as Chessfi Application (2025-10-16)

https://cti.nshc.net/events/view/19414

攻撃者は採用機関を装い、求職者を対象とした精巧なキャンペーンを実行しました。攻撃の流れは、悪性 NPM パッケージ "node-nvm-ssh" を通じて配布されたトロイの木馬化されたアプリケーション "Chessfi" のインストールから始まりました。この事件は偽の採用プロセスを通じて開始され、社会工学的手法を活用して被害者を欺く方法で進行しました。攻撃者は BeaverTail と OtterCookie として知られるツールを使用し、これらのツールは時間が経つにつれて機能が統合され始め、キーロギングおよびスクリーンショット機能を含むようになりました。主要なデータとスクリーンショットはコマンドおよびコントロールサーバーにアップロードされました。追加の技術分析を通じて、OtterCookie を配信する可能性のある VS Code 拡張が発見され、これは配信方法に関する実験が行われたことを示しています。追加の OtterCookie モジュールには、システムデータ収集およびコマンド実行のためのリモートシェルモジュール、特定のファイルタイプをターゲットとするファイルアップロードモジュール、そして暗号通貨拡張盗難プログラムが含まれています。これらのツールの最新バージョンは、データ窃取および難読化を通じた回避技術に重点を置いています。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. 偽の求人提案メールを送信する
   b. 社会工学技法で被害者誘引
2. [Execution] User Execution (T1204)
   a. 被害者が NPM パッケージインストール
   b. "Chessfi"アプリケーション実行
3. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. Node.js アプリケーションの持続的実行
   b. Malware 自動実行設定
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. コード難読化活用
   b. 探知回避技法適用
5. [Credential Access] Input Capture (T1056)
   a. キーロギング機能活性化

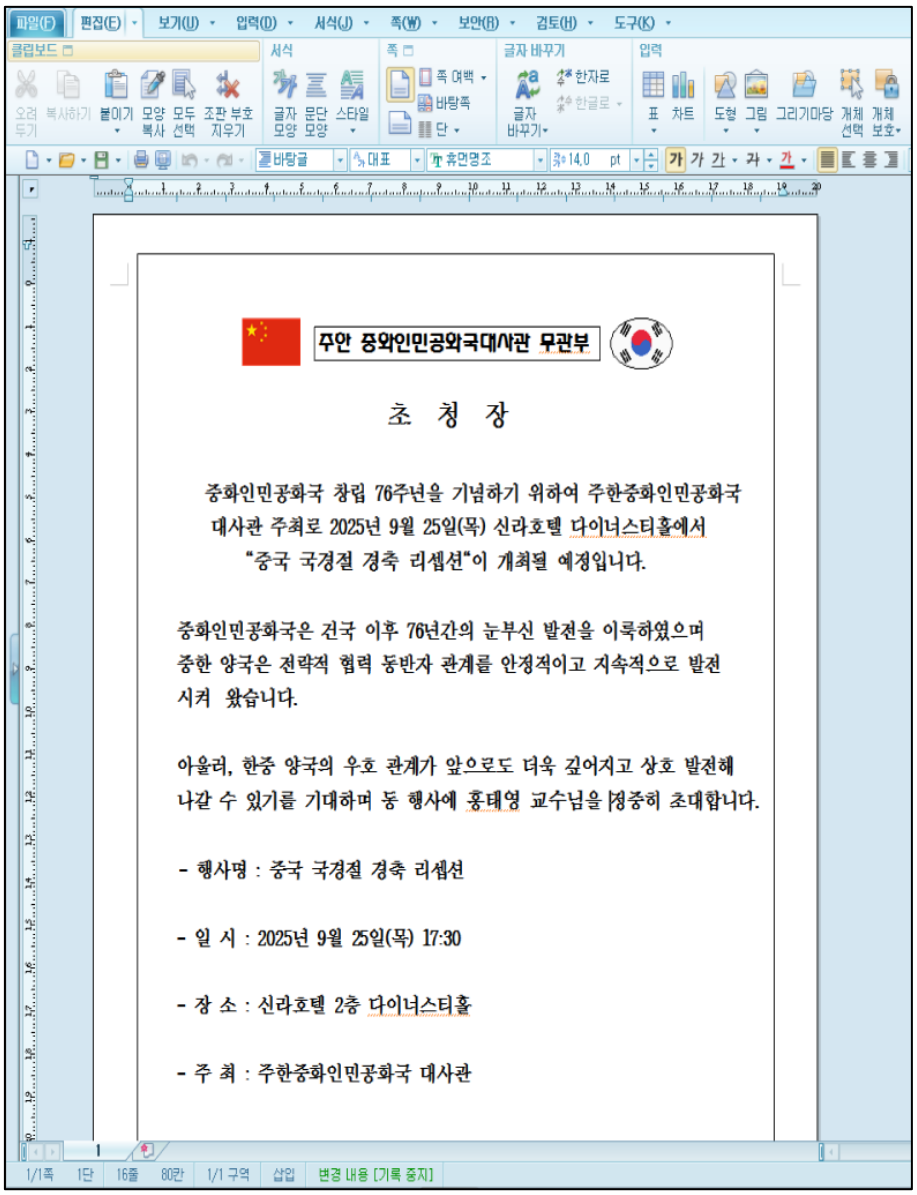
b. スクリーンショット定期的キャプチャ

6. [Collection] Data from Local System (T1005)
   a. システムからファイル収集
   b. 特定ファイルタイプターゲット
7. [Command and Control] Ingress Tool Transfer (T1105)
   a. BeaverTail および OtterCookie ツール伝達
   b. C2 サーバーとの通信設定
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. コマンドおよびコントロールサーバーへのデータ転送
   b. 収集されたキーロギングおよびスクリーンショットデータのアップロード

6) SectorA05 used LNK Malware disguised as Chinese Embassy Invite (2025-09-24)

https://cti.nshc.net/events/view/18869

攻撃者は国防大学校の安保政策学部の教授を対象に、駐韓中華人民共和国大使館の武官部を装った66,125 バイトの LNK ファイルを通じて Malware を配布しました。該当 LNK は攻撃対象に表示されないように PowerShell をバックグラウンドモードで実行し、Base64 エンコードで難読化されたスクリプトをロードします。該当スクリプトは現在のディレクトリと%TEMP%で LNK ファイルを検索し、ペイロードを抽出して.hwp ファイルを生成した後、元のファイルを削除します。Base64 でエンコードされた内容は追加スクリプトを生成・実行し、抽出された.hwp は%TEMP%にコピーされ、圧縮・実行された後、痕跡を除去します。攻撃者はサンドボックスおよび分析回避のために圧縮関連プロセスを終了する機能を含み、GitHub からリモートスクリプトをダウンロードして C2 通信を確立します。



[図 3: SectorA05 グループが活用したミッキ文書]

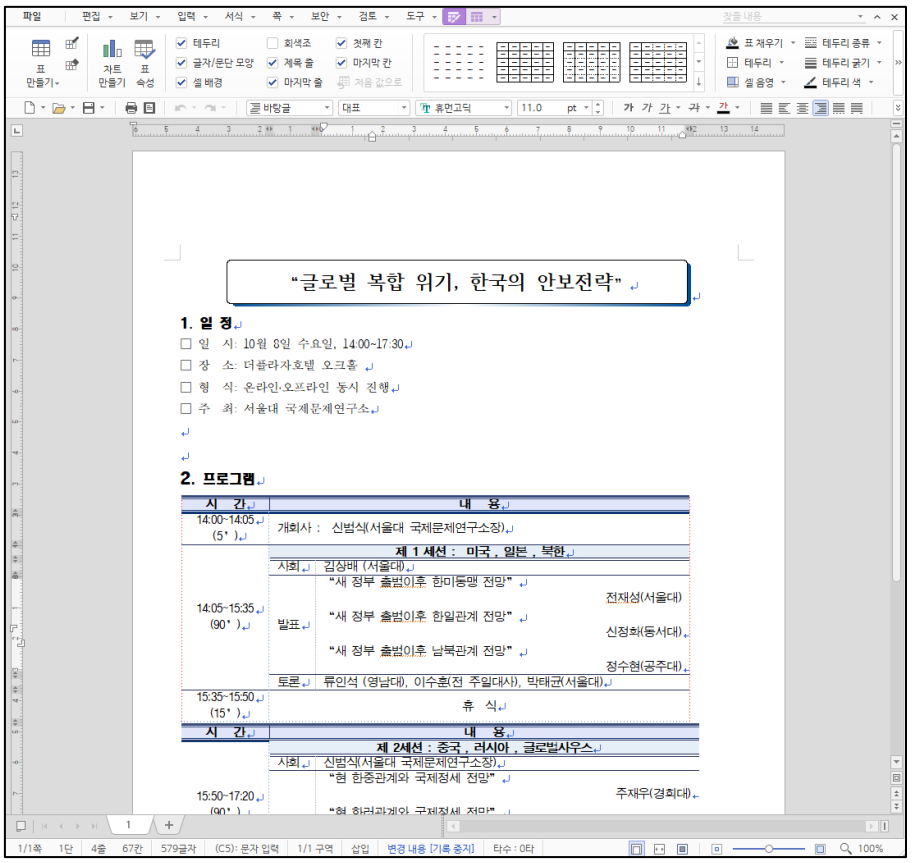
[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 在韓中国大使館の武官部を装った LNK ファイルを使用
   b. 国防大学校 教授ターゲット
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. 隠しおよび最小化された PowerShell スクリプト実行
   b. 文字列結合および Base64 エンコーディングで難読化
3. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Base64 エンコーディングでスクリプト難読化
   b. 文字列結合を通じたコード変形
4. [Discovery] File and Directory Discovery (T1083)

a. 現在のディレクトリと %TEMP% フォルダ検索
b. ファイルサイズに基づいて LNK ファイル識別
5. [Defense Evasion] Indicator Removal on Host (T1070.004)
a. 元の LNK ファイル削除
b. 実行後の痕跡除去
6. [Defense Evasion] Impair Defenses: Disable or Modify Tools (T1562.001)
a. Bandizip、WinRAR などの圧縮ツール関連プロセス終了
b. 分析ツール検出回避
7. [Collection] Data from Local System (T1005)
a. LNK ファイルから.hwp ファイルへペイロード抽出
b. .hwp ファイルを%TEMP%にコピー
8. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
a. GitHub からリモートスクリプトダウンロード
b. C2 通信確立

7) SectorA05 used LNK Malware disguised as Security Strategy Doc (2025-09-28)
https://cti.nshc.net/events/view/19190

攻撃者は「Global Complex Crisis Korea's Security Strategy.lnk」という名前の Malware ファイルを利用して攻撃を実行した。この攻撃はバックグラウンドモードで PowerShell スクリプトを実行することから始まり、現在のディレクトリで正確に 56,397 バイトのファイルを識別するか、ファイルがない場合は%TEMP%ディレクトリで代替ファイルを探す。スクリプトは識別された.lnk ファイルのすべてのバイトを読み取り、オフセット 5709 から 50,688 バイトの範囲を抽出して.hwp 拡張子で新しいファイルを生成し、即座に実行する。その後、元の.lnk ファイルを削除して痕跡を消す。攻撃は Base64 でエンコードされた文字列を繰り返しデコードし、PowerShell の“Invoke-Expression”コマンドを通じて実行し、追加ダウンロード、コマンド実行、C2 通信を確立する無限ループを形成する。この脅威は 10 月 8 日にソウル大学研究所で開催されたイベントと関連があり、標的接近方式を示唆している。



[図 4: SectorA05 グループが活用したミッキ文書]

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. ソウル大学研究所の行事を偽装する
   b. "Global Complex Crisis Korea's Security Strategy.lnk" ファイルを使用する
2. [Execution] User Execution (T1204)
   a. 抽出された .hwp ファイルを実行する
3. [Execution] Command and Scripting Interpreter (T1059)
   a. バックグラウンドモードで PowerShell スクリプトを実行する
   b. Invoke-Expression を使用してコマンドを実行する
4. [Defense Evasion] Indicator Removal on Host (T1070)
   a. 元の .lnk ファイルを強制的に削除する
5. [Discovery] File and Directory Discovery (T1083)
   a. 現在のディレクトリでファイルを検索する
   b. %TEMP% ディレクトリで代替ファイルを検索する
6. [Collection] Data from Local System (T1005)
   a. .lnk ファイルのバイトを読み取る
   b. 特定のバイト範囲を抽出する

7. [Command and Control] Application Layer Protocol (T1071)
   a. Base64 文字列をデコードしコマンドを実行する
   b. C2 通信を行う

8) SectorA05 used DLL Malware disguised as Windows Process (2025-10-08)

https://cti.nshc.net/events/view/19183

悪性 DLL ファイル “osinfo.dll”は Windows システムを主要な対象とするサイバー脅威に使用されました。このマルウェアは “regsvr32”を活用して実行され、正常なシステムパスの代わりにすべてのユーザーがアクセス可能な共用ユーザーディレクトリに “svchost.exe”を生成して偽装しました。DLL ファイルは 3 分ごとに悪性 “svchost.exe”がロードされるタスクスケジューラのタスクを登録して持続性を確保し、該当タスクは正常プロセスに偽装するために "IconCache"という名前で偽装しました。悪性コマンドは “cmd.exe”を通じて実行され、タスクスケジューラを活用した繰り返し実行で検出回避および長期的な生存性を図ります。

[Attack Flow]

1. [Execution] Command and Scripting Interpreter (T1059)
   a. regsvr32 を使用して“osinfo.dll”実行
   b. “cmd.exe”を通じてコマンド実行
2. [Defense Evasion] Masquerading (T1036)
   a. “svchost.exe”生成
   b. タスク名を"IconCache"に偽装
3. [Persistence] Scheduled Task/Job (T1053)
   a. schtasks で 3 分ごとに実行されるタスク生成
   b. 持続的な“svchost.exe”実行を通じて持続性維持
4. [Privilege Escalation] Create or Modify System Process: Windows Service (T1543.003)
   a. schtasks を通じて権限昇格試行
   b. システムサービスに偽装して検出回避
5. [Collection] Data from Local System (T1005)
   a. システム情報収集
6. [Command and Control] Application Layer Protocol (T1071)
   a. “svchost.exe”を通じたコマンド制御
   b. 持続的なネットワーク通信維持

9) SectorA05 used Phishing LNK disguised as EU Meeting Invite (2025-10-20)

https://cti.nshc.net/events/view/19504

攻撃対象産業群: 外交

攻撃者は 2025 年 5 月 13 日、EU 高位関係者を装い、西ヨーロッパの大使館を対象にフィッシング攻撃を実行した。メールには"Political Advisory Meeting to be held at the EU Delegation on May 14.pdf"という件名の ZIP ファイルが添付されており、これを通じて外交官に対し、近づく EU 会議に関する詳細情報を提供するかのように誘導した。攻撃は GitHub をコマンドおよびコントロールチャネルとして活用する Malware ショートカットファイル(.lnk)を使用した。このスクリプトは餌の PDF をダウンロードし、PowerShell コマンドを実行して持続性を維持し、追加のペイロードをダウンロードした。スクリプトは"MicrorfteguesoftUpdatemomentbrowHLDEU"という予約タスクを生成し、PowerShell スクリプトを定期的に実行した。主要技術にはファイル偽装、GitHub を通じたペイロード転送、タスクスケジューラの悪用および PowerShell ベースのコマンド実行が含まれていた。攻撃の意図は、敏感な外交データと通信への不正アクセスを獲得することだった。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. EU 高位関係者を装ったメール送信
   b. 外交官誘引のための ZIP ファイル添付
2. [Execution] User Execution: Malicious File (T1204.002)
   a. ZIP ファイル内の悪性ショートカットファイル(.lnk)実行
   b. PowerShell スクリプトを通じたコマンド実行
3. [Command and Control] Application Layer Protocol (T1071)
   a. GitHub を通じたコマンドおよび制御チャネル構築
   b. GitHub からペイロードファイルダウンロード
4. [Persistence] Scheduled Task/Job: Scheduled Task (T1053.005)
   a. "MicrorfteguesoftUpdatemomentbrowHLDEU"予約タスク作成
   b. PowerShell を隠しモードで定期実行
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Base64 エンコードおよび難読化されたスクリプト使用
   b. GitHub Personal Access Token を通じた隠匿性強化
6. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 外交データおよび通信への無断アクセス試行
   b. C2 チャネルを通じたデータ流出の可能性

10) SectorB65 used Backdoor variant (2025-09-23)

https://cti.nshc.net/events/view/19374

攻撃対象産業群: 通信

サイバー攻撃キャンペーンは 2022 年から中央および南アジアの通信および製造部門を対象に新しい PlugX 変種を活用して進行された。キャンペーンは合法的なアプリケーションに偽装して Malware を実行する DLL 検索順序ハイジャック手法を使用した。新しい PlugX 変種は RainyDay および Turian バックドアと DLL サイドローディング、モバイルポップアップアプリケーションを通じたローディング、XOR-RC4-RtlDecompressBuffer 暗号化方法などの特性を共有していた。これらのバックドアは RC4 キーを共有し、脅威行為者間の潜在的な協力またはツールソースの共有を示していた。Malware ローダーはメモリ内にシェルコードを復号化し、アンパッキングし、PlugX はプロセスインジェクションを実行し、Turian は特定の実行ファイルを使用してコード実行を行った。このキャンペーンはコード暗号化、圧縮および洗練された実行戦術を通じて隠密性を維持する洗練されたアプローチを示した。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
   a. メールの添付ファイルを介した初期アクセス
   b. 悪性文書ファイル実行
2. [Execution] DLL Search Order Hijacking (T1574.001)
   a. 悪性 DLL ファイル実行
   b. 合法的なプロセスを装ってコード実行
3. [Persistence] DLL Side-Loading (T1574.002)
   a. システム再起動時に持続性維持
   b. 正規アプリケーションと共に悪性 DLL ローディング
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. XOR-RC4-RtlDecompressBuffer 暗号化を通じたコード隠蔽
   b. コード圧縮および難読化
5. [Credential Access] Credential Dumping (T1003)
   a. メモリダンプを通じた資格情報収集
   b. パスワードハッシュ抽出
6. [Command and Control] Encrypted Channel (T1573)
   a. RC4 暗号化を通じた通信セキュリティ
   b. C2 サーバーとの暗号化されたデータ転送
7. [Execution] Process Injection (T1055)
   a. PlugX を通じたプロセスインジェクション実行
   b. 他のプロセスに悪性コード挿入
8. [Execution] Trusted Developer Utilities Proxy Execution (T1218)

a. Turian の特定実行ファイルを通じたコード実行
b. 信頼できるユーティリティを利用した回避実行

11) SectorB72 used NET-STAR Malware to Target IIS Web Servers (2025-09-30)

https://cti.nshc.net/events/view/19045

攻撃対象産業群: 政府・行政、通信、軍事機関

政府および通信部門を対象としてアフリカ、中東、アジアでサイバー諜報活動が実施された。主要な標的は外交部や大使館などの外交通信および防衛関連情報であり、これは関連国の戦略的利益と一致する。攻撃者は独自に開発されたツールと Malware を活用し、固有の戦術、技術、手順(TTP)を適用した。注目すべき点は、データ収集方法がメールサーバー中心から Microsoft SQL Server ベースのデータベース抽出に転換されたことである。データ抽出には“mssq.bat”スクリプトが使用されたことが確認された。また、IIS ウェブサーバーを標的とする新しい Malware 製品群'NET-STAR'を導入し、IIServerCore, AssemblyExecuter V1, AssemblyExecuter V2 といった構成要素を通じて多様な攻撃段階を実行し持続性を維持し、AMSI および ETW 回避技術といった検出回避技術を使用した。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. IIS ウェブサーバーの脆弱性を悪用する
   b. .NET ベースのマルウェアをインストールする
2. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.003)
   a. "mssq.bat" スクリプトを介して SQL Server に接続し、データを抽出する
   b. WMI を使用してリモートの SQL Server 上でスクリプトを実行する
3. [Persistence] Web Shell (T1505.003)
   a. "OutlookEN.aspx" のウェブシェルを使用する
   b. IIServerCore をメモリ内で実行する
4. [Defense Evasion] Timestomp (T1070.006)
   a. ASPX ファイルのタイムスタンプを変更する
   b. コンパイル時のタイムスタンプを未来の日付に変更する
5. [Credential Access] Credentials from Password Stores (T1555)
   a. Mimikatz を用いた資格情報の収集
   b. ネットワーク認証サービスの悪用による資格情報の窃取
6. [Collection] Data from Information Repositories (T1213)
   a. SQL データを CSV ファイルにエクスポートする
   b. 特定テーブルおよびキーワードで検索する

7. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 暗号化された C2 通信チャネルを使用する
   b. 収集したデータを暗号化して送信する
8. [Command and Control] Application Layer Protocol (T1071)
   a. AES 暗号化を使用した C2 通信
   b. Base64 エンコーディングを用いたデータ送信

12) SectorB79 used ArcGIS Web Shell disguised as Legitimate Java SOE (2025-10-14)

https://cti.nshc.net/events/view/19425

攻撃者は地理マッピングアプリケーションシステムを標的にして 1 年間にわたり悪意のある活動を維持するための精巧なサイバー攻撃を実行しました。攻撃者はアプリケーションの合法的なサーバーオブジェクト拡張 (SOE) を隠密な web shell に操作しました。彼らは損傷した資格情報とエンコードされたコマンドを使用してシステムにアクセスした後、web shell をシステムバックアップに含めて持続性を確保しました。ハードコーディングされたキーを活用してアクセスを制御し、他のユーザーがバックドアを変更できないようにしました。これらの方法はネットワーク全体での側面移動、コマンド実行、および資格情報収集といった直接的な活動を可能にしました。彼らの戦術には、持続的なアクセスのための名前が変更された VPN 実行ファイルの配布、ネットワークレベル C2 接続を合法的に見せること、そして悪用されたワークステーションを通じたデータ脱取が含まれていました。この攻撃は信頼できるシステムコンポーネントが攻撃者によって再利用される主要なセキュリティギャップを強調し、行動検出の改善と公開アプリケーションを高リスク資産として考慮する必要性を強調しました。

[Attack Flow]

1. [Initial Access] Valid Accounts (T1078)
   a. 侵害された資格情報を使用する
   b. ポータル管理者アカウントにログインする
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. エンコードされた PowerShell コマンド実行
   b. JavaSimpleRESTSOE 拡張使用
3. [Persistence] Create or Modify System Processes: Windows Services (T1543.003)
   a. 名前が変更された SoftEther VPN 実行ファイルアップロード
   b. 新しいサービス作成および自動開始設定
4. [Defense Evasion] Masquerading: Rename Legitimate Utilities (T1036.005)
   a. VPN 実行ファイルの名前変更

b. System32 ディレクトリに配置
5. [Credential Access] OS Credential Dumping (T1003)
   a. SAM データベースダンプ試行
   b. LSA シークレットアクセス
6. [Discovery] Account Discovery: Local Account (T1087.001)
   a. whoami コマンド実行
   b. ローカル管理者権限確認
7. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. HTTPS を通じた外部接続試行
   b. 攻撃者制御 IP へのトラフィック送信
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. データ C2 チャネルを通じた脱出
   b. ワークステーションからのデータ収集

13) SectorB86 exploited VMware vCenter with BRICKSTORM malware (2025-09-25)

https://cti.nshc.net/events/view/18863

攻撃対象産業群: 法律サービス、技術

攻撃者は最近、アメリカ内の複数の組織をターゲットに BRICKSTORM Malware を使用して持続的なアクセスを試みました。この活動は主に法律サービス、SaaS、BPO および技術分野の産業群を対象としており、伝統的なスパイ活動を超えてゼロデイエクスプロイトの開発を含むことを目指していました。キャンペーンは高度な技法を使用して平均 393 日間検出されずに留まり、初期侵入ベクトルはネットワーク機器のゼロデイ脆弱性を悪用する方法で頻繁に発生しました。BRICKSTORM は Go で書かれた SOCKS プロキシ機能を持つバックドアで、伝統的な EDR ツールをサポートしない Linux および BSD ベースの機器に配布されます。脅威行為者は初期侵入後、検出を避けるために起動スクリプトの修正、ウェブシェルの生成、カスタムドロッパーの使用などを含む高度な方法を使用して側面移動を行いました。資格情報は SOCKS プロキシ機能を使用して流出され、VMware vCenter サーバーが敏感な情報を含む仮想マシンの複製の主要な対象となりました。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. ネットワーク機器のゼロデイ脆弱性悪用
   b. リモートアクセスインフラ集中攻撃
2. [Persistence] Create or Modify System Process (T1543)
   a. 起動スクリプト修正
   b. カスタムドロッパーを使用したバックドアインストール

3. [Execution] Command and Scripting Interpreter: Unix Shell (T1059.004)
   a. Unix スクリプトを通じたコマンド実行
   b. Web シェルを通じたコマンド実行
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Malware 難読化
   b. 反検知技法使用
5. [Credential Access] Credentials in Files (T1552.001)
   a. 資格証明ファイルアクセス
   b. SOCKS プロキシ機能を通じた資格証明流出
6. [Lateral Movement] Remote Services (T1021)
   a. 有効な資格証明を使用した側面移動
   b. VMware vCenter サーバーへの移動
7. [Collection] Data from Information Repositories (T1213)
   a. vCenter サーバーの機密情報収集
   b. メールおよびコードリポジトリアクセス
8. [Exfiltration] Exfiltration Over Web Service (T1567)
   a. Web サービスを通じたデータ流出
   b. SOCKS プロキシを通じたファイル転送

14) SectorB110 used Malware disguised as Microsoft Debugger (2025-10-15)

https://cti.nshc.net/events/view/19398

攻撃対象産業群: IT、政府・行政

2025 年初、脅威行為者が南米、南アジア、台湾、そして特にロシアの複数の組織を対象に広範囲なサイバー諜報活動を行った。この活動は、ロシアのある IT サービスプロバイダーに対する長期間のアクセスを含み、ソフトウェアビルドシステムを活用したサプライチェーン攻撃と Yandex Cloud を通じたデータ窃取を可能にした。攻撃者は Yandex Cloud がロシア内で合法的なサービスと認識される点を利用して疑念を避けようとした。2025 年 7 月、南米のある政府機関は開発中の新しいバックドア配布で被害を受けた。この Malware は Microsoft Graph API と OneDrive をコマンド&コントロールに使用し、DLL サイドローディング、SMBExec、予約タスクを利用した側面移動および持続性を維持した。一方、2024 年末に侵害された台湾ソフトウェア会社のネットワークでは、DLL サイドローディング、ShadowPad Malware、BYOVD 技術が防御システムを無力化するために使用され、グループが合法的なツールとクラウドサービスを好んで使用し、隠密性と持続性を維持しようとする意図を強調した。これらの行動は、グループの持続的な洗練された Malware とサイバー諜報戦術の開発を示している。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. IIS サーバー脆弱性悪用
   b. Web シェル配布
2. [Execution] Command and Scripting Interpreter (T1059)
   a. CDB ツールを通じたシェルコード実行
   b. DLL サイドローディング活用
3. [Persistence] Scheduled Task/Job (T1053)
   a. 予約タスク作成
   b. 持続的ネットワークアクセス維持
4. [Privilege Escalation] Process Injection (T1055)
   a. “mspaint.exe”を通じたプロセス注入
   b. シェルコードメモリ実行
5. [Defense Evasion] Masquerading (T1036)
   a. 合法的バイナリ名変更
   b. KillAV ツールで防御ソリューション終了
6. [Credential Access] Credential Dumping (T1003)
   a. Mimikatz で資格情報ダンプ
   b. LSASS メモリから資格情報抽出
7. [Discovery] System Information Discovery (T1082)
   a. システム情報収集
   b. ネットワークホスト情報収集
8. [Lateral Movement] Remote Services (T1021)
   a. SMBExec でネットワーク移動
   b. AnyDesk リモート管理ソフトウェア使用
9. [Collection] Data from Local System (T1005)
   a. 対象システムからファイルリスト収集
   b. C:¥ProgramData¥application.ini にロギング
10. [Command and Control] Web Service (T1102)
    a. Microsoft Graph API 使用
    b. OneDrive を C&C サーバーとして活用
11. [Exfiltration] Exfiltration Over Web Service (T1567)
    a. Yandex Cloud でデータ送信
    b. OneDrive で情報アップロード

15) SectorB115 used Go-based Pantegana Backdoor in Espionage Campaign (2025-09-29)

https://cti.nshc.net/events/view/19010

攻撃対象産業群: 金融, 航空宇宙, ガス, 政府・行政, 国防, 軍事機関, 石油, 技術, 弁護士

攻撃者は 2024 年 6 月から 2025 年 7 月まで高度なサイバー諜報攻撃を全世界的に実行しました。この攻撃は、外交部、防衛産業、航空宇宙企業、法律事務所など主要な政府、国防、技術、民間部門機関のネットワークセキュリティ機器を標的にしました。攻撃者は侵入のために Go ベースのバックドアである Pantegana と Cobalt Strike を使用し、SonicWall、F5 BIG-IP、Fortinet FortiGate のような機器の脆弱性を利用して初期アクセス権を確保しました。彼らはスピアフィッシングと VPN およびその他のセキュリティ製品の既知の脆弱性の悪用を含む方法を使用しました。攻撃活動は台湾周辺の軍事訓練やパナマの外交的発展といった地政学的要因と顕著に一致しました。攻撃者はオープンソースツールを活用して大規模攻撃を可能にし、出所を隠しました。偵察および侵害活動は、アメリカ、台湾、韓国、東南アジアおよびヨーロッパの複数の国を中心に広範囲に展開されたことが確認されています。

AUSTAL
USA

August 27, 2024

From: Austal USA IT Department

To: All Employees

Subj: VMware Horizon Vulnerability and Patch Tool Download

Dear Employees,

We have recently identified a critical security vulnerability in VMware Horizon that could pose significant risks to our network systems. Here are a few key concerns:

- **Unauthorized Access:** Attackers may exploit the vulnerability to gain unauthorized access, potentially compromising sensitive company data.
- **Remote Code Execution:** The vulnerability allows attackers to execute malicious code on affected systems, leading to potential system crashes or data breaches.
- **Privilege Escalation:** Attackers may use the vulnerability to escalate privileges, bypassing existing security controls and gaining more extensive control over the system.

To ensure the security of our company's network systems, please download and install the patch tool provided by the Austal USA IT Department from Patch Tools Download immediately.

If you have any questions regarding this process or the patch tool, please contact your IT representative.

[図 5: SectorB115 グループが活用したフィッシング文書]

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. SonicWall, F5 BIG-IP, Fortinet FortiGate 脆弱性悪用
   b. Outlook Web Access および Ivanti Connect Secure VPN 攻撃

2. [Initial Access] Spearphishing Link (T1566.002)
   a. E メールを通じたスピアフィッシング攻撃
   b. 指定されたリンクを使用して Malware インストール
3. [Execution] Command and Scripting Interpreter (T1059)
   a. Cobalt Strike を通じたコマンド実行
   b. Pantegana バックドア活用
4. [Persistence] Protocol Tunneling (T1572)
   a. ExpressVPN を通じた内部ネットワーク維持
   b. Warp VPN を利用したリモート接続
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. オープンソースツールを使用して出所隠蔽
   b. PoC エクスプロイトを武器化して検知回避
6. [Command and Control] Application Layer Protocol (T1071)
   a. Cobalt Strike および Pantegana を通じた C2 通信
   b. SparkRAT バックドア使用
7. [Collection] Data from Information Repositories (T1213)
   a. 機密情報収集
   b. ネットワーク内データ獲得
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. C2 チャネルを通じたデータ流出
   b. 収集されたデータ送信

16) SectorB117 used GOVERSHELL disguised as Archive File Downloads (2025-10-08)

https://cti.nshc.net/events/view/19214

攻撃者は 2025 年 6 月から 9 月まで北米、アジア、ヨーロッパの複数の機関を対象にスピアフィッシングキャンペーンを実施した。攻撃者は存在しない組織の信頼できる人物になりすまし、様々な言語とペルソナでフィッシングメールを送信した。メールは受信者をクラウドサービスや攻撃者サーバーにホスティングされた悪性ペイロードに誘導した。初期接触が行われた後、攻撃者は「関係構築フィッシング」技法を活用して会話に参加し、その後悪性リンクを送信した。ペイロードである GOVERSHELL は、ZIP または RAR アーカイブに隠された合法的に見える実行ファイルに DLL ハイジャッキングを利用して Malware を実行した。GOVERSHELL は 5 つの変種に進化し、リモートコマンド実行を可能にし、スケジュールされたタスクを通じて持続性を維持した。技術的指標とキャンペーン特性の分析結果、この行為者は中国と関連する脅威グループと推定され、ChatGPT のような大規模言語モデル(LLM, Large Language Model)をフィッシングメール作成および Malware 開発過

程に活用したことを示している。このような LLM 活用の状況は、フィッシングメール内の文脈不一致や非論理的な内容などで間接的に明らかになったと分析される。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. 存在しない組織の信頼できる人物を装う
   b. 多様な言語と人物でフィッシングメール送信
2. [Execution] User Execution (T1204.002)
   a. ZIP または RAR アーカイブファイル実行
   b. 合法的に見える実行ファイルで DLL ハイジャック
3. [Persistence] Scheduled Task/Job (T1053.005)
   a. スケジュールされたタスクを通じた持続性維持
   b. GOVERSHELL の持続性設定
4. [Command and Control] Application Layer Protocol (T1071.001)
   a. 偽の TLS, HTTPS, WebSocket など多様な通信方式使用
   b. C2 サーバーとの暗号化通信
5. [Defense Evasion] Masquerading (T1036.005)
   a. 合法的な実行ファイルに偽装
6. [Collection] Input Capture (T1056)
   a. リモートコマンド実行機能提供
   b. 被害者システム情報収集および伝達

17) SectorB118 used Velociraptor to deploy LockBit and Babuk ransomware (2025-10-09)

https://cti.nshc.net/events/view/19217

攻撃対象産業群: IT

攻撃者は 2025 年 8 月、組織の IT インフラを対象に複雑なランサムウェア攻撃を実行した。Warlock、LockBit、Babuk を含む複数のランサムウェア変種を配布し、VMware ESXi 仮想マシンと Windows サーバーに被害を与えた。攻撃者は持続的なアクセスを確保するために脆弱なバージョンの Velociraptor を利用し、コマンド実行とコマンド＆コントロールサーバーへの潜在的なトンネル生成に活用した。Windows システムではファイルレス PowerShell スクリプトを使用して大量暗号化を実行し、リアルタイム保護、行動モニタリングおよびファイル活動のチェックを無効化するために Active Directory グループポリシーオブジェクトを修正した。Babuk ランサムウェアは ESXi サーバーで部分暗号化に独特に使用された。攻撃者はまた、データ脱取のために PowerShell スクリプトを使用し、“$ProgressPreference”を“SilentlyContinue”に設定して検出を回避した。この攻撃

は以前に知られている技術およびツールとの類似性を持つ特定の脅威グループと適度な関連性を持つ
。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. ToolShell 脆弱性悪用
   b. ウェブアプリケーション脆弱性利用
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. ファイルレス PowerShell スクリプト実行
   b. PowerShell を通じた大量暗号化実行
3. [Persistence] Account Manipulation (T1098)
   a. 管理アカウント作成
   b. Velociraptor を通じた持続的アクセス維持
4. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
   a. Velociraptor の脆弱性(CVE-2025-6264)悪用
   b. 管理者権限獲得試行
5. [Defense Evasion] Impair Defenses: Disable or Modify Tools (T1562.001)
   a. グループポリシーオブジェクト(GPO)修正
   b. リアルタイム保護およびモニタリング機能無効化
6. [Credential Access] OS Credential Dumping (T1003)
   a. 管理者権限獲得後資格情報ダンプ
   b. 内部ネットワーク移動のための資格情報収集
7. [Discovery] System Network Configuration Discovery (T1016)
   a. ネットワーク設定および構成情報収集
   b. 内部システムおよびサービス探索
8. [Lateral Movement] Remote Services: Remote Desktop Protocol (T1021.001)
   a. RDP を通じたシステム間移動
   b. Smbexec を使用したリモートコマンド実行
9. [Collection] Data from Information Repositories (T1213)
   a. 重要なファイルおよび情報収集
   b. ファイルおよびデータストア探索
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. PowerShell スクリプトを通じたデータ脱出
    b. $ProgressPreference を'SilentlyContinue'に設定して検知回避
11. [Impact] Data Encrypted for Impact (T1486)

a. Warlock, LockBit, Babuk を通じたデータ暗号化
b. ESXi サーバーの部分暗号化実行

18) SectorC14 used ClickFix with BAITSWITCH disguised webpage in Russia (2025-09-24)

https://cti.nshc.net/events/view/18894

攻撃対象産業群: 教育、ジャーナリスト、社会運動団体、市民団体

攻撃キャンペーン ClickFix は、ロシアの市民社会関連の個人と組織を対象とした高度な多段階攻撃チェーンです。攻撃は、被害者が市民活動家のためのリソースを装ったウェブページを訪問することから始まり、彼らは操作された Cloudflare Turnstile チェックボックスを通じて悪意のあるコマンドを実行するように欺かれます。このコマンドは、Windows “rundll32.exe”ユーティリティを使用して“machinerie.dll”という悪性 DLL、BAITSWITCH をダウンロードして実行します。BAITSWITCH は持続性を確立し、制御されたドメインから PowerShell ベースのバックドア SIMPLEFIX をダウンロードします。攻撃者は検出を回避するために難読化およびレジストリに保存されたペイロードを使用し、特定のユーザーエージェント文字列でエンコードされた C2 チャネルを通じて独自の通信を保証します。SIMPLEFIX は、情報収集、追加スクリプトの実行、および C2 サーバーへの報告など、複数のタスクを実行します。このキャンペーンは、クリップボード改ざん・プロセス持続性の確保・高度なデータ窃取技術を併用する高度な攻撃手法を使用しています。

[Attack Flow]

1. [Initial Access] Spear Phishing Link (T1566.002)
   a. 操作されたウェブページ訪問
   b. 悪性コマンド実行誘導
2. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.007)
   a. 悪性 JavaScript コード実行
3. [Persistence] Registry Run Keys / Startup Folder (T1547.001)
   a. UserInitMprLogonScript レジストリキー設定
   b. ログオン時に PowerShell スクリプト実行
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. 難読化された PowerShell スクリプト使用
   b. レジストリに暗号化されたペイロード保存
5. [Credential Access] OS Credential Dumping (T1003)
   a. システムユーザー情報収集
   b. ネットワーク構成情報収集
6. [Discovery] System Information Discovery (T1082)

a. システム情報収集コマンド実行
b. ユーザー情報およびネットワーク情報収集
7. [Collection] Data from Local System (T1005)
a. 特定ファイルタイプスキャンおよび収集
b. 文書およびアーカイブファイル収集
8. [Command and Control] Application Layer Protocol (T1071)
a. 特定ユーザーエージェント文字列で C2 サーバーと通信
b. HTTP リクエストを通じてコマンド受信および実行
9. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. 収集されたデータを C2 サーバーに送信

19) SectorC36 used FILEMESS Stealer with Telegram Exfiltration (2025-10-14)

https://cti.nshc.net/events/view/19408

攻撃対象産業群: 政府・行政、軍事機関

攻撃者たちは 2025 年 9 月下半期にウクライナの複数の地域防衛軍および地方政府機関を対象にサイバー攻撃を実行しました。この攻撃はウクライナ保安局の通信を装い、ロシアのサボタージュおよび偵察グループに対応するテーマを利用しました。主要な配信方法としては、Ukr.net や Gmail のようなサービスを通じてメールを送信し、VHD ファイルをダウンロードするリンクを含めたり、直接添付したりしました。これらのファイルは主に実行ファイルと PDF 形式の文書を含んでいました。攻撃者たちは GitHub で提供される多機能ツールである OrcaC2 と Go でコーディングされたファイル窃取ツールである FILEMESS を活用しました。FILEMESS は再帰的ファイル検索を実行し、Telegram API を通じてこれを流出させました。ファイルの持続性を確保するためにレジストリ項目を生成し、認証トークンを暗号化し、複数インスタンスの実行を防ぐためにこれを確認しました。OrcaC2 はコマンド実行、ファイル転送およびトラフィックトンネリングのような機能を提供しました。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
a. Ukr.net と Gmail を通じたメール送信
b. VHD ファイルダウンロードリンク添付
2. [Execution] User Execution (T1204)
a. VHD ファイル内実行ファイル実行
b. PDF ドキュメント閲覧誘導
3. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)

a. レジストリエントリ作成
4. [Collection] File and Directory Discovery (T1083)
a. FILEMESS を通じた再帰的ファイル検索
b. ファイル脱取準備
5. [Command and Control] Application Layer Protocol (T1071)
a. OrcaC2 を通じたコマンド実行
b. ファイル転送およびトラフィックトンネリング
6. [Exfiltration] Web Service (T1567.001)
a. Telegram API を通じたファイル流出

20) SectorD05 used Phishing Domains Disguised as Video Conferencing Sites (2025-09-27)

https://cti.nshc.net/events/view/19036

攻撃対象産業群: 政府・行政、軍事機関

攻撃者は 2025 年 7 月から複数のドメインを対象にフィッシング戦術を使用してサイバー脅威キャンペーンを進行した。このキャンペーンは主に合法的なビデオ会議サービス、例えば Google Meet を装う"online" TLD の類似ドメインを生成してフィッシング攻撃を実行した。攻撃者は"viliam"で始まるサブドメインパターンを使用して Malware コンテンツを配布し、被害者を誘引した。これらのドメイン、例えば"proof-video[.]online"や"look-together-online[.]online"はビデオ会議プラットフォームに偽装してイスラエルのユーザーを対象にしているように見える。攻撃者の一貫したフィッシングページ設定方法は、彼らのインフラ追跡を容易にした。このキャンペーンは依然として活性状態で、ビデオ会議サービスを対象とするサイバー諜報活動の継続的な脅威を強調している。

[Attack Flow]

1. [Reconnaissance] Gather Victim Information (T1589)
a. ドメインおよびサブドメイン調査
b. フィッシング対象選定および情報収集
2. [Resource Development] Acquire Infrastructure (T1583)
a. フィッシングドメイン登録
b. IPv4 アドレスを通じたドメイン設定
3. [Initial Access] Phishing: Spearphishing Link (T1566.002)
a. ビデオ会議サービスを装ったドメイン使用
b. "viliam" サブドメインパターン適用
4. [Execution] User Execution (T1204)
a. フィッシングリンククリック誘導

b. マルウェアページ接続誘導
5. [Credential Access] Input Capture (T1056)
a. 被害者資格証明収集
b. ログイン情報窃取
6. [Command and Control] Application Layer Protocol (T1071)
a. マルウェアページとの通信
b. 収集された情報送信

21) SectorD05 used Custom RATs for Phishing and DNS Manipulation (2025-10-07)

https://cti.nshc.net/events/view/19171

攻撃対象産業群: 金融, 政府・行政, エネルギー, 法律サービス

攻撃者は精巧なスパイ活動を遂行し、中東の政府、法律、学界、航空、エネルギー、金融部門を標的とした。アメリカとアジアも範囲に含まれた。流出した資料にはペルシャ語の文書が含まれており、組織構造と運営技法が明示されている。攻撃は “CVE-2024-1709” と DNS 変造を活用した。カスタマイズされたリモートアクセスツールと EDR 回避技法を使用して、長期的な持続性とデータ流出のための社会工学およびインフラ損傷を誘導した。プロセスインジェクション、EDR 回避、サプライチェーンピボット、複雑なフィッシングインフラを含む高度な技術を示した。この組織的な努力は、かなりの地域的スパイ能力を示し、サプライチェーンおよび国家安全保障のリスクを引き起こす。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
a. CVE-2024-1709 脆弱性悪用
b. ウェブアプリケーション脆弱性攻撃
2. [Execution] Command and Scripting Interpreter (T1059)
a. リモートアクセスツール実行
b. スクリプトベースの Malware 実行
3. [Persistence] Account Manipulation (T1098)
a. Active Directory アカウント制御
b. 長期的なアクセス維持
4. [Privilege Escalation] Process Injection (T1055)
a. プロセスメモリに Malware 挿入
b. 権限昇格のためのメモリ操作
5. [Defense Evasion] Obfuscated Files or Information (T1027)
a. EDR 回避のためのファイル難読化
b. DLL ペイロード改ざん

6. [Credential Access] Credential Dumping (T1003)
   a. Active Directory 資格情報ダンプ
   b. データベースパスワード抽出
7. [Discovery] System Information Discovery (T1082)
   a. システム情報収集
   b. ネットワークインフラマッピング
8. [Lateral Movement] Remote Services (T1021)
   a. リモートサービスを通じて移動
   b. 共有フォルダ列挙
9. [Collection] Data from Information Repositories (T1213)
   a. データベースダンプ
   b. メールアーカイブ抽出
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. C2 チャネルを通じたデータ送信
    b. 暗号化されたアーカイブファイル送信
11. [Impact] Data Manipulation (T1565)
    a. DNS 設定操作
    b. ウェブサイトおよびシステム設定変更

22) SectorD05 used GenAI for PDF disguised as RAND document (2025-10-15)

https://cti.nshc.net/events/view/19360

イランの脅威グループは最近のサイバーキャンペーンで生成 AI ツールを活用した。攻撃はアメリカの非営利研究機関の合法的な文書を装った悪性 PDF 文書を作成して実行された。この PDF はミキ文書として使用され、「PowerLess」として知られるマルウェアと共に配布された。表面的には本物の文書のように見えるこのファイルを通じて、対象のシステムを損傷させようとした。攻撃は PDF ファイルと"sin.dll", "sst.dll", "ssts.dll"を含む様々な DLL ファイルを活用して追加的な悪用を促進した。今回のキャンペーンは AI 生成コンテンツを統合して精巧なスピアフィッシングコンテンツを作成する事例を示し、人工知能を使用して攻撃戦術、技法、手順をさらに強化する進化する脅威環境を強調した。作戦の地理的焦点はアメリカであり、評判のある機関を装って敏感な情報を収集し侵入することを目的とした。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 悪性 PDF 文書を使用して誘引
   b. アメリカの非営利研究機関を装って信頼性を確保

2. [Execution] User Execution: Malicious File (T1204.002)
   a. PDF を通じて悪性ソフトウェアを実行
   b. PowerLess マルウェアを共に配布
3. [Defense Evasion] Masquerading: Match Legitimate Name or Location (T1036.005)
   a. 合法的な文書に似せて文書を作成
   b. DLL ファイルを合法的な名前で偽装
4. [Persistence] DLL Search Order Hijacking (T1574.001)
   a. sin.dll, sst.dll, ssts.dll ファイルを活用
   b. DLL ファイルを通じて持続性を確保
5. [Collection] Data from Local System (T1005)
   a. 敏感な情報を収集
   b. ターゲットシステムのデータを窃取
6. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 収集された情報を C2 チャネルを通じて流出
   b. 外部サーバーへデータを送信

23) SectorD15 used Phishing to Deliver MiniJunk Backdoor in Europe (2025-09-22)

https://cti.nshc.net/events/view/18799

攻撃対象産業群: 航空宇宙、通信、国防

攻撃者はヨーロッパの航空宇宙、防衛、通信部門を主要ターゲットとして、精巧なサイバー脅威キャンペーンを実行しました。デンマーク、スウェーデン、ポルトガルを中心に HR 採用担当者に偽装したスピアフィッシング戦術を使用し、各被害者にカスタマイズされた偽の求人ポータルを通じて攻撃を実行しました。攻撃は以前に文書化されていない API を利用して合法的なプロセスに悪性 DLL を挿入する複雑な多段階 DLL サイドローディング技法を活用しました。ツールセットには MiniJunk バックドアと MiniBrowse スティーラーが含まれており、コンパイラレベルの技法で強く難読化されて検出を回避します。MiniJunk は Minibike インプラントから発展した形態であり、Malware は有効なデジタル証明書とサイズ拡張技法を利用してセキュリティシステムを回避しました。コマンドおよびコントロールは複数の冗長サーバーとエンコードされた通信プロトコルを通じて実行されます。攻撃者は国家支援活動と連携した戦略的情報収集目標に合わせてヨーロッパのターゲットに焦点を拡大しました。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. HR 担当者として偽装したメール送信
   b. 偽の求人ポータルに接続するリンク提供

2. [Execution] User Execution (T1204)
   a. 被害者が"Setup.exe"を実行
   b. ユーザー環境 DLL(userenv.dll)サイドローディング
3. [Persistence] Scheduled Task/Job (T1053)
   a. "MigAutoPlay.exe"で実行ファイルコピー
   b. スケジュールされたタスク作成
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. コンパイラーレベルの難読化適用
   b. ファイルサイズ拡張技法
5. [Credential Access] Credentials from Web Browsers (T1555.003)
   a. ブラウザに保存されたクレデンシャル収集
   b. MiniBrowse スティーラー使用
6. [Discovery] System Information Discovery (T1082)
   a. コンピュータ名およびドメイン名収集
   b. ユーザー名収集
7. [Command and Control] Encrypted Channel (T1573)
   a. HTTPS リクエストを通じた C2 通信
   b. エンコードされたプロトコル使用
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 収集されたデータを C2 サーバーに送信
   b. ファイルデータチャンク送信およびリクエストパース

24) SectorE03 used CMD Backdoor and LNK Malware in Phishing Attacks (2025-09-29)

https://cti.nshc.net/events/view/19051

サイバー脅威組織は 2020 年から 2021 年の間に持続的な諜報活動を展開した。彼らは現地契約業者のような外注業者を活用して攻撃を実行し、このようなアプローチは低コストと基本的な技術的方法を可能にする。最近公開された情報によれば、このグループはフィッシングフレームワークを通じて攻撃を行っており、核心的な作業は"DeliveryBoy"というドロッパーを通じて"MadBoy"のようなローダーを配布し、持続性を維持する"Win"という CMD コマンド実行インプラントを含む。ローダーは動的にペイロードをロードし、プロセスインジェクションを使用する精巧な技術を活用する。また、GitHub に偽のプロジェクトを生成し、.xlsm ファイルのような悪性マクロを配布して資格情報を収集し、コマンド＆コントロールサーバーに接続して持続性を維持する。テスト結果はクラウドストレージをペイロード配信に活用し、Tor ノードを匿名性確保に使用していることを示している。これ

らのツールおよび技術の露出は、これらのサイバー脅威を正確にプロファイリングし予測することにおいて持続的な困難を強調する。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. フィッシングフレームワークを使用
   b. 悪性 zip ファイル添付
2. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.003)
   a. CMD コマンド実行
   b. C2 サーバーと接続
3. [Persistence] Scheduled Task/Job (T1053)
   a. DrivOneUpdat スケジュールタスク生成
   b. 持続性維持
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. ファイル分割および動的ローディング
   b. プロセスインジェクション使用
5. [Credential Access] Input Capture (T1056)
   a. 資格情報収集
   b. 悪性マクロ活用
6. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. C2 サーバーとウェブプロトコルで通信
   b. クラウドストレージでペイロード送信
7. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 収集されたデータ送信
   b. Tor ノード使用して匿名性確保

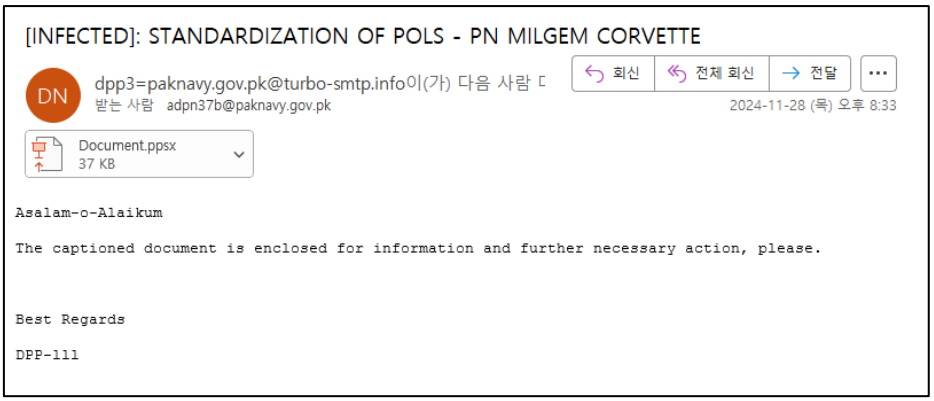
25) SectorE03 used Python Backdoor Malware disguised as PDFs on Windows (2025-10-02)

https://cti.nshc.net/events/view/19111

攻撃対象産業群: 政府・行政, 国防, 軍事機関

攻撃者は主に南アジアの Windows プラットフォームを対象にサイバー諜報活動を行った。特にパキスタンの政府、軍事、防衛、重要な産業を集中的に狙った。初期アクセスベクターとしてスピアフィッシングと悪性文書を活用し進化した。最近の活動は WooperStealer のような情報窃取型 Malware から Python ベースのバックドアおよび AnonDoor のような高度なツールへと発展し、技術的適応力を誇示した。数ヶ月にわたるキャンペーンでは武器化された Office 文書、LNK ファイル、カスタ

ム Python RAT を使用した。攻撃は権限スプーフィングを利用したフィッシングメールで始まり、OLE オブジェクトトリガー感染を通じてリモート URL に接続し、様々な悪性ソフトウェアコンポーネントをダウンロードした。ここには WooperStealer が含まれ、様々なファイルタイプをリモートサーバーに流出させ、システムプロファイリングおよび情報窃取のための構造化されたコマンドを使用した。より進歩した技法には DLL サイドローディングおよび Python ベースのバックドアが含まれ、技術的敏捷性と持続性を示した。悪性ソフトウェアは DLL サイドローディングおよびスケジュールされたタスクを利用して長期的なアクセスを目指し、エンコードされたコンポーネントを活用して可視性を減らした。



[図 6: SectorE03 グループが送信したスピアフィッシングメール]

[Attack Flow]

1. [Initial Access] SpearPhishing Attachment (T1566.001)
   a. フィッシングメール送信
   b. 武器化された Office 文書添付
2. [Execution] User Execution (T1204)
   a. 権限スプーフィングでユーザー実行誘導
   b. OLE オブジェクトでリモート URL 接続
3. [Persistence] Scheduled Task/Job (T1053)
   a. スケジュールされたタスクを通じて持続性維持
   b. Python バックドアを実行
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. エンコードされたコンポーネント使用
   b. 検知回避のための難読化
5. [Credential Access] Credential Dumping (T1003)
   a. PasswordDumper で資格情報抽出
   b. 追加の Python ファイルダウンロードおよび実行
6. [Collection] Data from Local System (T1005)

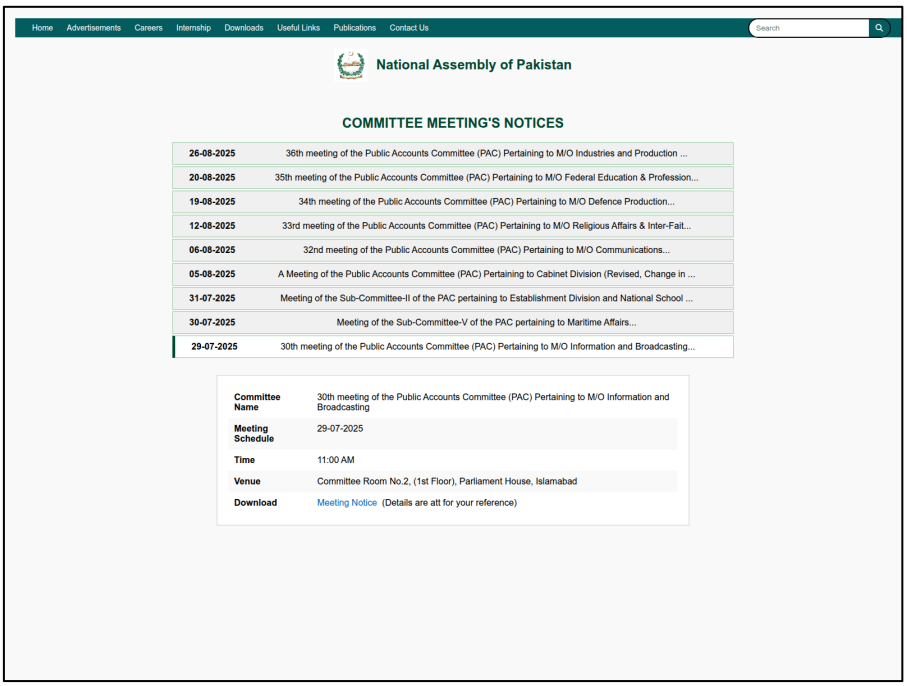
a. システムファイルタイプ収集
b. システムプロファイリング実行
7. [Command and Control] Application Layer Protocol (T1071)
a. C2 サーバーと通信
b. 構造化されたコマンド送信および受信
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. 収集されたデータをリモートサーバーに送信

26) SectorE04 used Hosting Platforms for Phishing and Malware Distribution (2025-10-01)

https://cti.nshc.net/events/view/19161

攻撃対象産業群: 政府・行政、軍事機関、海上、航空宇宙、研究・革新機関、通信

"Operation SouthNet"は南アジア諸国を対象とした精巧なサイバー脅威作戦であり、主にパキスタンとスリランカに集中し、バングラデシュ、ネパール、ミャンマー、シンガポールまで活動を拡張しました。このキャンペーンは Netlify、pages[.]dev、workers[.]dev、b4a[.]run のような無料ホスティングプラットフォームを活用して資格証明収集ポータルと海洋および政府テーマの餌文書を配布しました。50 以上の Malware ドメインが確認され、多くのドメインが地域ドメインに合わせた Outlook および Zimbra ウェブメールポータルのような合法的な政府サービスを装いました。攻撃者は古い C2 資産を再利用し、インフラを重ねることで持続的かつ適応的な技術を使用しました。
2025 年 8 月と 9 月の間には、長官委員会、二国間訪問、防衛調達を対象とする誘引文書がオープンディレクトリと実行ファイルを使用して配布されました。この作戦は新しいフィッシングドメインが数日ごとに登場する高い速度を示しました。部門別ターゲティングはパキスタンの SUPARCO、通信および航空宇宙部門を狙い、ミャンマー中央銀行とネパール財務部を偽装して進行しました。バングラデシュでは国防調達総局を模倣したポータルが拡散され、シンガポールでは人材部を偽装したフィッシングが集中しました。このキャンペーンは重要な国家部門を侵入しようとする意図を明らかにし、迅速なドメイン切り替えと精巧な社会工学技法を活用して諜報目的を持続的に達成しました。



[図 7: SectorE04 グループが活用したフィッシングページ]

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. 無料ホスティングプラットフォーム使用
   b. 政府サービス詐称ポータル使用
2. [Execution] User Execution (T1204)
   a. 誘引文書実行
   b. Web メールログインページへの誘導
3. [Credential Access] Input Capture (T1056)
   a. 資格証明収集ポータル配布
   b. 直接的な POST リクエスト使用
4. [Persistence] Valid Accounts (T1078)
   a. 盗用された資格証明使用
   b. 複数 Web メールポータルでのセッション維持
5. [Defense Evasion] Masquerading (T1036)
   a. 合法的な政府サービスに偽装
   b. 地域ドメインに合わせた Web メールポータル詐称
6. [Command and Control] Application Layer Protocol (T1071)
   a. 古い C2 インフラ再利用
   b. 複数プラットフォームを通じた C2 通信
7. [Exfiltration] Exfiltration Over C2 Channel (T1041)

a. 資格証明およびデータを C2 サーバーへ送信
b. セッション追跡のための隠されたインボックスフィールド使用

27) SectorE08 delivered malicious documents via phishing emails (2025-10-15)

https://cti.nshc.net/events/view/19399

攻撃対象産業群: 政府・行政、外交、金融、産業

APT グループはアジア-太平洋地域の政府機関および外交分野を積極的に攻撃し、主にパキスタン、バングラデシュ、スリランカを集中的に狙っている。2023 年に初めて識別されたこのグループは、既存の攻撃者と類似した戦術を使用したが、その後独自の運用方式を開発した。2025 年初頭に識別された最新キャンペーンは、戦術と技術の変化を示し、カスタマイズされたメールを使用したスピアフィッシングを通じて目標に侵入する。BabShell と MemLoader のようなカスタムおよびオープンソースツールを活用し、攻撃者は PowerShell スクリプトとリバースシェル機能を使用して持続性とコマンド実行を行う精巧な攻撃を実行する。MemLoader 変形を使用して高度なメモリ内実行および回避技術でペイロードを配信する。データ窃取は WhatsApp 通信に集中し、ChromeStealer Exfiltrator のようなモジュールを活用してファイルと Chrome データを盗む。該当グループのインフラはワイルドカード DNS、VPS、クラウドサービスを使用して運用弾力性を維持する。今回のキャンペーンは、地域サイバーセキュリティに対するグループの技術的精巧さと持続的な脅威レベルを強調する。

[Attack Flow]

1. [Initial Access] Spear Phishing Attachment (T1566.001)
   a. カスタマイズされたメールを使用して標的に侵入する
   b. スピアフィッシングメール内に悪性文書添付
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. PowerShell スクリプトで命令実行
   b. C2 サーバーから追加ペイロードダウンロード
3. [Persistence] Create or Modify System Process: Windows Service (T1543.003)
   a. サービス登録を通じた持続性維持
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. XOR 暗号化および Base64 エンコーディング使用
   b. MemLoader HidenDesk によるメモリ内ペイロードローディング
5. [Credential Access] Credential Dumping: LSASS Memory (T1003.001)
   a. LSASS メモリダンプを通じた資格情報獲得
   b. ChromeStealer Exfiltrator を通じた Chrome データ脱取
6. [Discovery] System Information Discovery (T1082)

a. システム情報収集
b. ユーザー名、コンピュータ名および MAC アドレス確認
7. [Collection] Data from Local System (T1005)
a. WhatsApp ファイルおよびデータ収集
b. ChromeStealer Exfiltrator 使用を通じたファイル脱取
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. C2 サーバーへ脱取されたデータ送信
b. BabShell を通じた命令実行結果送信
9. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
a. HTTPS を通じて C2 サーバーと通信
b. ワイルドカード DNS および VPS 使用して通信経路隠匿

28) SectorH03 used StealthServer Backdoor disguised as PDF shortcuts (2025-10-15)

https://cti.nshc.net/events/view/19494

攻撃対象産業群: 国防

攻撃者は 7 月初めから南アジア地域の Windows および Linux プラットフォームを対象に「StealthServer」という Malware を使用してサイバー攻撃を敢行した。この Malware は政治や軍事会議のテーマを含む Windows PPT ファイルの悪性マクロと Linux .desktop ファイルの PDF に偽装されたショートカットを含むフィッシングメールを通じて配布された。実行時に、これらのファイルは正常なドキュメントを開きながら Malware を配布した。この Malware は Go で開発されており、ファイル脱取およびコマンド＆コントロール（C2）サーバーを通じたリモートコマンド実行機能を備えたクロスプラットフォーム機能をサポートしていた。StealthServer はジャンクコードおよびダミー関数を挿入してリバースエンジニアリングを困難にした。この Malware は多様なネットワークプロトコルを使用して通信し、Windows 変種は TCP または WebSocket を、Linux 変種は HTTP または WebSocket を使用した。C2 サーバーとの通信は公式政府ドメインに類似したドメイン名を使用し、ペイロードを難読化して分析を困難にした。Malware はシステムサービスを登録し、開始スクリプトを修正し、予約タスクを生成するなどの技法を使用して感染したシステムに持続性を確立した。C2 サーバーと JSON 形式のデータを交換し、ファイルリストの照会、アップロードおよびダウンロードなどのコマンドを実行することができた。特に、ファイル脱取は検出回避のために AES 暗号化を通じて行われた。全体としてこのキャンペーンは高度な脅威戦術を示し、隠れた状態でターゲットシステムに対する制御を維持しようとする意図を明らかにした。

[Attack Flow]

1. [Initial Access] Phishing: Spear Phishing Attachment (T1566.001)

a. 悪性マクロを含む Windows の PPT ファイル
b. PDF に偽装した Linux の .desktop ショートカット
2. [Execution] User Execution: Malicious File (T1204.002)
a. 正常な文書を開くと同時にマルウェアを実行する
b. Linux の .desktop ファイルの実行によりマルウェアを配布する
3. [Defense Evasion] Obfuscated Files or Information (T1027)
a. ジャンクコードおよびダミー関数を挿入する
b. ペイロードを難読化する
4. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
a. システムサービスとして登録する
b. 起動スクリプトを変更する
5. [Command and Control] Application Layer Protocol: WebSocket (T1071.001)
a. Windows 亜種は TCP または WebSocket を使用する
b. Linux 亜種は HTTP または WebSocket を使用する
6. [Exfiltration] Exfiltration Over Alternative Protocol: Exfiltration Over WebSocket (T1048.003)
a. AES 暗号化を用いてファイルを流出させる
b. JSON 形式でデータを交換しコマンドを処理する

29) SectorH03 used ELF Malware Disguised as PDF Documents (2025-10-17)

https://cti.nshc.net/events/view/19443

攻撃対象産業群: 政府・行政、国防、軍事機関

攻撃者は Windows と Linux システムを対象にした精巧なサイバー脅威キャンペーンを実行しました。Windows では、攻撃者が.ppam ファイルを通じてマルウェアマクロを含め、ペイロードをダウンロードし、多段階攻撃チェーンを実行してデータ流出を目指しました。これらの.ppam ファイルは "Jammu Kashmir Police Letter"という名前を使用して実行を誘導しました。マクロスクリプトは静的検出を避けるために暗号で保護された ZIP ファイルをダウンロードし、ハードコーディングされたパスワードを使用してこれを復号し、リモート制御実行ファイルを配布しました。Linux では、攻撃者が.pdf 拡張子で偽装された.desktop ファイルを使用してユーザーを欺き、実行を誘導し、実行時に ELF 実行ファイルをダウンロードしました。ELF ペイロードは Golang で開発された新しい RAT で、“system”構成で持続性を維持し、リモートコマンド実行およびデータ窃取を行う機能を持っていました。両プラットフォームは共通ドメインを使用してペイロードを配布し、これは協調されたクロスプラットフォーム戦略を示しています。このキャンペーンは攻撃者の高度な回避技術と持続的なデータ窃取目標を強調しました。

[Attack Flow]

1. [Initial Access] Spearphishing Attachment (T1566.001)
   a. Windows: .ppam ファイル使用
   b. Linux: .desktop ファイル使用
2. [Execution] User Execution (T1204)
   a. Windows: マクロ実行誘導
   b. Linux: .desktop ファイル実行誘導
3. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. Windows: Registry にパス登録
   b. Linux: systemd を通じた持続性維持
4. [Command and Control] Application Layer Protocol (T1071)
   a. Windows: TCP を通じた C2 サーバー接続
   b. Linux: HTTP リクエストを通じた C2 サーバー接続
5. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. Windows: ファイル収集および転送
   b. Linux: ファイル収集および転送
6. [Collection] Data from Local System (T1005)
   a. Windows: ローカルシステム情報収集
   b. Linux: ユーザーおよびシステム情報収集

30) SectorT01 used Zimbra CVE-2025-27915 Exploit via Malicious .ICS File (2025-09-30)

https://cti.nshc.net/events/view/19177

攻撃対象産業群: 軍事機関

攻撃者は 2025 年リビア海軍儀典室を装い、ブラジル軍を対象に Zimbra コラボレーションスイートのゼロデイ脆弱性(CVE-2025-27915)を利用した攻撃を実行しました。この攻撃は、悪性.ICS ファイルを使用して Zimbra に似たオープンソースのコラボレーションツールの脆弱性をメールを通じて悪用しました。このスクリプトは Zimbra Web メールをターゲットとする包括的なデータ窃取 Malware で、資格情報、メール、連絡先、共有フォルダを含む様々なデータを ffrk[.]net/apache2_config_default_51_2_1 のコマンド＆コントロールサーバーに流出させました。Malware は実行遅延、3 日周期の実行頻度制限、ユーザーインターフェース要素の非表示などの回避技術を使用して検出を回避しました。ユーザー活動を監視し、非アクティブ状態が検出されるとデータを窃取しました。非同期 JavaScript 関数を使用して資格情報窃取、メール窃取を行い、ProtonMail アカウントにメールをリダイレクトする悪性メールフィルタルールを追加しました。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. スプーフィングされた発信者の使用
   b. 悪性 .ICS ファイル添付
2. [Execution] Exploitation for Client Execution (T1203)
   a. Zimbra コラボレーションスイートのゼロデイ脆弱性 (CVE-2025-27915) 活用
   b. メールを通じた脆弱性悪用
3. [Credential Access] Input Capture (T1056)
   a. ユーザー名とパスワードをキャプチャするための隠し入力フィールド生成
   b. ログインフォームでの資格情報窃取
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. ユーザーインターフェース要素の隠蔽
   b. コード実行の遅延および実行頻度の制限
5. [Persistence] Email Forwarding Rule (T1104)
   a. 悪性メールフィルタールールの追加
   b. メールを ProtonMail アカウントにリダイレクト
6. [Collection] Email Collection (T1114)
   a. 이메일폴더でメール検索および攻撃者サーバーへ送信
   b. Zimbra SOAP API を使用したメール検索
7. [Command and Control] Web Service (T1102)
   a. 非同期 JavaScript 関数でコマンド送信
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 脱取されたデータをコマンドおよび制御サーバーへ送信
   b. POST リクエストと"no-cors"モード使用

2. サイバー犯罪(Cyber Crime) ハッキンググループ活動

1) SectorJ04 used Oracle EBS Zero-Day CVE-2025-61882 for Data Theft (2025-10-06)

https://cti.nshc.net/events/view/19158

攻撃者は CVE-2025-61882 ゼロデイ脆弱性を利用して Oracle E-Business Suite (EBS)アプリケーションを対象に大規模攻撃を実行しました。2025 年 8 月 9 日に初めて観察されたこの攻撃の目的はデータの窃取でした。攻撃の流れは、認証されていないリモートコード実行脆弱性を活用し、特定の

HTTP POST リクエストを通じて認証を回避した後、Oracle の XML Publisher Template Manager を通じてマルウェアテンプレートをアップロードし、コードを実行する方式で進行されました。攻撃チェーンは持続的なアクセス維持のために web shell を配布することを含んでいました。Telegram を通じて PoC コードが流布され、これは多数の脅威行為者が関与している可能性を示唆しました。Oracle は 2025 年 10 月 4 日に該当脆弱性を公開し、公開後に機会主義的な悪用の可能性が高まりました。攻撃者制御サーバーへのアウトバウンド接続はポート 443 を通じて行われ、マルウェアテンプレートのアップロードおよびプレビューのための特定の GET および POST リクエストシーケンスが観察されました。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. CVE-2025-61882 脆弱性利用
   b. Oracle EBS アプリケーションターゲティング
2. [Execution] Command and Scripting Interpreter (T1059)
   a. マルウェアテンプレートアップロード
   b. コード実行のために XSLT テンプレート使用
3. [Persistence] Web Shell (T1505.003)
   a. Web シェル配布
   b. 持続的アクセス維持
4. [Collection] Data from Information Repositories (T1213)
   a. データ脱取試み
   b. Oracle EBS データベースアクセス
5. [Exfiltration] Exfiltration Over Web Service (T1041)
   a. ポート 443 を通じたアウトバウンド接続
   b. 攻撃者制御サーバーへのデータ送信

2) SectorJ165 delivered JavaScript Malware Disguised as Tax Form to Deploy C2 Tools (2025-09-29)

https://cti.nshc.net/events/view/19018

攻撃は 2024 年 5 月、税金フォームに偽装した悪性 JavaScript ファイルの実行で始まりました。このファイルは MSI インストーラーを通じて Brute Ratel ペイロードを実行し、Latrodectus および Cobalt Strike を含む様々な Malware を配布しました。攻撃者は LSASS、ブラウザデータ、Windows 応答(Answer)ファイルから収集した資格情報を通じて Windows システムにアクセスしました。侵入後 20 日目に、Rclone と FTP を使用してデータの窃取が発生しました。攻撃者はプロセスインジェクション、スケジュールされたタスクおよびレジストリ実行キーなどの複数のコマンド&

コントロール技術を活用して持続性を維持しました。作戦はほぼ 2 か月間続き、洗練された横移動とデータ窃取の戦術が特徴的でしたが、ランサムウェアは配布されませんでした。BackConnect VNC を通じて断続的に通信を維持し、様々なネットワーク環境で複数のペイロードを使用して脅威を管理しました。

[Attack Flow]

1. [Execution] Command and Scripting Interpreter: JavaScript (T1059.007)
   a. JavaScript ファイルでマルウェア実行
   b. MSI インストーラーで追加ペイロード実行
2. [Persistence] Registry Run Keys / Startup Folder (T1547.001)
   a. レジストリ実行キー作成
   b. 複数回レジストリキー更新
3. [Privilege Escalation] Bypass User Account Control (T1548.002)
   a. UAC 回避技法使用
   b. 権限昇格試行
4. [Defense Evasion] Process Injection (T1055)
   a. explorer.exe で Latrodectus インジェクション
   b. 複数プロセスに Cobalt Strike インジェクション
5. [Credential Access] OS Credential Dumping: LSASS Memory (T1003.001)
   a. LSASS プロセスから資格情報収集
   b. Veeam バックアップソフトウェアを通じて資格情報収集
6. [Discovery] System Information Discovery (T1082)
   a. Windows コマンドを使用してシステム情報収集
   b. Active Directory 情報収集
7. [Lateral Movement] Remote Services: SMB/Windows Admin Shares (T1021.002)
   a. PsExec でリモートホストにアクセス
   b. Zerologon 脆弱性を使用して移動
8. [Collection] Data from Information Repositories (T1213)
   a. ファイル共有サーバーからデータ収集
   b. メールおよびブラウザデータ収集
9. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. CloudFlare および Akamai を通じた C2 通信
   b. Brute Ratel および Cobalt Strike を通じた通信
10. [Exfiltration] Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003)
    a. Rclone および FTP を通じたデータ脱出
    b. ファイル共有サーバーから FTP サーバーへのデータ転送

3) SectorJ199 used StealC Stealer disguised as BlockBlasters patch (2025-09-22)

https://cti.nshc.net/events/view/18825

BlockBlasters ゲームは 2025 年 8 月 30 日のパッチ以降、悪性行動を示し始めた。このゲームは Steam プラットフォームで提供されており、アップデート過程で悪性コードが注入された。悪性パッチはプレイヤーがゲームを進行する間に暗号化通貨ウォレット情報を含む敏感なユーザーデータを脱取した。攻撃は"game2.bat"というトロイアンスティーラーバッチファイルで始まり、位置追跡、アンチウイルス検出、Steam ログインデータ収集などの機能を実行した。収集された情報はコマンド＆コントロール(C2)サーバーにアップロードされた。以降の段階では VBS ローダーが追加のバッチファイルを実行し、ブラウザ拡張プログラムと暗号化通貨ウォレットデータを収集した。主要ペイロードはパスワードが設定された圧縮ファイルに含まれており、バックドアおよび情報を脱取する機能を持っている。RC4 暗号化を使用して API 呼び出しを隠匿した。この事件は数百人のユーザーに影響を与え、該当ゲームは Steam から削除されたことが確認されている。

[Attack Flow]

1. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.003)
   a. "game2.bat" を実行する
   b. cmd.exe を介してバッチファイルを実行する
2. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. システム起動時に自動実行するよう設定する
   b. Windows Defender の例外リストに追加する
3. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. RC4 暗号化を用いて API 呼び出しを隠蔽する
4. [Credential Access] Credentials from Password Stores (T1555)
   a. Steam のログイン情報を収集する
   b. ブラウザに保存された暗号化パスワードを窃取する
5. [Discovery] System Information Discovery (T1082)
   a. IP および位置情報を収集する
   b. インストールされているアンチウイルス製品を検出する
6. [Collection] Data from Local System (T1005)
   a. 暗号通貨ウォレットのデータを収集する
   b. ブラウザ拡張機能の情報を収集する
7. [Command and Control] Encrypted Channel (T1573)
   a. RC4 暗号化を使用する
   b. C2 サーバーとの通信を維持する

8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 収集した情報を C2 サーバーに送信する
   b. 継続的に IP 情報を更新する

4) SectorJ212 used SVG Files to Deploy StarFish Reverse Shell Malware (2025-10-07)

https://cti.nshc.net/events/view/19164

2025 年 6 月、脅威行為者がドイツを対象に新しいフィッシングキャンペーンを実施しました。攻撃者は悪性 SVG ファイルを利用して StarFish というリバースシェル Malware をダウンロードしました。このスクリプトは持続的なアクセスを確立し、追加ペイロードの配布を可能にして脅威行為者の意図に変化をもたらしました。2 次ペイロードにはスクリーンショットモジュールと資格情報収集 Malware である“Strela Stealer”の変形が含まれていました。キャンペーンは盗まれた合法的なメールを再利用し、元のファイル名を保持しながら添付ファイルを SVG 形式に変更しました。メールは SPF 検査を通過して信頼性を高めました。6 月 4 日から 6 月 19 日までの初期波は、悪性ドメインの迅速な閉鎖によりすぐに影響を失いました。しかし、7 月 3 日に開始された後続キャンペーンはドメイン使用を拡大し、潜在的な影響を増加させました。該当 Malware はレジストリベースの持続性メカニズムを確立し、実行環境がサンドボックスかどうかを検査した後、Strela Stealer を配布しました。これらの展開は、伝統的な資格情報窃取技法を超えた技術的進化と能力向上を示唆しています。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. ドイツ目標にフィッシングメール使用
2. [Execution] User Execution (T1204)
   a. SVG ファイルを通じた Malware ダウンロード
   b. HTML 埋め込みを通じた ZIP ファイル実行
3. [Persistence] Registry Run Keys / Startup Folder (T1547.001)
   a. レジストリアクセス持続性確保
   b. StarFish リバースシェル持続性確保
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. JavaScript ファイル難読化
   b. ポリグロットファイルおよびコード署名証明書使用
5. [Credential Access] Credential Dumping (T1003)
   a. Strela Stealer を通じたメール資格情報収集
   b. PowerShell 基盤資格情報窃取
6. [Command and Control] Application Layer Protocol (T1071)
   a. C2 サーバーと HTTP 通信

b. コマンド実行後結果報告

7. [Collection] Screen Capture (T1113)
   a. スクリーンショットモジュールを通じた画面キャプチャ
   b. キャプチャされた画像ファイルホスティングサイトアップロード
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 資格情報ファイル C2 サーバーへ送信
   b. curl コマンドを通じたデータ流出

5) SectorJ250 used RaaS Network to Encrypt VMware ESXi Environments (2025-09-22)

https://cti.nshc.net/events/view/18685

攻撃対象産業群: 銀行, 投資, 製造, 通信, エネルギー, 小売, 保険, 観光・宿泊, 自動車

攻撃者は AI 基盤の音声フィッシング(vishing)と供給網システムを損傷し、小売、航空、通信などの複数分野の企業ネットワークに無断でアクセスしました。彼らは Git バージョン管理、BrowserStack、クラウドプロジェクト管理プラットフォームなどで高権限エンジニアリングアカウントを標的にし、CI/CD パイプラインに侵入して供給網攻撃を試みました。Malware 内部者が企業ネットワークに直接アクセスできるように支援しました。攻撃者は IT 職員を装い、Salesforce アプリケーションを損傷し、顧客データを奪取して最大 7 桁の金額を要求する脅迫を行いました。また、VMware ESXi 環境を対象とするサービス型ランサムウェア(Ransomware as a Service, RaaS)ネットワークを構築し、脅迫手段と影響力を拡大しようとする動きを見せました。これらの活動は AI 基盤の音声エージェントを活用した高度な社会工学的手法とソフトウェア供給網の悪用を核心戦略としていることを示しています。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Voice (T1566.004)
   a. 音声フィッシングを通じたユーザー認証情報の脱取
2. [Execution] User Execution: Malicious Link (T1204.001)
   a. 悪性リンクを通じたユーザー実行誘導
3. [Persistence] Create Account: Cloud Account (T1136.003)
   a. クラウドアカウント生成による持続性確保
4. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
   a. 権限昇格のための脆弱性悪用
   b. 高権限ユーザーアカウントアクセス
5. [Defense Evasion] Multi-Factor Authentication Interception (T1111)
   a. 多要素認証回避

b. ユーザー認証情報の傍受

6. [Credential Access] Steal Application Access Token (T1528)
   a. アプリケーションアクセス トークンの脱取
   b. セッションクッキーの脱取
7. [Discovery] Cloud Service Discovery (T1526)
   a. クラウドサービス探索
8. [Lateral Movement] Exploitation of Remote Services (T1210)
   a. リモートサービスの脆弱性を悪用した内部ネットワーク側面移動
9. [Collection] Data from Information Repositories (T1213)
   a. 情報リポジトリからのデータ収集
   b. Salesforce ダッシュボードからのデータ脱取
10. [Exfiltration] Exfiltration to Cloud Storage (T1567.002)
    a. クラウドストレージへのデータ流出
    b. 顧客データの外部送信
11. [Impact] Data Encrypted for Impact (T1486)
    a. ランサムウェアによるデータ暗号化

6) SectorJ251 used BlotchyQuasar disguised as Colombia Gov Emails (2025-10-01)

https://cti.nshc.net/events/view/19307

2024 年 1 月、サイバー攻撃イベントがコロンビア政府機関である Migración Colombia とコロンビア司法府を装った詐欺性メールキャンペーンとして発生した。このメールは PDF 添付ファイルを含み、受信者に暗号化された.LHA アーカイブをダウンロードするよう誘導した。添付ファイルを開くと、一連の実行プロセスが開始され、“BlotchyQuasar”バンキングトロイの木馬が配布された。この攻撃ベクターは一見合法的な文書を通じて実行され、悪意のあるファイルを隠してユーザーが知らないうちにシステムで Malware を実行させた。主要な目的はシステム侵入を通じた不正アクセスとデータ窃取であり、特に金融に関連する資格情報の収集に焦点が当てられていると分析される。この事件は政府機関を装った巧妙な社会工学技術の例を示し、公式機関に対する信頼を悪用して Malware を拡散する持続的な脅威を強調している。

[図 8: SectorJ251 グループが活用したフィッシング文書]

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 이메일캠페인
   b. 政府機関詐称
2. [Execution] User Execution (T1204)
   a. PDF 添付ファイルを開く
   b. ファイル内埋め込みリンク実行
3. [Credential Access] Credential Dumping (T1003)
   a. 銀行資格証明収集
   b. 不正アクセス試行
4. [Command and Control] Encrypted Channel (T1573)
   a. 暗号化された通信チャネル使用
   b. リモート制御およびデータ窃取

7) SectorJ252 used BadIIS Malware disguised as SEO Tools (2025-10-02)

https://cti.nshc.net/events/view/19313

攻撃対象産業群: 通信、技術、学界 - 大学

中国語を使用するサイバー犯罪グループがインド、タイ、ベトナム、カナダ、ブラジルの高価値 IIS サーバーを対象に検索エンジン最適化(SEO)詐欺と資格証明窃取を実行した。該当グループは大学、技術企業、通信提供業者のような組織を対象に検索結果の露出を悪意的に操作しデータを窃取し、脆弱性を利用して web shell をアップロードし偵察を行い、追加悪用のために Remote Desktop Protocol (RDP)アクセスを有効化した。該当グループは持続性を維持するために RDP と SoftEther VPN、EasyTier のような分散 VPN ツール、FRP リバースプロキシを組み合わせて活用した。また、BadIIS Malware を配布し権限昇格のために公開されたツールを使用し、彼らの拠点を確保するための防御メカニズムを使用した。彼らは Cobalt Strike をバックドアとして使用し DLL サイドローディングを通じて持続性を維持し、オートメーションスクリプトを利用してログ、資格証明、証明書など高価値データを収集した。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. 웹サーバーのファイルアップロード機能の弱点を利用
   b. Web シェルをアップロードして初期アクセス権限を獲得
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. システム情報収集のためのコマンド実行
   b. ネットワーク情報の探索および収集
3. [Persistence] Create Account (T1136)
   a. ゲストアカウントを有効化し、管理者権限で権限昇格
   b. 隠しアカウントを作成し、Administrator 権限を付与
4. [Persistence] External Remote Services (T1133)
   a. RDP を通じたリモートアクセス設定
   b. SoftEther VPN, EasyTier, FRP を通じた持続的アクセス維持
5. [Privilege Escalation] Shared Public Tools (T1088)
   a. 共有ツールを活用してシステム権限を獲得
   b. Procdump を使用して資格情報を抽出
6. [Defense Evasion] Virtualization/Sandbox Evasion (T1497)
   a. BadIIS Malware のコード構造変更
   b. 検出を避けるための高度な回避戦術使用
7. [Collection] Archive Collected Data (T1560)
   a. WinRAR を使用して収集されたデータを圧縮
   b. 証明書、ログ、資格情報などの高価値データ収集
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. C2 サーバーを通じたデータ外部送信
   b. 収集されたデータを隠しディレクトリに保存後送信

9. [Command and Control] Application Layer Protocol (T1071)
   a. Cobalt Strike を通じたバックドアインストール
   b. DLL サイドローディングを通じた持続的な制御維持

8) SectorJ253 exploited GoAnywhere MFT vulnerability CVE-2025-10035 (2025-10-06)

https://cti.nshc.net/events/view/19310

攻撃者は 2025 年 9 月 18 日、GoAnywhere MFT の License Servlet で発見された致命的な逆シリアル化脆弱性(CVE-2025-10035)を利用しました。この脆弱性は、偽造されたライセンス応答署名を通じて任意のオブジェクトを逆シリアル化できるようにし、コマンドインジェクションおよびリモートコード実行(RCE)を引き起こしました。この脆弱性を利用するサイバー犯罪グループは Medusa ランサムウェアを使用することで知られています。攻撃者は有効なライセンス応答を作成または傍受できる場合、認証なしで脆弱性を悪用することができました。この脆弱性は特にインターネットに露出したインスタンスに脅威となり、攻撃者が長期的なアクセス権を得てマルウェアツールを配布することを可能にしました。攻撃者は持続性を確保するために SimpleHelp および MeshAgent のような RMM ツールを使用し、Cloudflare トンネルを設定して安全な C2 通信を構築しました。データ漏洩段階では Rclone が使用され、少なくとも 1 つの事例で Medusa ランサムウェアが最終的に配布される活動が確認されました。攻撃は多段階戦術を特徴としており、ゼロデイ脆弱性を悪用してアクセス権を取得し、RMM ツールを活用してシステム探索および横方向移動を実行しました。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. GoAnywhere MFT のライセンスサービス逆シリアル化脆弱性悪用
   b. 偽造されたライセンス応答署名の作成および使用
2. [Persistence] Implant: Remote Access Tool (T1105)
   a. RMM ツール SimpleHelp および MeshAgent のインストールおよび運用
   b. GoAnywhere MFT ディレクトリに.jsp ファイル生成
3. [Discovery] System Network Configuration Discovery (T1016)
   a. ユーザーおよびシステム情報収集コマンド実行
   b. ネットワーク探索ツール netscan 配布
4. [Lateral Movement] Remote Services (T1021)
   a. “mstsc.exe”を利用したシステム間移動
   b. 内部ネットワークでの側面移動
5. [Command and Control] Encrypted Channel (T1573)
   a. RMM ツールを通じた C2 インフラ構築

b. Cloudflare トンネル設定による安全な C2 通信
6. [Exfiltration] Automated Exfiltration (T1020)
a. Rclone を使用したデータ流出
7. [Impact] Data Encrypted for Impact (T1486)
a. Medusa ランサムウェア配布および実行
b. ランサムウェアを通じたデータ暗号化

9) SectorJ254 used Go Bot Malware disguised as Job Description PDF (2025-09-25)
https://cti.nshc.net/events/view/19197

ベトナムの脅威グループは、求職者とデジタルマーケティングの専門家を対象としたキャンペーンを実施しました。この作戦は、社会工学の戦術を利用して Malware を職務説明書に偽装したファイルを通じて配布しました。これらのファイルは主に PDF に偽装した悪性 LNK ファイルが含まれた ZIP アーカイブを通じて配信されました。実行時に、PowerShell スクリプトが活性化され、追加の Malware をダウンロードしました。主要な Malware 構成要素は、システム監視とデータ窃取のために設計された Go ベースのボット"Vampire"でした。このボットは、サーバーに AES 暗号化されたビーコンを送信して C2 通信を確立しました。継続的にデスクトップのスクリーンショットを WEBP 画像としてキャプチャし、HTTPS を通じて送信して検出を回避しました。脅威行為者は、合法的なリモートアクセスソフトウェアを使用して感染したシステムを制御しました。C2 インフラは、合法的な企業を模倣したドメインを使用することで知られるベトナムの脅威行為者に追跡されました。このキャンペーンは、クロスプラットフォームの活用性と高度な回避技術を備えた Go バイナリを使用して精巧さを示しました。

[Attack Flow]
1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
a. 求職者対象のメール送信
b. ZIP ファイル添付
2. [Execution] User Execution: Malicious File (T1204.002)
a. PDF に偽装された LNK ファイル実行
b. 悪性 PowerShell スクリプト活性化
3. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
a. 追加悪性コードダウンロード
b. XtraViewer 実行
4. [Defense Evasion] Masquerading: Match Legitimate Name or Location (T1036.005)
a. ファイル名に空白追加
b. システムおよび隠し属性設定

5. [Collection] Screen Capture (T1113)
   a. デスクトップスクリーンショットキャプチャ
   b. WEBP イメージとして保存
6. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. AES 暗号化されたデータ送信
   b. HTTPS を通じた C2 サーバー通信
7. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. データ脱取
   b. TLS 暗号化チャネル使用

10) SectorJ255 used MonsterV2 RAT with IRS-themed phishing lure (2025-10-13)

https://cti.nshc.net/events/view/19426

攻撃対象産業群: 金融、会計

攻撃者は最近、高度化されたサイバー犯罪活動を独立して実行しました。この攻撃者はサイバー犯罪環境内で革新性を示し、2025 年 2 月から観察された MonsterV2 という Malware を頻繁に配布しました。MonsterV2 は地下フォーラムで販売され、リモートアクセス型トロイの木馬、情報窃取型 Malware およびローダーとして機能し、独立国家共同体(CIS)内のシステムを回避しながら、機密データを列挙し流出させる能力があると知られています。初期キャンペーンでは IRS をテーマにした餌メッセージを使用し、ClickFix という手法を活用して悪性 PowerShell コマンドを実行し、最終的に MonsterV2 をインストールしました。攻撃者は JavaScript 注入を通じたウェブインジェクションキャンペーンを管理し、CAPTCHA 検証に偽装した悪性行為を誘導して PowerShell スクリプトを通じて Malware を実行しました。別の戦術としては、GitHub 通知を利用してユーザーをセキュリティ警告を模倣した攻撃者が制御するサイトに誘導しました。MonsterV2 に加えて、これらのキャンペーンは Rhadamanthys という別の Malware 変種を配布しました。SonicCrypt は MonsterV2 をパッキングするために使用されたクリプターで、検出回避技術を含み、タスクスケジューラーを通じてペイロードを実行し、隠密なプロファイルを維持しました。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. IRS テーマのメール送信
   b. GitHub 通知に偽装したフィッシングコンテンツの活用
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. ClickFix 技法を通じた PowerShell コマンドの実行
   b. CAPTCHA に偽装したスクリプトを通じた PowerShell の実行
3. [Defense Evasion] Obfuscated Files or Information (T1027)

a. SonicCrypt クリプターの使用
b. コード難読化技法の適用
4. [Credential Access] Input Capture (T1056)
a. 情報の窃取および流出機能
b. クリップボードデータの改ざん
5. [Command and Control] Application Layer Protocol (T1071)
a. C2 サーバーとの暗号化通信
b. 多様なコマンドの受信および実行
6. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. 敏感データの外部送信
b. システム情報の収集および送信

11) SectorJ256 used Sorillus RAT via Invoice-themed Phishing (2025-10-16)
https://cti.nshc.net/events/view/19493

サイバー脅威グループは 2025 年 7 月から 10 月の間に Sorillus リモートアクセス型トロイの木馬(RAT)を配信するキャンペーンを実施した。彼らは以前の作戦と類似した戦術を使用した。2025 年 5 月と 6 月にはスペイン、イタリア、ポルトガルの個人をメールおよびフィッシングキャンペーンを通じて標的にし、RATty と Sorillus マルウェアを配布した。グループの技術には、メールキャンペーンと請求書テーマのフィッシング手法を活用してヨーロッパ全域にマルウェアを拡散することが含まれる。これらのキャンペーンは一貫した戦術、技法、手順パターンを明らかにし、このサイバー行為者の徹底した努力を示している。グループの起源はブラジルと推定され、これは攻撃で観察されたインフラと方法でさらに証明される。彼らの攻撃戦略は、メールおよびフィッシングベクターを活用して目標を達成する方向に進化している。

[Attack Flow]
1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
a. 송장테마피싱메일 送信
2. [Execution] User Execution (T1204)
a. 悪性ファイルダウンロード
b. 添付ファイル実行
3. [Persistence] Registry Run Keys / Startup Folder (T1547)
a. レジストリキー生成
b. スタートアップフォルダに Malware 追加
4. [Command and Control] Application Layer Protocol (T1071)
a. C2 サーバーと通信

b. HTTP プロトコル使用

5. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 敏感データ送信
   b. C2 チャネル活用
6. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. コード難読化
   b. ファイル暗号化使用

12) SectorJ258 used AWS IAM Weaknesses for Data Exfiltration and Extortion (2025-10-08)

https://cti.nshc.net/events/view/19283

新たに登場したサイバー脅威グループが AWS クラウド環境を標的にデータ脱取および脅迫を活発に行った。最近数週間、このグループは GitLab の非公開リポジトリ脱取を含む攻撃を敢行した。攻撃者は「TruffleHog」ツールを使用して流出した AWS 長期アクセスキーを検索し、初期アクセスを試みた。アクセスに成功した後、AWS API 呼び出しを通じて新しいユーザーを生成し、AdministratorAccess ポリシーを付与して権限を昇格させた。彼らの主要な目標は、データベース、プロジェクトリポジトリおよびその他の重要データを収集することである。攻撃者は EC2 インスタンス、VPC、RDS、EBS ボリューム、そして SMS および SES 割り当てを含むクラウドインフラを詳細に評価するために AWS API 呼び出しを活用した。データ収集はデータベースマスターパスワードの修正および EBS ボリュームとデータベースのスナップショット生成を通じて実行された。脱取は損傷した資格情報を使用して行われ、AWS S3 サービスと過度に許可されたセキュリティグループを広範に活用した。データ脱取に成功すると、AWS SES(Simple Email Service)を活用して脅迫メッセージを送った。複数の IP アドレスの使用と過度に許可された IAM 構成は、精巧なアプローチを示唆している。

[Attack Flow]

1. [Initial Access] Valid Accounts: Cloud Accounts (T1078.004)
   a. TruffleHog ツールを使用して流出した AWS 資格情報を検索する
   b. 長期アクセスキーを通じて初期アクセス試行
2. [Persistence] Create Account: Cloud Account (T1136.003)
   a. AWS API 呼び出しを通じて新しいユーザー生成
   b. CreateLoginProfile API でユーザーにログインプロファイル生成
3. [Privilege Escalation] Privilege Escalation (T1068)
   a. AttachUserPolicy API で AdministratorAccess ポリシー付与
   b. SimulatePrincipalPolicy API でポリシーシミュレーション実行

4. [Discovery] Cloud Storage Object Discovery (T1619)
   a. EC2, VPC, RDS, EBS ボリュームなどクラウドインフラ詳細情報収集
5. [Collection] Data Staged: Remote Data Staging (T1074.002)
   a. RDS インスタンスのマスターパスワード修正
   b. EBS ボリュームおよびデータベーススナップショット生成
6. [Exfiltration] Exfiltration Over Web Service (T1567.002)
   a. GetObject API で S3 バケットからデータ脱取
   b. 過度に許可されたセキュリティグループを通じたデータ転送
7. [Impact] Data Manipulation (T1565)
   a. AWS Simple Email Service を通じた脅迫メッセージ送信
   b. 被害者に脱取されたデータの範囲通知

今月のサイバー脅威の特徴

今回報告された事例は、Windows・macOS・Linux を包括するクロスプラットフォーム戦術を繰り返し活用し、合法ソフトウェアアップデート・偽ドライバー・採用関連ソーシャルエンジニアリングなどを初期アクセスベクターとして悪用し、ターゲット内部への侵入を試みる特徴を示している。これらの偽装手法は、ターゲット化されたサプライチェーン侵入と合法サービス偽装を結合し、組織エコシステム全体に攻撃効果を拡散させようとする戦略的意図を明らかにしている。
また、情報窃取型 Malware の機能統合と資格情報再利用の自動化が目立っています。ブラウザクレデンシャル・暗号通貨ウォレット・2 次認証トークンなど、さまざまな資産を同時に収集する統合型スティーラーが報告されており、窃取情報の自動検証および再利用を通じた初期アクセス拡張の自動化が確認されています。これにより、アカウント盗用後の側面移動および権限昇格につながる伝播速度が加速化する傾向が観察されています。
攻撃インフラの側面では、C2・配布インフラのモジュール化および再利用が顕著である。脅威行為者は、無料ホスティング、クラウドストレージ、正常サービスの認証・API を通信チャネルやペイロード配信経路として悪用することで、検出回避と迅速なインフラ再構築を可能にしている。これと並行して、多重冗長 C2、エンコードされた通信プロトコル、暗号化されたペイロードの多段階復号ルーチンが広範囲に使用され、既存のシグネチャベースの検出の有用性を低下させている。
ランサムウェアおよび金銭的動機に基づく活動は、データ流出とダブルエクストーション戦略が一般化しており、中小のサプライチェーンノードの脆弱性を悪用した下流への侵入が頻発している。この過程では、マルウェアの難読化、プロセスインジェクション、タスクスケジューラを活用した持続性確保といった従来の手法に加え、DLL サイドローディングやコード署名の悪用などコンポーネントレベルの高度な回避手法が組み合わされている。

特に注目すべき点は、生成型 AI・LLM を攻撃補助ツールとして活用することである。攻撃者は LLM を利用してスピアフィッシングコンテンツを自動生成したり、餌文書の自然さを高めるために自動翻訳・文脈補正に AI を適用した状況が捕捉されている。AI ツールの活用は、社会工学の精巧さを加速し、ターゲット別のカスタマイズされた誘引でフィッシング成功率を高める一方、フィッシングキャンペーン設計・ソースコード難読化・インフラ転換を自動化することに寄与する。これにより、検出・分析・対応体制は言語的・文脈的信号の検証能力を強化する必要性が増大している。
総合すると、今月の脅威地形は量的拡大よりも精密化、自動化、インフラ共有化が核心軸として機能しています。脅威行為者は既存技法を結合・モジュール化して検知回避と拡散効率を向上させ、AI とクラウド基盤サービスの悪用は今後、社会工学基盤侵入脅威の強度をさらに増大させると判断されます。したがって、CTI 観点では IOC・TTP 基盤相関分析を高度化し、クロスプラットフォーム行為者の共通モジュール・インフラを迅速に識別する脅威ハンティングおよびインテリジェンス共有体制の強化が求められます。

今月のサイバー脅威の示唆点

最近、多数のサイバー脅威活動分析結果、攻撃者たちが Windows、macOS、Linux など多重プラットフォームを同時対象とする精巧化された攻撃戦術を積極的に活用することが確認された。特に 10 月には正常ソフトウェアアップデートに偽装したり、正常文書・インストールファイルに悪性スクリプトを挿入する方式が多数観察され、ブラウザクレデンシャル・暗号通貨ウォレット・2 次認証トークンなど敏感資産を同時収集する統合型スティーラーの使用が目立った。これらの攻撃は単一脆弱性(CVE)悪用よりも社会工学基盤の初期浸透に集中しており、偽の採用手続きや偽装されたプロジェクトファイルを通じて開発者・技術従事者を直接標的とする形態が繰り返された。攻撃者は BeaverTail、OtterCookie、OtterCandy など情報窃取型 Malware を結合して持続的な感染体系を構成し、Socket.IO、WebSocket、PowerShell など正常プロトコルを悪用した暗号化された通信で検出を回避した。さらに暗号化されたペイロード及び多段階復号ルーチンを通じて分析難易度を高め、多重 C2 インフラを活用した分散命令遂行構造を維持することで長期的システム掌握を試みた。
セキュリティ戦略の観点から、組織はこれらの複合的な脅威に対応するために多層防御システムを強化する必要があります。第一に、定期的な脆弱性スキャニングとパッチ管理を通じて、既知の脆弱性の露出を最小化する必要があります。第二に、スピアフィッシング・ソーシャルエンジニアリングへの対応のためにセキュリティ意識教育を定例化し、ユーザーアカウントアクセスに対する多要素認証(MFA) を義務化する必要があります。第三に、EDR および NIDS を通じて行動ベースの検出を強化し、C2 通信や異常なネットワークトラフィックをリアルタイムで遮断できる環境を整える必要があります。第四に、データ暗号化および最小権限の原則 (PoLP) に基づく RBAC ポリシーを再検討し、不要なアクセス権を削除する必要があります。また、クラウドおよびコラボレーションツール環境で

の資産インベントリ管理システムを改善し、ログ相関分析を通じて異常な認証・アクセスイベントを早期に検出するシステムを整える必要があります。

今月の脅威パターンで特に注目すべき点は、攻撃インフラのモジュール化と再利用です。脅威行為者は、無料ホスティングサービス、クラウドストレージ、API 認証機能を通信チャネルやペイロード配信経路として悪用し、検出回避とインフラ再構築を容易にしています。これと並行して、Base64 エンコーディング、RC4 暗号化、ファイル保護アーカイブなどの古典的な回避技法が依然として広範囲に活用されており、DLL サイドローディングとコード署名の濫用も頻繁に観察されます。特に攻撃者は組織のサプライチェーンを標的にしてトップダウンの侵入を行い、これを通じて主要機関や技術企業の内部ネットワークに拡散します。このような流れは、技術的脆弱性だけでなく人的要因までをも網羅する多次元防御アプローチの重要性を示唆しています。

一方、AI ベースのツール の導入は攻撃者の社会工学技術を精密化する要因として作用している。生成형 AI はフィッシングメッセージの言語的精巧化、カスタマイズされた餌コンテンツの制作、インフラ自動転換など攻撃の効率性と隠密性を同時に向上させるために活用されている。したがって CTI 観点から組織は IOC・TTP 기반相関関係分析を高度化し、脅威行為者間の共通インフラおよびコードを早期に識別できる脅威ハンティング能力を確保しなければならない。また、外部脅威インテリジェンスフィードを積極的に受容し、最新攻撃手法とインフラパターンを常時モニタリングすることによって潜在脅威を早期に遮断できるようにしなければならない。このような総合的アプローチは組織のセキュリティ態勢を強化し、デジタル資産保護とサイバー環境の安定性を維持する核心基盤となる。

Recommendation

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

1. 脆弱性保護 (Exploit Protection)

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

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

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

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

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

3. セキュリティ認識教育 (User Training)

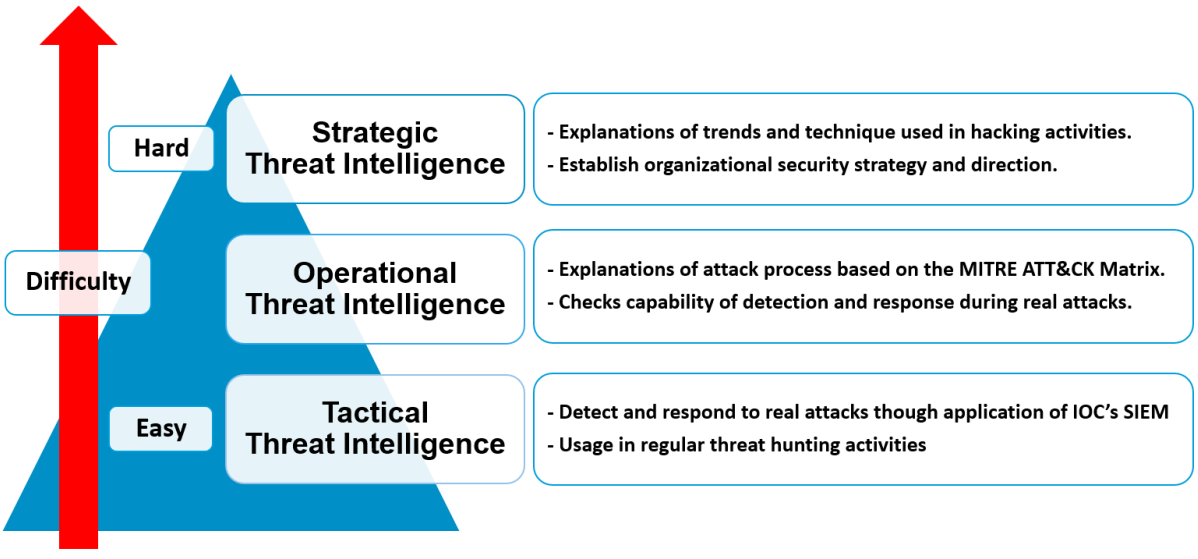
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

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

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

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

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



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

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

5. ネットワークにおける脅威緩和

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

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

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

2) ネットワーク細分化 (Network Segmentation)

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

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

6. ユーザーアカウントの脅威緩和

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

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

2) アカウント使用政策 (Account Use Policies)

アカウントのセキュリティ設定に関した政策設定の検討が必要

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

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

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

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

7. エンドポイントの脅威緩和

1) ソフトウェアアップデート(Update Software)

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

2) OSの構成 (Operating System Configuration)

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

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

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

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

4) 実行防止 (Execution Prevention)

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

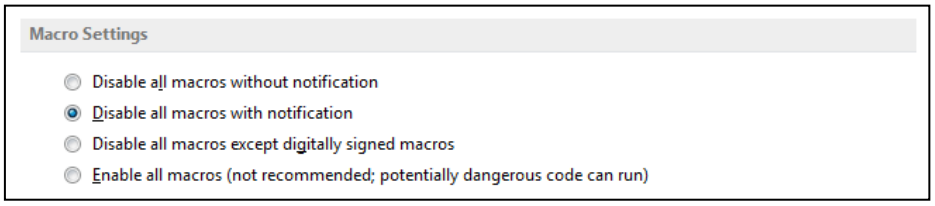
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

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

Program)

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

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



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

6) コード署名 (Code Signing)

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

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

7) アンチウイルス (Antivirus)

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

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

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

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

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

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

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

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

10) 企業モバイル政策 (Enterprise Policy)

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

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

LEGAL DISCLAIMER

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

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

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

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

NSHC.

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