NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI2026011402

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

Dec 2025

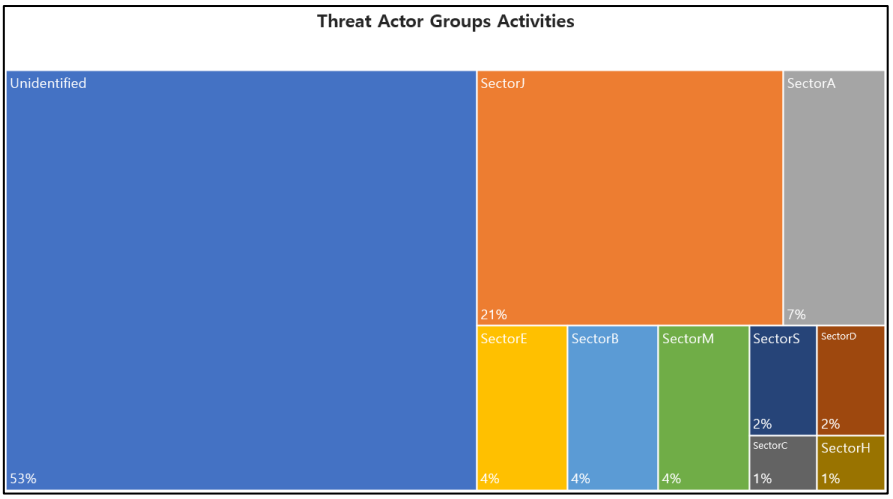
NSHC PTE. LTD.

このレポートは 2025 年 11 月 21 日から 2025 年 12 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

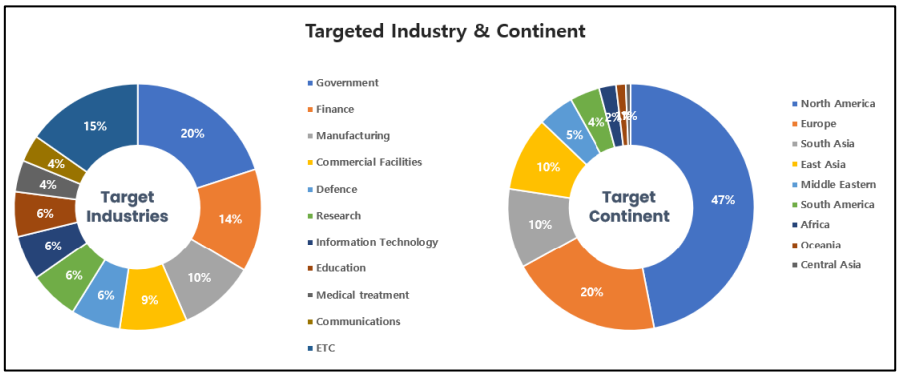
Executive Summary

2025 年 11 月 21 日から 2025 年 12 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 Threat Actor Group の活動を要約整理した内容である。
2025 年 12 月に確認されたハッキンググループの活動は合計 99 件であり、そのうち未識別(Unidentified)グループが 53%を占め、SectorJ および SectorA グループの活動がこれに続いた。



[図 1: 2025 年 12 月に確認されたハッキンググループ別活動統計]

今回 12 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る。



[図 2: 2025 年 12 月攻撃対象となった産業分野と国家統計]

SectorA グループに関連するハッキング活動は、金融、技術、政府など複数の部門を対象とし、高度な戦術・技術・手順(TTP)を用いた多面的なサイバー犯罪活動として確認されている。このグループ

の作戦は、カスタム Malware、社会工学、戦略的インフラを活用して目標を達成する高いレベルの技術的能力を明らかにしている。当該作戦では、資格情報の窃取およびリモートアクセスを目的とした LummaC2 や OtterCookie といった情報窃取型マルウェアの使用が確認されている。これらのツールはしばしば VM 検出、難読化、GitHub および Dropbox のような合法的なサービスを使用して Malware 活動を正常なネットワークトラフィックと混合する高度な回避技術を使用する。このグループのキャンペーンはしばしば WinRAR 脆弱性のようなソフトウェア脆弱性の悪用を含み、暗号通貨ウォレットおよびブラウザ資格情報のような敏感なユーザーデータを対象とするペイロードを配信する。フィッシングと社会工学の使用が一般的であり、偽の求人インタビューから税務当局のなりすましに至るまで戦術を多様に使用して目標システムにアクセスするために人間の行動を操作する能力を示している。SectorA グループはまた、Malware パッケージで npm エコシステムに侵入し、ソフトウェアサプライチェーンへの関心を示し、開発者ネットワークをより広く悪用できる能力を強調している。彼らのインフラは、コマンドおよびコントロール(C2)サーバー、VPN、Slack および Dropbox のような通信プラットフォームを使用して調整およびデータ漏洩のための強力なインフラを活用している。このグループの作戦は、内部調整およびインフラ共有の証拠とともに高いレベルの組織化を示しており、共有開発リポジトリおよび C2 サーバーの使用で見ることができる。彼らの技術的精巧さにもかかわらず、グループは時折、制御されたモニタリング環境を通じて明らかにされた通信断絶およびインフラ共有のような脆弱性を明らかにする。全体として、SectorA グループの活動は、複数のドメインにわたって複雑な攻撃を実行しながらサイバー脅威環境で持続的な存在を維持できるよく組織され技術的に熟練したサイバー犯罪作戦を反映している。

SectorB グループは、多様なマルウェアおよび高度な戦術、技術、手順(TTP)を特徴とする洗練された適応的なサイバー作戦アプローチを示している。彼らの作戦は、データ盗難およびペイロードステージングのために Google Drive API を活用する WMLOADER および NANOREMOTE のような複雑なマルウェアの配布で特徴付けられる。これらは AES-CBC 暗号化および Zlib 圧縮を使用して C2 通信を難読化する。このグループは IIS および SharePoint サーバーの既知の脆弱性を活用して初期アクセスを設定し、ShadowPad のようなカスタムモジュールを使用して侵害されたサーバーを彼らの C2 インフラに統合する高い技術的能力を示している。彼らのマルウェアはしばしば合法的なプロセスに偽装され、検出回避と持続性のために設計された FinalDraft の変種を含む。SectorB グループのキャンペーンは、広範な側面移動、資格情報収集、権限昇格を特徴とし、LSASS ダンピングおよびアイドル RDP セッションの悪用のような技術を活用する。VMware プラットフォームでの BRICKSTORM マルウェアの使用は、長期的な持続性と洗練された回避のための彼らの能力をさらに強調し、複数の暗号化レイヤーおよび SOCKS プロキシを使用して側面移動を行う。彼らの作戦はしばしば Microsoft Azure および Google Drive のようなクラウドサービスを C2 に使用し、MFA 操作および高度なトンネリング技術を含むクラウド意識戦略を強調する。SectorB グループの適応および進化能力は、Discord API のようなオープンソースツールを C2 に使用して検出を回避するために合法的なユーザー活動を模倣するトラフィックパターンを生成することでも明らかである。彼らのキャンペーンは主に C#/.NET アプリケーションを活用し、グループポリシーを通じてマルウェア配布お

よび側面移動を行うカスタムツールの使用を含む。このグループの適応能力は、サプライチェーン攻撃およびフィッシングキャンペーンの戦略的使用、洗練された難読化技術の活用、マルウェア配布のための合法的なクラウドサービスの活用を通じてさらに証明される。全体として、SectorB グループの作戦は成熟したモジュラーサイバースパイ活動アプローチを反映し、高度な回避、持続性技術および高いレベルの運用を示している。

SectorC グループは 2021 年から 2025 年にかけて、複数のキャンペーンを通じ、多様な戦術・技術・手順(TTP)を用いた持続的かつ高度なサイバー作戦を展開している。彼らの作戦は一貫して重要なインフラ、政府機関、戦略的部門を対象としており、資格情報収集およびソフトウェア脆弱性の悪用を活用しています。彼らの代表的な戦略の一つは、偽のログインポータルおよびスピアフィッシングメールを活用してユーザー資格情報や二要素認証コードまで捕捉するフィッシングキャンペーンの使用です。彼らはインフラ戦術を変更して適応性を示し、検知および法執行介入にもかかわらず持続性を維持するために、損傷したルーターから ngrok トンネルに移行します。このグループはまた、ルーターおよび VPN 集線装置のような誤って構成されたネットワークデバイスを悪用して初期アクセスを得て、被害者ネットワーク内で側面移動を行います。これらのアプローチは持続可能なアクセスおよび作戦の深さに重点を置き、最小限の露出で体系的な資格情報再生攻撃を実行できるようにします。彼らのキャンペーンは、さまざまなプログラミング言語で書かれたインプラントを含む精巧な Malware の使用で特徴付けられ、リモートシェルアクセスを提供し、データ漏洩を実行します。

SectorC グループはまた、WinRAR の CVE-2025-8088 を使用してウクライナ政府部門を対象としたスピアフィッシング攻撃を実行するなど、ソフトウェア脆弱性を悪用する卓越した能力を示しました。これはディレクトリトラバーサル欠陥を通じて悪性ペイロードを配布し、開始ディレクトリおよび予約されたタスクを通じた持続的感染につながりました。Base64 エンコーディングおよび文字置換のような複雑な難読化技術の使用は、検知をさらに複雑にします。伝統的なフィッシング方法に加えて、SectorC グループは OAuth およびデバイスコード認証の悪用を使用して偽のウェブサイトを作成し、国際セキュリティイベントを模倣して被害者が OAuth トークンを共有するよう誘導する革新を示しました。これは進化するセキュリティ環境に適応し、社会工学戦術を活用してメッセージングアプリを通じた関係構築を通じてフィッシング努力を強化する能力を反映しています。彼らのキャンペーン全体にわたり、SectorC グループは多層的持続性戦略、弾力的なコマンドおよびコントロール通信、複雑な暗号化技術を一貫して使用して隠密な作戦を保証します。Telegram および Discord のような公共プラットフォームを C2 通信に使用することは、検知を回避するために合法的なネットワークトラフィックを悪用する戦略的転換を強調します。全体として、SectorC グループの作戦は多様な目標および地域にわたり、検知回避、持続性および作戦の柔軟性に重点を置いたよく資源化され熟練した脅威行為者を明らかにします。

SectorD グループは、高度な技術能力と細心の計画で特徴づけられる非常に精巧で組織的なサイバー作戦アプローチを示している。彼らの活動は、カスタム Malware の配布とスパイ活動および破壊目標を達成するための脆弱性悪用で特徴づけられる。このグループは、リモートコントロール、データ漏洩、資格情報盗難といった特定の機能のためにカスタマイズされた UDPGangster、MuddyViper

、Foudre、Tonnerre を含む様々な Malware を使用する。例えば、UDPGangster はマクロが含まれた Word 文書を使用するフィッシングメールを通じて配信され、侵害されたシステムでのリモートアクセスと持続性を可能にする。この Malware は、デバッガーおよび仮想マシンに対する環境検査を含む分析回避技術を使用して検出を回避する。同様に、MuddyViper は Fooder ローダーを通じて実行され、検出回避のためにカスタム遅延機能を使用する。SectorD グループのキャンペーンは、データ保護のための CNG 使用といった精巧な暗号化方法をしばしば含み、コマンド＆コントロール作戦のために Amazon および DigitalOcean といったプラットフォームにホスティングされたインフラを活用する。彼らの作戦は、公式化されたワークフローを持つよく構造化されたサイバーユニットによって支援され、Exchange 脆弱性悪用および長期情報収集に重点を置く。このグループのインフラは、調達および作戦物流を詳細に説明するスプレッドシートで細心に文書化されており、暗号化を使用して慎重に資金を調達する。彼らのドメイン生成アルゴリズムおよび Telegram ボット API を通じた C2 リダイレクションを含む高度な C2 技術への依存は、彼らの技術的能力および適応性を強調する。全体として、SectorD グループの活動は、機会主義的攻撃よりも情報収集および長期持続性に重点を置いた高いレベルの運用および戦略的計画を反映している。

SectorE グループは主にアジア地域を対象にしており、サービス、小売、通信、医療といった部門に焦点を当てた洗練された進化するサイバースパイ活動アプローチを示している。このグループの活動は、StreamSpy トロイの木馬およびその他の洗練されたツールの配布に見られるように、高度な Malware および回避技術の使用によって特徴付けられる。StreamSpy は PDF 文書に偽装した ZIP ファイルのような餌ファイルを通じて配布され、WebSocket および HTTP のような複雑な通信プロトコルを使用して彼らのコマンドおよびコントロール(C2)インフラと隠密な接続を維持する。このインフラは特に"www.mydropboxbackup[.]com"と関連しており、認証目的で固有のデバイス識別子を生成するために使用される詳細なシステム情報を収集する。この Malware は、予約されたタスク、レジストリの修正、LNK ファイルの生成といった様々な方法を通じて持続性を保証し、侵害されたシステムでの足場を維持する。このグループの合法的な Microsoft Defender バイナリを使用した DLL サイドローディング技術の使用は、検出をさらに複雑にし、評判ベースの防御を回避するための公共クラウドストレージおよび URL 短縮機の戦略的使用も同様である。Malware ペイロード実行のための合法的なバイナリの活用および特定のタイムゾーンのシステムをターゲットにするためのジオフェンシングの使用を通じて、SectorE グループは伝統的なセキュリティ対策を効果的に回避する。彼らの作戦は定期的なハートビート更新およびリモートコマンド実行およびファイル転送のためのエンコードされた WebSocket ストリームで特徴付けられ、脅威行為者間の高いレベルの洗練およびリソース共有を反映している。これらの戦術、技術、手順(TTP)の継続的な進化は、地域内の重要な部門に対する SectorE グループの継続的な脅威を強調している。

SectorH グループは特に Linux 基盤 BOSS 環境を対象とした精巧なサイバースパイ活動のアプローチを示した。彼らの攻撃方法論は、Malware .desktop ファイルを配信するスピアフィッシングメールで始まる。これらのファイルは合法的に見えるよう巧妙に偽装されているが、バックグラウンドで悪意のあるコマンドを実行し、ターゲット環境に溶け込むグループの能力を示している。

Malware .desktop ファイルは彼らの戦略の重要な構成要素であり、"lionsdenim[.]xyz"ドメインおよび"185.235.137[.]90" IP アドレスにホスティングされた専用の悪意のあるインフラから追加のペイロードをダウンロードする。このインフラは ELF バイナリおよびシェルスクリプトを取得するために重要であり、これはコマンドを実行し、侵害されたシステム内で持続性を確立するために使用される。.desktop ファイルの使用は特に注目に値し、これは Malware が合法的なシステムレベルの実行権限で動作し、スムーズなデータ流出を可能にする。SectorH グループの戦術には持続性のための systemd サービスの使用も含まれており、これは Linux システムに対する深い理解と重要なインフラへの長期的なアクセスを維持しようとする意志を示している。彼らのマルチプラットフォーム戦略はまた、ネイティブな運用環境を効果的に悪用できる適応力と技術的能力を強調している。 本キャンペーンを通じて、当該グループが高度な技術的能力を有し、国家連携が疑われる水準のサイバー活動を実行していることが確認されている。

SectorS グループは彼らのサイバー攻撃キャンペーンで技術的能力および適応性を強調する多層的戦略を使用して、精巧なアプローチを示した。このグループは初期ベクターとしてフィッシングメールを使用し、損傷したメールアカウントを悪用して彼らの悪性通信に信頼性を与える。これらのメールは法的通知として巧妙に偽装されており、Base64 でエンコードされた HTML ページが含まれた SVG イメージを使用して公式ポータルを模倣し、ユーザーの相互作用の可能性を高める。対象がこれらのポータルと相互作用すると、JavaScript および PowerShell コマンドを通じた複数段階の難読化解除に基づくファイルレス攻撃チェーンが開始される。攻撃の注目すべき側面は、Base64 でエンコードされたペイロードを隠すためにイメージファイルを使用することであり、これは.NET アセンブリである Caminho としてロードされ、マルウェアダウンローダーとして機能し、Discord でテキストファイルを検索して MSBuild.exe を使用したプロセスハロウィングを通じて実行される。攻撃チェーンの頂点は、キーロギングおよびディスクアクセスなどの機能を持つリモートアクセス型トロイの木馬である DCRAT の配布であり、検出を回避するために暗号化でさらに強化される。SectorS グループの Discord をペイロード配信に使用することと高度な難読化技術の使用は、彼らの作戦での検出回避と持続性への献身を強調する。このキャンペーンは各段階が伝統的なセキュリティ対策を回避し、目標システム内で足場を維持するために細心に設計された高いレベルの精巧さを反映している。Discord および MSBuild.exe のような一般的なツールおよびプラットフォームを活用するグループの焦点は、合法的なネットワークトラフィックと混合して検出可能性を減少させる戦略的アプローチを示している。全体として、SectorS グループの活動は、社会工学的手法と技術的手段を組み合わせ、検知回避を重視した計画的な攻撃活動として整理される。

SectorT グループは、高度な社会工学および技術回避技術で特徴づけられるサイバー攻撃に対する洗練されたアプローチを示しました。彼らの作戦は主にマクロが含まれた悪性 Word 文書の使用を特徴としており、これは検出および分析を回避するよう巧妙に偽装されています。注目すべき戦術は、ユーザーを偽の CAPTCHA を確認するように欺き、Malware を実行させる「CAPTCHA マクロ」技術の展開を含みます。この方法はセキュリティ対策を回避するだけでなく、政府テーマのコンテンツが含まれた餌文書を表示して合法的な相互作用の幻想を維持します。主要ペイロード

は%LOCALAPPDATA%¥¥EReciver ディレクトリに戦略的に配置され、regsvr32.exe を通じて実行される.NET DLL ファイル「EdgeService.dll」の展開を含みます。この DLL はコマンド＆コントロールサーバーとの継続的な通信を確立し、定期的な間隔で HTTP POST リクエストを通じてエンコードされたシステム情報を送信する役割を果たします。攻撃インフラは特定の地域を対象とする特定の文書およびファイル名の使用によってさらに特徴づけられ、他の地理的な場所に対する以前の攻撃で類似の戦術の証拠があります。フィッシング作戦は、「Лист мадопомога.doc」のような文書が伝統的なセキュリティ防御を回避するために動的マクロを使用するなど、細心の注意を払って設計されています。これらのマクロは主要な悪性ペイロードを実行するだけでなく、検出および分析をさらに複雑にするために自動化されたプロセスを通じて生成されたと見られる高度な難読化技術を統合しています。SectorT グループの作戦は、多数の目標にわたって彼らの目標を達成するために社会工学および Malware 開発を両方活用する高いレベルの技術的洗練を反映しています。

SectorJ グループと関連するハッキング活動は、サイバー攻撃を実行する際の彼らの適応力と技術的能力を強調する洗練された多様な戦術、技術、手順(TTP)を示している。SectorJ グループは Malware を配布するためにデジタル署名されたファイルを活用し、検出を回避するために高度なアンチサンドボックスおよびアンチデバッグ技術を使用する一貫したパターンを示した。彼らの Malware はしばしば追加のペイロードをダウンロードして実行するために Amazon AWS S3 バケットのような外部クラウドサービスと通信し、これはコマンドおよびコントロール作戦のためのクラウドインフラへの依存を示している。合法的な会社のデジタル署名を使用することは、セキュリティ対策を回避し、対象システム内で信頼を得ようとする努力を示唆している。また、このグループは広範なアンチ仮想マシン検査を使用して彼らの Malware が制御された環境で検出されないようにしている。SectorJ グループのキャンペーンはしばしば偽の求職申請書や損傷した合法的なウェブサイトのような社会工学戦術で始まり、初期アクセスを得る。彼らは Malware .lnk ファイル、DLL および PowerShell スクリプトを使用してペイロードを実行することで知られており、これは洗練された Malware である more_eggs および Cobalt Strike の配布で終わる多段階感染チェーンを示している。彼らの側面移動技術は、既知の脆弱性の悪用、ローカル管理者アカウントの作成、環境列挙のための SharpShares および Seatbelt のようなツールの使用を含む。持続性は Windows サービスの作成およびネットワークアクセスのための Cloudflared トンネルの使用を通じて達成される。このグループの Malware 武器庫には、フィッシングキャンペーンおよび悪意のある広告を通じてシステムに侵入するために使用される CastleLoader および CastleRAT のようなカスタム開発ツールが含まれている。これらのツールは検出を回避するためにコード難読化およびプロセスインジェクションを特徴としている。SectorJ グループはまた、Warlock および QWCrypt のようなランサムウェアを選択的に配布し、データ窃盗と財政的恐喝を統合する作戦への転換を示している。彼らの攻撃は、セキュリティ防御を回避するために Bring Your Own Vulnerable Driver (BYOVD)攻撃および DLL サイドローディングを含む高度な回避技術で特徴づけられる。SectorJ グループの作戦はまた、持続的で強力な回避行動を支援するインフラを活用し、サービス型 Malware(MaaS)モデルを使用することで特徴づけられる。彼らのキャンペーンはしばしば物流、ホスピタリティ、政府のような特定のセクターを

対象とし、影響力を最大化するために産業別の脆弱性を悪用する。ハイブリッドフィッシングキットおよびモバイル Malware 使用で見られるように、彼らの戦術を適応し進化させる能力は、彼らの作戦の複雑性が増していることを強調している。全体として、SectorJ グループの活動は、高度に組織化された体制のもとで複雑なサイバー攻撃を実行する能力を有する脅威行為として整理される。

Detail information

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

1) SectorA01 used Lazarus tools for stealthy remote desktop attacks (2025-11-21)

https://cti.nshc.net/events/view/20505

攻撃対象産業群: IT

最近の分析によると、脅威グループが使用した精巧なスパイウェアが金融、政府、航空宇宙、軍事などのグローバル部門を対象に諜報と金銭的利益のために使用されたという。このツールは、組織内での隠密な作戦のために設計されたリモートデスクトップ制御が可能なカスタムモニタリングプログラムである。このプログラムは持続性と隠蔽性を保証するために Windows Shell 拡張メカニズムを悪用し、DLL ファイルとバックグラウンドプロセスを使用して持続的なリモートモニタリングと制御を行う。Windows Update を通じて合法的なサービスに偽装し、Windows Defender のようなセキュリティ対策を無効化するためにシステム構成を操作する。このプログラムの広範な機能にはスクリーンショット撮影、データをリモートサーバーにアップロード、リモートデスクトップ接続の設定などが含まれ、システムの安定性を維持した状態で悪意のある行為が行われる。分析結果、これらの活動は以前に北東アジアで観察された精巧な持続的脅威と一致し、高価値ターゲットを対象とした情報収集活動が文書化されている。これはこれらの努力に対する高いレベルの組織的支援を示している。

[Attack Flow]

1. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. Windows Shell 拡張メカニズムを悪用し、悪性コンポーネントが自動実行されるように設定
   b. DLL ファイルをバックグラウンドプロセスとしてロードし、持続的な実行環境を維持
2. [Defense Evasion] Impair Defenses (T1562)
   a. Windows Defender 機能を無効化し、セキュリティ検出を回避
   b. Windows Update サービスに偽装することで、悪性行為を正規の動作として隠蔽
3. [Collection] Screen Capture (T1113)
   a. 感染したシステムにおいて定期的に画面をキャプチャ

b. ユーザーの活動を継続的にモニタリング

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

a. 収集されたデータをリモートサーバーへ送信

b. リモートデスクトップ接続を設定し、システムを制御

2) SectorA01 used OtterCookie Malware in Malicious npm Packages (2025-11-26)

https://cti.nshc.net/events/view/20573

「Contagious Interview」として識別されたサイバー攻撃作戦は、npm エコシステムを体系的に標的とし、2025 年 10 月以降、少なくとも 197 個の新たな悪性パッケージを侵入させている。脅威行為者は偽の面接や課題を用いて、ブロックチェーンおよび Web3 開発者を狙う。このキャンペーンは、GitHub、Vercel、そしてコマンド＆コントロール（C2）サーバを利用する高度なインフラストラクチャを伴い、OtterCookie と呼ばれる悪性コードの亜種を配布する。
この悪性コードは、多段階の情報窃取およびリモートアクセス機能を備え、仮想マシンの検知、クリップボード情報の窃取、グローバルキー入力記録、ファイルシステムスキャン、複数のオペレーティングシステムにおける認証情報窃取といった機能を含む。脅威行為者は「tailwind-magic」などのタイポスクワッティングされた npm パッケージを使用し、リモートコード実行機能を持つローダとして活用するとともに、GitHub リポジトリなどのプラットフォームを利用して正規の開発プロジェクトに見せかける。インフラストラクチャは、GitHub にホスティングされた開発用リポジトリ、Vercel によるペイロード配信、そして感染したホストに対してタスクを割り当てる独立した C2 サーバで構成される。この作戦は、ソフトウェアサプライチェーン攻撃に対する体系的なアプローチを示し、現代の開発ワークフローを狙って継続的な更新と回避技術を駆使している。

[Attack Flow]

1. [Initial Access] Supply Chain Compromise: Compromise Software Dependencies and Development Tools (T1195.002)

a. タイポスクワッティング npm パッケージ掲示

b. npm エコシステムを通じたマルウェア配布

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

a. postinstall スクリプト実行

b. JavaScript ペイロードのロードおよび実行

3. [Defense Evasion] Virtualization/Sandbox Evasion (T1497)

a. 仮想環境検出

b. サンドボックス回避検査

4. [Discovery] System Information Discovery (T1082)

a. オペレーティングシステムおよび環境識別

b. ホスト指紋収集

5. [Credential Access] Input Capture: Keylogging (T1056.001)
   a. キー入力収集
   b. クリップボードデータの脱取
6. [Collection] Data from Local System (T1005)
   a. ファイルシステムスキャン
   b. 資格証明および機密情報の収集
7. [Command and Control] Application Layer Protocol (T1071)
   a. C2 サーバー通信
   b. 作業指示受信およびデータ転送

3) SectorA01 exposed Infrastructure following LummaC2 Infostealer Infection (2025-12-04)

https://cti.nshc.net/events/view/20755

北朝鮮政府が後援する脅威行為者が一般的にサイバー犯罪活動で使用される情報脱取型 Malware に感染する事件が発生し、彼らの作戦に対する洞察を明らかにした。この感染はサイバー犯罪情報会社によって発見され、14 億ドル規模の暗号通貨脱取に関連する北朝鮮 Malware 開発者の機器に追跡された。この事件は LummaC2 情報脱取型 Malware が Bybit 取引所侵害を支援するフィッシングドメインを登録するために使用されたメールを含む資格情報を捕捉しながら発生した。損傷した機器は Visual Studio や Enigma Protector のようなツールを備えた精巧な装備で、専門的な Malware 開発能力を示している。分析結果、Astrill VPN を通じたアメリカ IP 使用と中国および韓国作戦との関連性を示唆する言語設定が明らかになった。Slack や Dropbox のような通信アプリは内部調整を示した。この事件は国家と連携したサイバー犯罪の運用インフラを明らかにし、そのような組織的な攻撃の作動方式に対する稀な洞察を提供し、一般的に安全な設定内の脆弱性を強調する。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. ダウンロードリンクへの誘導
2. [Execution] User Execution (T1204)
   a. LummaC2 情報窃取型マルウェアの実行
3. [Credential Access] Credential Dumping (T1003)
   a. メールアカウントの資格情報窃取
4. [Discovery] System Information Discovery (T1082)
   a. システム環境情報の収集
   b. 開発ツールのインストール有無の確認

5. [Collection] Data from Local System (T1005)
   a. 保存された資格情報の収集
   b. アプリケーションデータの収集

4) SectorA01 used Identity Fraud to Infiltrate U.S. Financial Firms (2025-12-04)

https://cti.nshc.net/events/view/20756

攻撃対象産業群: 金融, IT

サイバー脅威分析で、アメリカ金融および暗号通貨部門にリモート IT 労働者を配置しようとする北朝鮮の作戦が明らかになった。これは、制裁を受けた政権のための資金を生成するための企業スパイ活動として機能する。侵入者たちは、社会工学技法を通じて盗用した身元を使用し、IT 労働者に偽装し、高度な Malware を避けた。募集は GitHub と Telegram を通じて広範囲に行われ、被害者たちは個人データとデバイスへのアクセスを提供した。この作戦は AnyDesk、Google Remote Desktop、AI インタビューヘルパーのようなツールを活用した。予測可能なツールの使用がセキュリティの脆弱性を明らかにしたにもかかわらず、作戦は成功した社会工学戦術のおかげで続けられた。調査官たちは、制御された環境を作り、作戦要員の方法をモニタリングし分析し、内部コミュニケーションの断絶とインフラ共有に対する脆弱性を明らかにした。これは、シミュレーションされたノートブック農場(laptop farm)での活動をモニタリングすることで詳細に明らかにされた。これは、開発者ネットワークを悪用するより広い戦略と彼らの運用行動に対する稀な洞察を提供する。

[Attack Flow]

1. [Initial Access] Valid Accounts (T1078)
a. 採用を通じて合法的アカウント発行
   b. 内部システムおよび協力ツールアクセス
2. [Persistence] Account Manipulation (T1098)
   a. リモートワークアカウントの長期維持
   b. 正常なユーザーとして活動し、アクセス権限を変更しない
3. [Defense Evasion] Proxy (T1090)
   a. VPN サービス使用
   b. 接続位置の隠蔽を目的とした住宅用プロキシの使用
4. [Command and Control] Remote Access Software (T1219)
   a. AnyDesk を通じたリモートワーク環境の維持
   b. Google Remote Desktop 活用
5. [Collection] Data from Information Repositories (T1213)
   a. 内部コードリポジトリアクセス
   b. 業務文書および内部システム情報の収集

6. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. リモートアクセスセッションを通じた情報の持ち出し
   b. 外部制御インフラへのデータ移行
7. [Impact] Financial Theft (T1657)
a. 給与受領
   b. 制裁回避目的の外貨収益創出

5) SectorA01 used Pharos Automation Bot-themed Archive for Malware Delivery (2025-12-12)

https://cti.nshc.net/events/view/21003

攻撃対象産業群: 金融, 航空宇宙, 製造, 政府・行政

最近のサイバー脅威作戦は、WinRAR の脆弱性 (CVE-2025-8088) を悪用して "Pharos.rar" という悪性 RAR ファイルを配信しました。このファイルは合法的な自動化ツールに偽装し、解凍時にディレクトリトラバーサルを引き起こしました。被害者がファイルを解凍した際、開始ディレクトリに悪性スクリプトを展開し、Dropbox から追加の Malware をダウンロードさせました。主要ペイロードである "Blank Grabber" は、Chromium ベースのブラウザ、Discord、Telegram、そして 20 以上の暗号通貨ウォレットから資格情報を狙いました。攻撃は、複数の層にわたる base64 デコードと ZIP 解凍を含む多段階の難読化解除技術を使用し、予約タスクを通じて持続的な環境を作成しました。この作戦は、デジタル資産市場内でのかなりの窃取を専門とする高度持続脅威グループの知られた戦術と一致し、貴重なデータを精密にターゲットし、暗号通貨の窃取に戦略的に集中していることを示しています。

[Attack Flow]

1. [Execution] User Execution: Malicious File (T1204.002)
   a. 悪性 RAR ファイル圧縮解除
   b. ディレクトリトラバーサルを通じた悪性スクリプト生成
2. [Execution] Command and Scripting Interpreter (T1059)
   a. マルウェアスクリプト実行
   b. Dropbox ベースの追加ペイロードのダウンロード
3. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder (T1547.001)
   a. Startup program path に悪性スクリプトを登録
4. [Persistence] Scheduled Task/Job: Scheduled Task (T1053.005)
   a. 予約タスクの作成
5. [Defense Evasion] Obfuscated Files or Information (T1027)

a. 多段階エンコーディングおよび圧縮解除
b. base64 デコードおよび ZIP 圧縮解除
6. [Credential Access] Credentials from Password Stores (T1555)
a. Chromium ベースのブラウザ認証情報の窃取
b. 暗号通貨ウォレット資格証明窃取
7. [Collection] Data from Local System (T1005)
a. Discord アプリケーションデータ収集
b. Telegram アプリケーションデータ収集

6) SectorA02 used Node.js Malware disguised as Gaming Cheat Tools (2025-12-17)

https://cti.nshc.net/events/view/21142

攻撃対象産業群: 政府・行政、軍事機関

最近の分析では、YouTube Ghost Network に関連するサイバー脅威を詳しく説明する。このネットワークは、損傷したアカウントを利用して悪性ビデオを通じて Malware を拡散させる。特に注目すべき点は、GachiLoader という Node.js ベースの Malware ローダーを使用していることで、これは難読化および分析防止技術を通じて追加ペイロードを配布する役割を果たす。このキャンペーンは 2024 年 12 月 22 日に初めて検出され、220,000 回以上の再生回数を記録し、ゲームチートビデオを餌として使用する。GachiLoader は回避に長けており、ハードウェア中断点と Vectored Exception Handling を実装して精巧な PE 注入を行う。この技術は Vectored Overloading という新しいアプローチを含み、これは Windows OS ローダーのメカニズムを使用してメモリ内で合法的な DLL を悪性ペイロードに置き換えるものである。脅威行為者は Windows 内部に関する高度な知識を持っており、損傷したアカウントを通じて配信される Rhadamanthys 情報窃取型 Malware で疑わないユーザーを標的にする。この Malware は多様なサンドボックス検出方法論を使用して検出を回避し、ユーザーアクセス制御プロンプトを通じて権限を変更する。

[Attack Flow]

1. [Execution] User Execution: Malicious File (T1204.002)
a. マルウェアリンクベースのファイルダウンロード
b. ゲームチート偽装ファイル実行
2. [Execution] Command and Scripting Interpreter: JavaScript (T1059.007)
a. Node.js 基盤 GachiLoader 実行
b. 追加ペイロードロード
3. [Defense Evasion] Obfuscated Files or Information (T1027)
a. JavaScript 難読化 適用
b. サンドボックス検出および分析回避

4. [Defense Evasion] Process Injection (T1055)
   a. Vectored Exception Handling 悪用
   b. Vectored Overloading 基盤 PE 注入
5. [Privilege Escalation] Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
   a. UAC プロンプト操作
6. [Command and Control] Application Layer Protocol (T1071)
   a. HTTP ベースの C2 通信
   b. 作業指示受信

7) SectorA05 LNK-Based Lure to Deploy KimJongRAT (2025-11-21)

https://cti.nshc.net/events/view/20569

攻撃対象産業群: 市民

2010 年代に遡る変種 Malware を含む精巧なサイバー脅威がフィッシングメールを通じて敏感なユーザーデータを持続的に狙う。この攻撃はモジュール型 Malware を使用してシステムおよびブラウザ情報を奪取することを目的としており、敏感な情報を解読するためのマスターキーを抽出して Chromium ベースのブラウザをターゲットにする。脅威行為者は GitHub および Google Drive インフラを悪用して Malware 変種を迅速に配布する。エンジニアは関連インフラと公共機関の公式通信に偽装した他のタイプのスピアフィッシングメールを識別し、これは社会工学的戦術を使用してユーザーが本物のファイルに偽装された悪性スクリプトを実行するよう強制する。このキャンペーンはローカルシステムでデータを奪取するために DLL インジェクションと PowerShell スクリプトを活用し、検出を避けるために複数のレイヤーの難読化を使用する。攻撃者はまた、被害者を合法的なログインページを模倣した偽のログインページにリダイレクトしてログイン資格情報を盗むフィッシング手法を使用し、これは韓国技術ユーザーを対象としたキャンペーンで観察された。この脅威は社会工学と技術的なトリックを活用して侵害されたシステムへの足場を維持する高度持続脅威がもたらすリスクを強調する。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 公共機関を装ったスピアフィッシングメール
   b. 悪性文書および LNK ファイルを添付
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. Base64 エンコーディングされた PowerShell の実行
   b. 難読化されたスクリプトのロード
3. [Persistence] Boot or Logon Autostart Execution (T1547)

a. レジストリの Run キーへの登録
b. 予約タスクを利用したスクリプトの登録
4. [Defense Evasion] Obfuscated Files or Information (T1027)
a. PowerShell コマンドの難読化
b. 動的 API 呼び出しの隠蔽
5. [Credential Access] Input Capture: Keylogging (T1056.001)
a. キー入力の収集
b. クリップボードデータの収集
6. [Discovery] System Information Discovery (T1082)
a. システムおよび OS 情報の収集
b. ブラウザ環境情報の確認
7. [Collection] Data from Local System (T1005)
a. ブラウザ資格情報の収集
b. 証明書および機密ファイルの収集
8. [Command and Control] Application Layer Protocol (T1071)
a. HTTP ベースの C2 通信
b. POST リクエストを用いたデータ送信
9. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. 収集データの圧縮
b. 暗号化されたデータの転送

8) SectorA05 used Phishing Emails Disguised as Tax Notifications (2025-11-28)
https://cti.nshc.net/events/view/20613

フィッシングキャンペーンが 11 月税金申告および納付に関する税務当局の通知を装うメールを使用して実行された。メールは受信者に特定期限までに文書を確認するよう促し、これを通じてフィッシングサイトにリダイレクトされた。脅威行為者たちは合法的なメールサービスである Zoho Mail を使用してこれらのフィッシングメールを送信し、サービスの合法性を悪用して基本メールフィルターを回避した。メールは精巧に作成されており、SPF、DKIM、DMARC 認証検査を通過し、これはメールが検証済みの Zoho サーバーから送信されたことを示している。送信者はドメインをスプーフィングせずに Zoho のインフラを使用しているように見え、これはドメインスプーフィングよりもフィッシングのためのプラットフォーム悪用を示唆している。技術的合法性検査を通過したにもかかわらず、送信者アドレスとメール形式はフィッシングの意図を示し、主要メールサービスプロバイダーのユーザーを対象としている。この攻撃は信頼を悪用し、セキュリティ対策を回避するために合法的なインフラを使用するフィッシングキャンペーンの効果を強調している。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. 税務当局を装ったフィッシングメールの送信
   b. メール本文に文書確認を装ったリンクを挿入
   c. 受信者がリンクをクリックすると外部のフィッシングサイトへリダイレクト
2. [Defense Evasion] Abuse of Trusted Infrastructure (T1583)
   a. Zoho Mail の正規送信インフラを悪用したメール送信
   b. SPF、DKIM、DMARC 認証検査を通過し、技術的セキュリティフィルターを回避
   c. ドメインスプーフィングを行わず、合法的な送信構造を維持
3. [Credential Access] Input Capture: Credentials from Web Forms (T1056.004)
   a. 正規サービスのログインページを模倣したフィッシング Web ページの提供
   b. ユーザーにアカウント情報の入力を誘導
   c. Web フォームを通じて入力された資格情報の収集
4. [Collection] Data from Information Repositories (T1213)
   a. 収集した資格情報を攻撃者側のストレージへ送信
   b. 将来的なアカウント乗っ取りおよび追加悪用を目的とした情報の蓄積

9) SectorA05 used LNK Malware disguised as a Tax Notice Statement (2025-12-03)

https://cti.nshc.net/events/view/20831

Sophisticated cyber threats include malicious zip files impersonating tax orders in specific regions, suspected to be distributed by a North Korean group. 2013 年に開始されたこの攻撃は、PE ファイルと PowerShell を使用して、ブラウザデータや暗号通貨ウォレット情報を含む重要なユーザーデータを実行および収集します。実行時に、Malware は仮想環境を確認し、餌の PDF ファイルのパスワードを表示します。この Malware は主にメールを通じて被害者を対象とし、Windows Defender 設定の脆弱性を悪用します。Windows Defender が無効化されている場合、システムデータ、暗号化キー、通信ソフトウェアセッションを含む機密情報を収集するファイルをダウンロードします。データは Base64、XOR、AES のような暗号化技法を使用して指定された C2 サーバーに漏洩されます。持続性はレジストリの修正と PowerShell スクリプトを通じて達成されます。このキャンペーンは主要なブラウザと暗号通貨拡張機能からデータを漏洩することを目標としており、特に韓国のユーザーと金融データを重点的に狙っています。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 税金通知文書を装ったメール送信
   b. 悪意のある ZIP ファイル添付

2. [Execution] User Execution: Malicious File (T1204.002)
   a. Malware ファイル実行
   b. PowerShell スクリプト ロード
3. [Defense Evasion] Impair Defenses: Disable or Modify Tools (T1562.001)
   a. Windows Defender 設定確認
   b. セキュリティ機能無効化の判断
4. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder (T1547.001)
   a. レジストリ Run キー修正
   b. PowerShell ベースの開始項目登録
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. PowerShell コマンド難読化
   b. エンコードされたスクリプト実行
6. [Discovery] System Information Discovery (T1082)
a. システムおよびハードウェア情報収集
   b. 仮想環境検出
7. [Credential Access] Credentials from Password Stores (T1555)
   a. ブラウザ保存資格情報復号化
   b. 暗号通貨ウォレットキー収集
8. [Collection] Data from Local System (T1005)
a. ブラウザデータ収集
   b. 通信アプリケーションセッションデータ収集
9. [Command and Control] Application Layer Protocol (T1071)
   a. HTTP ベースの C2 通信
   b. 状態情報送信
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 収集データ暗号化
   b. C2 サーバーへのデータ転送

10) SectorA05 used music-themed VBS downloader (2025-12-08)

https://cti.nshc.net/events/view/20899

サイバー脅威事件は、対象システムで悪性行動を実行するように設計された VBS 다운로더と関連している。この Malware は、ファイルをダウンロードして実行できる能力で特徴付けられ、スクリプトを使用して作業を行う Windows 環境を特定の対象としている。技術的過程には、プログラム実行のための WScript.Shell オブジェクト生成、ファイル操作のための

FileSystemObject、HTTP リクエストのための MSXML2.XMLHTTP 生成が含まれる。ダウンローダーは特定の URL からファイルを取得し、ここには S3 バケット(proadead[.]s3[.]sa-east-1[.]amazonaws[.]com)と関連する IP アドレス(152[.]42[.]226[.]161)が含まれている。これらのファイルはユーザーを欺くために musicx.exe と proton.mp4 のような合法的なメディアファイルに偽装されて公用ディレクトリに保存された。実行過程では、musicx.exe を目立たせて実行し、同時にメディアプレーヤーで proton.mp4 を開いて悪性活動を正常な行動に偽装した。コードはシーザー暗号基盤の難読化を使用し、特定のファイルがないことを確認した後にのみ行動を実行し、主な役割がその後の Malware 拡散のためのローダーやドロッパーとして機能することを示している。

[Attack Flow]

1. [Execution] User Execution: Malicious Script (T1204.001)
   a. VBS ダウンローダーの実行
   b. メディアファイルに偽装されたスクリプトの実行
2. [Execution] User Execution: Malicious File (T1204.002)
   a. musicx.exe の実行
   b. proton.mp4 の同時再生を通じた行為の偽装
3. [Execution] Command and Scripting Interpreter: Visual Basic (T1059.005)
   a. WScript.Shell オブジェクトの生成
   b. FileSystemObject を基盤としたファイル操作
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. シーザー暗号を基盤とした難読化
5. [Discovery] System Information Discovery (T1082)
   a. 環境変数の確認
   b. 特定ファイルの存在有無の確認
6. [Command and Control] Application Layer Protocol (T1071)
   a. MSXML2.XMLHTTP を基盤とした HTTP リクエスト
   b. S3 バケットからのファイルダウンロード

11) SectorA05 used LNK Malware disguised as US Security Strategy (2025-12-12)

https://cti.nshc.net/events/view/21058

本サイバーセキュリティ脅威は、「2025 National Security Strategy of the United States of America.lnk」に偽装したマルウェアを含む。このマルウェアは、Base64 でエンコードされた PowerShell コードを使用する。まず、ペイロードは「%TEMP%¥check.ps1」にデコードされて保存され、隠しウィンドウで実行される。当該スクリプトは、GitHub の個人アクセストークンを使用

して追加の悪意あるスクリプトをダウンロードし、「2025-National-Security-Strategy of the United States of America.pdf」という名称の PDF ファイルをデコイとして使用する。マルウェアは「%AppData%¥edge.ps1」を生成し、これを NVidia ドライバーアップデートに偽装して Windows タスクスケジューラに登録することで持続性を確保し、30 分ごとに実行される。スクリプトは、隠し・非対話型オプションで動作し、ローカルの ExecutionPolicy 設定を回避する。本マルウェアは、国家安全保障に関連するユーザーを標的として悪意あるペイロードを実行し、実行後に痕跡を削除する。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 政策文書に偽装した LNK ファイルの添付
   b. 誘導用 PDF ファイルの提供
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. Base64 エンコーディングされた PowerShell スクリプトのデコード
   b. 隠しウィンドウでのスクリプト実行
3. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Base64 エンコーディングの使用
4. [Defense Evasion] Impair Defenses: Disable or Modify Tools (T1562.001)
   a. ExecutionPolicy の回避
   b. 非対話型オプションによる実行
5. [Persistence] Scheduled Task/Job: Scheduled Task (T1053.005)
   a. タスクスケジューラへの登録
   b. NVidia ドライバーアップデートへの偽装
6. [Defense Evasion] Masquerading (T1036)
   a. 正規アップデート名称の使用
   b. 正常な処理に偽装したスケジュール登録
7. [Command and Control] Application Layer Protocol (T1071)
   a. GitHub インフラへのアクセス
   b. 追加マルウェアスクリプトのダウンロード
8. [Defense Evasion] Indicator Removal on Host (T1070)
   a. 実行後のファイル削除
   b. 痕跡の除去

12) SectorA05 used HWPX Malware disguised as Graduate Document (2025-12-14)

https://cti.nshc.net/events/view/21054

攻撃対象産業群: 高等教育

Malware キャンペーンは、2026 年韓国の修士夜間課程大学院生選抜に関連する文書に偽装した Malware を配布することを含む。攻撃はユーザーを欺くために偽の支援文書が含まれた zip ファイルを含むメールを送信することから始まる。ファイルを開くと、Base64 でエンコードされた ZIP ペイロードが配布され、"%ALLUSERSPROFILE%¥"ディレクトリにバイナリファイルを保存する。攻撃はその後、MSXML2.XMLHTTP を活用して損傷したソースから見かけ上合法的な Visual Studio Code CLI ZIP ファイルをダウンロードし、これを対象システム内に展開する。その後、code.exe が実行され、検出を避けるために偽装された識別子を使用してトンネルが設定される。トンネル出力ログは重要な運用詳細を含んでおり、定期的に確認されて外部サーバーに送信される。この作業は承認されていないリモートアクセスを容易にし、システム悪用、内部ネットワーク移動、追加情報抽出につながる可能性があり、主に大学院支援に関連する個人を対象としている。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 大学院支援文書を装ったメール送信
b. 悪意のある ZIP ファイル添付
2. [Execution] User Execution: Malicious File (T1204.002)
   a. 偽装されたサポートドキュメントファイルの実行
   b. Base64 エンコードされたペイロードのデコード
3. [Execution] Command and Scripting Interpreter: JavaScript (T1059.007)
   a. JScript ベースのスクリプト実行
   b. バイナリファイル生成および実行
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Base64 エンコーディング ZIP ペイロード
   b. スクリプトベースの難読化
5. [Command and Control] Application Layer Protocol (T1071)
   a. MSXML2.XMLHTTP 基盤ファイルダウンロード
   b. code.exe を利用したトンネル設定
6. [Collection] Data from Local System (T1005)
   a. トンネル出力ログ生成
   b. ログファイル定期的確認
7. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. ログデータ外部サーバー転送
   b. URL エンコーディング データ 送信

13) SectorA05 used Android Malware disguised as Delivery Apps (2025-12-16)

https://cti.nshc.net/events/view/21132

2025 年 9 月、「DOCSWAP」という Malware モバイルアプリがフィッシングサイトを通じて配布され、ユーザーが QR コードと通知プロンプトを使用してこれをインストールし実行するよう誘導されました。このアプリはコマンド＆コントロール（C2）サーバーと通信し、リモートアクセスツール（RAT）サービスを登録することが判明しました。攻撃者は新たに追加されたネイティブ復号化機能と多様な餌行動を使用して疑念を減らしました。分析の結果、メタデータとインフラから他の Malware アプリおよび C2 サーバーとの類似性を含む、既知の脅威キャンペーンとの接続が明らかになりました。配布方法はスミッシングとフィッシングメールを通じて URL を含め、配送会社を模倣しており、PC でアクセスする際にモバイル中心のインターフェースに被害者をリダイレクトしました。アプリである SecDelivery.apk は XOR 復号化と追加のビット演算のような複雑な技術を使用して埋め込まれた Malware APK ファイルを復号化し、ペイロードを実行するために複数の権限を登録しました。攻撃インフラは類似の属性を持つ複数の C2 サーバーを含み、既知のプラットフォームのためのプロキシベースのフィッシングサイトを使用するより広範なフィッシングキャンペーンと接続されていました。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. 配送業者を装ったスミッシングおよびフィッシングメッセージの送信
   b. QR コードおよび URL を通じたフィッシングサイトへの誘導
2. [Execution] User Execution: Malicious File (T1204.002)
   a. マルウェア APK のダウンロード
   b. ユーザー承認に基づくアプリのインストールおよび実行
3. [Defense Evasion] Masquerading (T1655)
   a. 配送関連アプリへの偽装
   b. 誘導用 UI および通知プロンプトの使用
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. XOR 方式によるペイロードの復号
   b. 追加のビット演算を通じたコード隠蔽
5. [Persistence] Event Triggered Execution: Broadcast Receivers (T1624.001)
   a. ブロードキャストレシーバーの登録
   b. RAT サービスの自動実行
6. [Privilege Escalation] Abuse Elevation Control Mechanism (T1548)
   a. 過剰な権限要求
   b. ランタイム権限の濫用
7. [Discovery] System Information Discovery (T1426)

a. デバイス情報の収集
b. インストール済みアプリケーションの列挙
8. [Collection] Input Capture: Keylogging (T1417.001)
a. アクセシビリティサービスの悪用
b. キー入力の収集
9. [Command and Control] Application Layer Protocol (T1437)
a. C2 サーバーとの通信
b. 暗号化されたペイロードの交換
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. 収集データの圧縮

14) SectorB49 used BADAUDIO disguised as legitimate DLLs (2025-11-21)

https://cti.nshc.net/events/view/20366

脅威行為者によって 3 年にわたり進行された適応型サイバースパイキャンペーンが発見され、BADAUDIO Malware を最初の段階のダウンロードプログラムとして配布し、ネットワークへの持続的なアクセスを確立します。初期には広範囲なウェブ損傷を使用しましたが、攻撃者は戦術を変更し、台湾の組織を特定ターゲットにしてデジタルマーケティング会社を損傷し、サプライチェーン攻撃を開始し、フィッシングキャンペーンを調整しました。C++で作成された BADAUDIO は、コマンド＆コントロールサーバーから AES で暗号化されたペイロードを復号化して実行し、初期にはシステム情報を収集して暗号化された状態で送信します。この Malware は、制御フロー平坦化、DLL 検索順序ハイジャック、悪性 DLL を含む暗号化されたアーカイブのインストールなどの高度な難読化技術を活用して持続性を維持します。戦略的に、ウェブ損傷キャンペーンは指紋認識のために JavaScript を悪用し、Windows システムをターゲットにして偽のダイアログボックスを使用して BADAUDIO のダウンロードを誘導しました。このキャンペーンはまた、合法的なクラウドサービスを配布に活用し、追跡リンクを使用した社会工学を通じてターゲティングを強化し、高度な持続性と適応能力を示しています。

[Attack Flow]

1. [Initial Access] Supply Chain Compromise: Compromise Software Dependencies and Development Tools (T1195.001)
a. デジタルマーケティング企業の侵害
b. JavaScript ライブラリへのマルウェア挿入
2. [Initial Access] Phishing: Spearphishing Link (T1566.002)
a. ターゲット組織を対象としたフィッシングキャンペーン
b. 追跡リンクを用いた社会工学的誘導

3. [Execution] User Execution: Malicious File (T1204.002)
   a. 偽のダイアログボックスの表示
   b. BADAUDIO のダウンロードおよび実行
4. [Execution] Command and Scripting Interpreter: JavaScript (T1059.007)
   a. 悪性 JavaScript のロード
   b. 動的依存関係のロード
5. [Persistence] Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
   a. DLL サイドローディング
   b. 正規実行ファイルの実行フローのハイジャック
6. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. 制御フローの平坦化
   b. 暗号化されたアーカイブの使用
7. [Discovery] System Information Discovery (T1082)
   a. システム情報の収集
   b. ホストおよびブラウザのフィンガープリント収集
8. [Collection] Data from Local System (T1005)
   a. 基本的なシステム情報の収集
   b. クッキーへのデータ埋め込み
9. [Command and Control] Application Layer Protocol (T1071)
   a. 暗号化された C2 通信
   b. クッキーを用いたデータ送信
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. 偵察データの隠匿転送
    b. Base64 エンコーディングによるデータ流出

15) SectorB94 used Discord API for Backdoor Malware Deployment (2025-11-26)

https://cti.nshc.net/events/view/20567

最近のサイバー脅威事件で攻撃者たちは、Discord API をコマンドおよびコントロール(C2)チャンネルとして使用し、バックドア Malware を配布しました。この事件は 2025 年 11 月 26 日に発生し、システムを長期間にわたって制御するために標的化されました。初期には vshell のような既知のバックドアを使用してシステムに侵入し、その後、検出を避けるために Discord ボットベースのバックドアをインストールしました。Discord API を使用することで、攻撃者たちは既存のセキュリティ対策を回避し、合法的なユーザー活動に似たトラフィックパターンを生成しました。この戦略は攻撃者たちの持続性モデルと一致し、既存のサーバーが検出またはブロックされた場合に代替 C2 チャンネルを保証します。GitHub の Discordgo モジュールを使用して作成されたバックドアは、Discord の

MessageCreate イベントを通じてコマンドを受信すると実行されました。これはコマンド実行、ファイルのアップロード/ダウンロード、システム情報の収集といった機能を可能にし、オープンソースライブラリを活用しました。攻撃者たちの方法は、アクセス可能なツールを使用して隠密な Malware を簡単に生成できることを強調し、サイバー攻撃におけるオープンソース悪用の増加する脅威を浮き彫りにします。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. vshell バックドアの悪用
   b. 公開サービスを対象とした侵入
2. [Execution] Command and Scripting Interpreter: Bash (T1059.004)
   a. MessageCreate イベントの受信
   b. bash コマンドの実行
3. [Command and Control] Application Layer Protocol: Web Services (T1071.001)
   a. Discord API を基盤とした C2 通信
   b. 正常なユーザートラフィックパターンの模倣
4. [Command and Control] Proxy: Internal Proxy (T1090.001)
   a. Discord ボットを基盤とした内部プロキシ構成
   b. 代替 C2 チャネルの維持
5. [Collection] Data from Local System (T1005)
   a. システム情報の収集
   b. オープンソースライブラリの活用
6. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 実行結果の Discord 送信
   b. 一時ファイルを基盤としたデータ処理

16) SectorB110 used Malware Disguised as Bitdefender Program (2025-12-10)

https://cti.nshc.net/events/view/20924

この洗練された Malware は、データ脱取とペイロードステージングを容易にするために Google Drive API を活用し、検出を困難にします。該当 Malware は、ファイル転送、コマンド実行、偵察を可能にするタスク管理システムを含みます。主要構成要素には WMLOADER があり、これは合法的なセキュリティプログラムに偽装し、ファイルで AES-CBC を使用して復号化された埋め込みシェルコードを通じて NANOREMOTE をロードします。この Malware は API 認証のためにパイプで区切られた設定を使用し、システムプロファイリングやファイル転送などの多様な機能を許可する 22 のコマンドハンドラーを持っています。C2 通信は HTTP を通じて行われ、Zlib 圧縮と AES 暗号化を

使用します。NANOREMOTE は FINALDRAFT とコードの類似性を共有し、ステルスのためのカスタム PE ローディングのような技法を含みます。この Malware の能力は複雑な回避技法を示し、企業ネットワークに深刻な脅威となります。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. セキュリティプログラムに偽装された WMLOADER の配信
   b. デジタル署名エラーを含むファイルの添付
2. [Execution] User Execution: Malicious File (T1204.002)
   a. WMLOADER の実行
   b. 埋め込みシェルコードのデコード
3. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.003)
   a. シェルコードを用いた NANOREMOTE のロード
   b. コマンド実行処理
4. [Defense Evasion] Masquerading (T1036)
   a. Bitdefender 構成要素への偽装
   b. 正規セキュリティファイル名の使用
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. AES-CBC を基盤としたペイロード暗号化
   b. Zlib 圧縮データの処理
6. [Discovery] System Information Discovery (T1082)
   a. システムおよびユーザー情報の収集
   b. ホスト環境のプロファイリング
7. [Collection] Data from Local System (T1005)
   a. ファイルの収集
   b. 作業管理コマンドの処理
8. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. HTTP ベースの C2 通信
   b. 暗号化されたコマンドの交換
9. [Exfiltration] Exfiltration Over Web Service: Cloud Storage (T1567.002)
   a. Google Drive API を用いたファイルアップロード
   b. 暗号化されたデータの転送

17) SectorB110 used ShadowPad Backdoor disguised in IIS servers (2025-12-16)

https://cti.nshc.net/events/view/21082

攻撃対象産業群: 政府・行政、通信

最近のサイバー攻撃の波は、ヨーロッパ、東南アジア、南アメリカ全域の政府機関を対象とする洗練され、能力のあるサイバー脅威行為者に起因する。このグループは、既知の IIS 誤った構成と脆弱性、例えば ViewState 逆シリアル化と ToolShell 脆弱性を利用して、脆弱な IIS と SharePoint サーバーに初期アクセスを得る。アクセスを得た後、彼らはカスタム ShadowPad IIS Listener モジュールを使用して、侵害されたサーバーを分散リレーネットワークに含め、C2 インフラの一部に変換する。このグループはまた、強化されたデータ流出と隠蔽のために FinalDraft Malware の新しい変種を展開する。彼らの戦略は、侵害されたホストを通信ノードに変換し、合法的な IIS プロセスに統合されたインターセプト機能を含む。彼らのキャンペーンは、LSASS ダンプとアイドル RDP セッションの悪用を含む複数の技術を使用して、包括的な側面移動、資格情報収集、権限昇格を通じてドメイン支配に至る。彼らの作戦は成熟し、モジュール化されたサイバースパイ活動のアプローチを反映し、高度な回避および持続性技術を示している。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. ViewState 逆シリアル化 脆弱性 悪用
   b. SharePoint ToolShell 脆弱性悪用
2. [Execution] Command and Scripting Interpreter (T1059)
a. ShadowPad ローダー配布
   b. CDBLoader 実行
3. [Persistence] Server Software Component (T1505)
a. ShadowPad IIS Listener モジュール設置
   b. IIS プロセス内 マルウェア モジュール ロード
4. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
   a. PrintNotifyPotato 脆弱性悪用
   b. SYSTEM 権限獲得
5. [Defense Evasion] Masquerading (T1036)
   a. 正常なバイナリ名でファイルを偽装
   b. デジタル署名されたバイナリ活用
6. [Credential Access] OS Credential Dumping (T1003)
a. LSASS メモリ ダンプ
   b. レジストリハイブ抽出
7. [Discovery] System Information Discovery (T1082)
   a. ホストシステムプロファイリング
   b. ネットワークアダプタ情報収集
8. [Lateral Movement] Remote Services (T1021)

a. アイドル状態の RDP セッションの悪用
b. ShadowPad トンネリング基盤移動
9. [Collection] Data from Local System (T1005)
a. ファイルおよびレジストリデータアクセス
b. RDP 使用履歴収集
10. [Command and Control] Application Layer Protocol (T1071)
a. ShadowPad リレー ネットワーク 通信
b. Microsoft Graph API 基盤 C2 使用
11. [Exfiltration] Exfiltration Over Alternative Protocol (T1048)
a. BackgroundFileTransfer 基盤データ転送
b. 非同期式大容量データ流出

18) SectorB118 used Cloudflare Tunnel prior to Warlock Ransomware Deployment (2025-12-03)

https://cti.nshc.net/events/view/20827

2025 年 11 月初、ランサムウェア侵入事件でリモートコマンド実行を可能にするために、複数のエンドポイントに Velociraptor が配布された。攻撃者はシステム点検を実行し、トンネルを構築し、接続性をテストするために Base64 でエンコードされた PowerShell コマンドを発行した。トンネリングユーティリティをインストールし、OpenSSH を開始しようとする複数の試みがあり、初期にはシステム制限で失敗したが、防御コントロールが無効化された後に成功した。新しいローカル管理者アカウントが作成され、側面移動に使用された。攻撃者は Visual Studio Code トンネリングを活用し、リモートデスクトップソフトウェアをインストールし、持続的な実行のために構成された Malware サービスを登録してアクセスを拡張した。この活動はランサムウェア配布につながり、暗号化後の復旧試行を示す復号化バイナリ実行が続いた。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
a. ToolShell 脆弱性の悪用
b. WSUS 脆弱性の悪用
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
a. Base64 エンコードされた PowerShell コマンドの実行
b. システム点検および接続性テストの実施
3. [Defense Evasion] Impair Defenses: Disable or Modify Tools (T1562.001)
a. Windows Defender の無効化
b. 正規ツールを用いた回避

4. [Persistence] Create or Modify System Process: Windows Service (T1543.003)
   a. Velociraptor サービスのインストール
   b. マルウェアサービスの登録
5. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. Velociraptor C2 の構成
   b. Visual Studio Code トンネリングの使用
6. [Privilege Escalation] Create Account: Local Account (T1136.001)
   a. ローカル管理者アカウントの生成
   b. 権限を有するアカウントの確保
7. [Lateral Movement] Remote Services: Remote Desktop Protocol (T1021.001)
   a. 管理者アカウントによる RDP ログイン
   b. リモートシステムへのアクセス
8. [Discovery] System Network Connections Discovery (T1049)
   a. ネットワーク接続状態の確認
   b. トンネルおよびサービスの点検
9. [Impact] Data Encrypted for Impact (T1486)
   a. ランサムウェアの配布
   b. データ暗号化の実行および復号化ツールの実行

19) SectorB123 used BRICKSTORM Malware on VMware vSphere Servers (2025-12-04)

https://cti.nshc.net/events/view/20814

攻撃対象産業群: IT、政府・行政

中華人民共和国の国家支援サイバー行為者が政府サービスおよび情報技術部門内のシステムで長期的な持続性を確保するために BRICKSTORM Malware を使用することが明らかになった。この Malware は、VMware vCenter および VMware ESXi サーバーを含む VMware vSphere プラットフォームと Windows 環境を対象とする高度な Go ベースのバックドアである。Web シェルを通じてアクセスが行われると、Malware は複製された仮想マシンスナップショットを通じて資格情報抽出を容易にし、隠された仮想マシンを生成することができる。BRICKSTORM はシステムファイルと環境変数を修正し、妨害された場合に自動で再インストールまたは再起動されるようにして持続性のための高度な方法を使用する。コマンドおよび制御のために HTTPS と WebSockets を含む複数の暗号化レイヤーを使用して通信を保護し、損傷したシステムを管理する。また、SOCKS プロキシを実装して側面移動を可能にし、合法的なサービスおよびネットワークトラフィックを模倣して自身の存在を隠すことにより、被害者システムに対する広範な制御を許可する。このキャンペーンは 2024 年 4 月から 2025 年 9 月までその基盤を維持してきた。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. Web Shell を通じたサーバーアクセス
b. 公開ウェブサービス侵害
2. [Execution] Command and Scripting Interpreter (T1059)
a. シェルコマンド実行
   b. 対話型シェルセッションの使用
3. [Persistence] Server Software Component: Web Shell (T1505.003)
   a. Web Shell インストール
   b. システムファイルおよび環境変数の修正
4. [Privilege Escalation] Abuse Elevation Control Mechanism: Sudo (T1548.003)
   a. sudo コマンド 使用
   b. 管理者権限獲得
5. [Defense Evasion] Masquerading (T1036)
   a. 合法サービス名称偽装
   b. PATH 環境変数操作
6. [Credential Access] OS Credential Dumping (T1003)
   a. 仮想マシン スナップショット 複製
   b. 資格証明書抽出
7. [Discovery] System Network Connections Discovery (T1049)
   a. ネットワーク経路識別
   b. 内部ネットワークマッピング
8. [Lateral Movement] Remote Services: SSH (T1021.004)
a. SSH 基盤の側面移動
   b. SOCKS プロキシ 活用
9. [Collection] Data from Information Repositories (T1213)
   a. 仮想マシンスナップショット収集
   b. 暗号化キーおよび設定データ収集
10. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. HTTPS 基盤 C2 通信
   b. WebSocket 暗号化接続
11. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. データ収集のアップロード
   b. 暗号化されたチャネルを通じたデータ転送

20) SectorB123 used Golang Malware disguised as legitimate vCenter processes (2025-12-04)

https://cti.nshc.net/events/view/20749

攻撃対象産業群: 製造、法律サービス、技術

2025 年の間、精巧なサイバー脅威行為者がアメリカ拠点の機関の VMware vCenter 環境を標的にし、BRICKSTORM Malware、JSP Web シェル、Junction および GuestConduit という 2 つの新しいインプラントを展開しました。この行為者は高度な運用セキュリティを示し、名前が明らかにされていない国家の戦略的利益と一致する可能性のある情報収集のために長期的な隠密アクセスを維持しています。初期アクセスは主にインターネットに露出したデバイスと VMware 環境の脆弱性を悪用して行われました。側面移動は SSH と有効な資格情報、特に vpxuser アカウントを含む権限のあるアカウントを使用して達成されました。この行為者はログ削除、ファイルタイムスタンプ変更、登録されていない VM 生成などの技術を使用して検出回避を行い、BRICKSTORM を使用してトラフィックをトンネリングし、インプラントを合法的なプロセスに偽装しました。7-Zip を使用してデータ流出を準備し、セッショントークンとユーザーセッション再生を活用して Microsoft Azure 環境を通じて敏感なクラウドデータにアクセスしました。この攻撃は MFA 操作と高度なトンネリングおよび難読化技術を使用して検出を避けるなど、高度なクラウド認識侵入を示しました。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. Ivanti デバイスの脆弱性悪用
   b. vCenter 露出脆弱性の悪用
2. [Initial Access] Valid Accounts: Cloud Accounts (T1078.004)
   a. 有効なクラウドアカウントの使用
   b. vpxuser アカウントの悪用
3. [Execution] Command and Scripting Interpreter: Java (T1059.007)
   a. JSP Web シェルによるコマンド実行
   b. Junction インプラントのコマンド処理
4. [Persistence] Server Software Component: Web Shell (T1505.003)
   a. JSP Web シェルの配置
   b. BRICKSTORM インプラントのロード
5. [Persistence] Account Manipulation (T1098.001)
   a. MFA デバイスの登録
   b. クラウドアクセスの維持
6. [Defense Evasion] Masquerading: Masquerade Task or Service (T1036.004)
   a. vCenter プロセスへの偽装

b. ESXi サービスへの偽装
7. [Defense Evasion] Indicator Removal on Host: File Deletion (T1070.004)
a. ログの削除
b. 痕跡ファイルの削除
8. [Defense Evasion] Hide Artifacts (T1564)
a. 未登録仮想マシンの生成
b. ファイルタイムスタンプの変更
9. [Discovery] File and Directory Discovery (T1083)
a. ファイルシステムの探索
b. 機密データの所在確認
10. [Lateral Movement] Remote Services: SSH (T1021.004)
a. SSH を基盤とした側面移動
b. SFTP セッションの活用
11. [Collection] Data from Information Repositories: Cloud Storage Object (T1213.002)
a. SharePoint ファイルへのアクセス
b. ドメインコントローラーVM スナップショットの収集
12. [Collection] Archive Collected Data: Archive via Utility (T1560.001)
a. 7-Zip によるデータ圧縮
b. データ漏洩準備用バンドルの生成
13. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
a. WebSockets over TLS 通信
b. DNS-over-HTTPS を基盤とした C2 通信
14. [Command and Control] Protocol Tunneling (T1572)
a. BRICKSTORM トラフィックのトンネリング
b. VSOCK 接続の使用
15. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. 圧縮データの外部転送
b. トンネリングチャネルを通じたデータ流出

21) SectorB128 exploited Cisco AsyncOS Software with AquaShell Backdoor (2025-12-17)

https://cti.nshc.net/events/view/21094

サイバー脅威キャンペーンが Cisco Secure Email Gateway と Cisco Secure Email and Web Manager を対象として識別されており、システムレベルのコマンドの無断実行と持続的なバックドア配布を可能にします。中国関連の APT と疑われる攻撃者は AquaShell Malware を使用しました

。これは、認証されていない HTTP POST リクエストを通じてエンコードされたコマンドを処理する軽量の Python ベースプログラムです。2025 年 11 月末から検出されたこの攻撃は、また、逆トンネリング作業のために AquaTunnel と Chisel、ログ削除のために AquaPurge を使用しました。侵害されたインスタンスは、しばしば Cisco の勧告で言及された非標準構成を含んでいました。攻撃方法には AquaTunnel を通じたリバース SSH トンネリングと Chisel を通じたトラフィックプロキシが含まれ、ネットワーク内での横移動を容易にしました。AquaShell はエンコードされた形で配信され、ウェブサーバーファイルに埋め込まれ、コマンドはデコードプロセスを経てシステムシェルで実行されました。これらのツールと戦術は、知られている中国 APT 技術と一致し、脅威の洗練さと影響を強化します。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. 非標準構成環境の悪用
   b. Cisco Secure Email Gateway の侵害
2. [Execution] Command and Scripting Interpreter: Unix Shell (T1059.004)
   a. システムレベルでのコマンド実行
   b. AquaShell バックドアの配布
3. [Persistence] Implant Internal Image (T1525)
   a. Web サーバーファイルへの AquaShell の挿入
   b. エンコードされたデータブロブの使用
4. [Defense Evasion] Indicator Removal on Host (T1070)
   a. AquaPurge を介したログの削除
   b. 特定のログ項目の削除
5. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. AquaShell 基盤の HTTP POST 通信
   b. デコードされたコマンドの受信および実行
6. [Command and Control] Non-Standard Port (T1571)
   a. AquaTunnel を利用したリバース SSH 接続
   b. Chisel プロキシを介したトラフィック中継
7. [Command and Control] Protocol Tunneling (T1572)
   a. AquaTunnel 基盤のトンネリング
   b. Chisel を利用した内部ネットワークへのピボット

22) SectorB129 used Group Policy to Deploy Malware in Gov Networks (2025-12-18)

https://cti.nshc.net/events/view/21140

攻撃対象産業群: 政府・行政

2024 年初、研究員たちは東南アジア政府機関のネットワークで以前に文書化されていない Malware を発見し、これは新たに確認された中国関連 APT グループによるものと推定される。このグループはサイバースパイ活動を目的として東南アジアと日本の政府機関を特定の対象としており、少なくとも 2023 年 9 月から活動してきた。このグループは Malware 配布と侵害されたネットワーク内の側面移動のためにグループポリシーを使用し、Microsoft OneDrive や Google Drive のようなクラウドサービスをコマンド＆コントロール通信に活用する。このグループは主に C#/.NET アプリケーションで構成されたカスタムツールセットを運用に使用する。主要なツールには、追加の侵害対象を識別するためにブラウザ履歴を収集する NosyHistorian と、クラウドストレージを C2 に使用し AppDomainManager 注入を通じて Malware を実行するバックドアである NosyDoor がある。他のツールには、ブラウザデータを抽出する NosyStealer、ペイロード配信のための NosyDownloader 、キーロガーである NosyLogger、そしてオープンソースリバースプロキシである ReverseSocks5 がある。この組織の TTP は、既知の脅威行為者との重複性を示すが、グループポリシー使用のような独特の技術を含んでいる。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 悪性添付ファイルの配信
   b. 電子メールを基盤とした初期侵入
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. PowerShell スクリプトの実行
   b. 難読化されたコマンドの実行
3. [Persistence] Domain Policy Modification: Group Policy Modification (T1484.001)
   a. グループポリシーを通じたマルウェア配布
   b. ドメイン環境内での持続的な実行の維持
4. [Defense Evasion] Obfuscated Files or Information: Encrypted/Encoded File (T1027.013)
   a. ペイロードの暗号化
   b. Base64 エンコーディングの使用
5. [Defense Evasion] Masquerading: Match Legitimate Name or Location (T1036.005)
   a. 正規ファイル名およびパスへの偽装
   b. グループポリシーオブジェクトへの偽装
6. [Defense Evasion] Signed Binary Proxy Execution (T1218)
   a. UevAppMonitor.exe の悪用
   b. LOLBins を基盤とした実行
7. [Defense Evasion] Process Injection (T1055)
   a. 正規プロセスへのインジェクション

b. CreateRemoteThread の使用

8. [Discovery] Browser Information Discovery (T1217)
   a. ブラウザ履歴の収集
   b. 追加侵入対象の識別
9. [Discovery] System Information Discovery (T1082)
   a. システムメタデータの収集
   b. ホスト環境の把握
10. [Collection] Input Capture: Keylogging (T1056.001)
   a. キー入力の収集
   b. クリップボードデータの収集
11. [Collection] Screen Capture (T1113)
   a. 画面アクティビティのキャプチャ
   b. オーディオおよびビデオの収集
12. [Command and Control] Web Service: Bidirectional Communication (T1102.002)
   a. OneDrive を基盤とした C2 通信
   b. Google Drive を通じた双方向通信
13. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 収集データの送信
   b. 暗号化されたチャネルの使用

23) SectorC01 used Phishing Pages for Credential Harvesting (2025-12-17)

https://cti.nshc.net/events/view/21098

攻撃対象産業群: 物流、政府・行政、国防、シンクタンク

2024 年 6 月から 2025 年 4 月の間に、国家支援を受けた脅威行為者がウクライナのウェブメールサービスである UKR.NET のユーザーを対象に資格情報収集キャンペーンを実施しました。このキャンペーンは以前の作戦に基づき、ユーザー名、パスワード、二要素認証コードを収集するためのフィッシング活動を含んでいました。攻撃者は Mocky、DNS EXIT のような無料ウェブサービスにホスティングされた偽の UKR.NET ログインポータルと、ngrok、Serveo のようなプロキシトンネリングプラットフォームを使用しました。これらのページにリンクする PDF 誘引がメールフィルタリングを回避するために配布されました。JavaScript を活用してページは資格情報をキャプチャし、指定されたドメインに送信しました。攻撃者はインフラの除去に対応して、侵害されたルーターから ngrok トンネルに切り替えることで適応しました。2025 年のアップデートには、新しいインフラ層と ngrok のサブドメインの使用が含まれていました。法執行の圧力にもかかわらず、このキャンペーンは継続され、ウクライナ紛争中のロシア軍事目標を支援するための情報収集に対する GRU の継続的な関心を強調しています。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. PDF 誘引資料内リンクの配布
   b. 偽の UKR.NET ログインページへの誘導
2. [Credential Access] Input Capture: Credentials from Web Forms (T1056.004)
   a. フィッシングログインフォームを通じた資格情報入力の誘導
   b. ユーザーアカウント、パスワード、2FA コードの収集
3. [Command and Control] Web Service: Bidirectional Communication (T1102.002)
   a. Mocky および DNS EXIT 基盤のデータ中継
   b. ngrok および Serveo トンネルを通じた通信の維持
4. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. HTTP/HTTPS 基盤のデータ転送
   b. ngrok サブドメインを通じたインフラの隠蔽

24) SectorC05 used Misconfigured Devices in Energy Sector Campaign (2025-12-16)

https://cti.nshc.net/events/view/21124

攻撃対象産業群: エネルギー

2021 年から 2025 年まで、ある国家と連携したサイバーキャンペーンは、誤って構成されたネットワークエッジデバイスを利用して主要インフラ部門内の組織のネットワークに初期アクセスを試みた。特に北米とヨーロッパ全域のエネルギー産業を主要なターゲットとした。脆弱性の悪用からデバイス構成エラーの悪用へと戦術を転換することで、被害インフラ内での露出リスクを減らしながら、効率的な資格情報収集と側面移動が可能になった。このキャンペーンは、誤って構成されたルーター、VPN 集約装置、クラウドホスティングプロジェクトを活用し、パケットキャプチャとトラフィック分析を通じて資格情報を傍受し、体系的な資格情報再利用攻撃を実行した。主要な損傷デバイスはクラウドプラットフォームにホスティングされており、中東を含む複数の地域にわたるグローバルな脅威の範囲を強調した。他の知られた作戦との関連があり、より大規模な協力された努力があることを示唆している。このキャンペーンは、ターゲットとした主要インフラドメイン内で持続可能なアクセスと運用を重視する戦略的転換を示している。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. ネットワークエッジデバイスの構成エラーの悪用
   b. クラウドホスティングインフラへの侵入
2. [Credential Access] Network Sniffing (T1040)

a. パケットキャプチャの実行
b. 認証トラフィックの分析
3. [Credential Access] Credentials from Network Traffic (T1557)
a. 平文認証情報の傍受
b. セッション資格情報の収集
4. [Lateral Movement] Use Alternate Authentication Material (T1550)
a. 取得した資格情報の再利用
b. オンラインサービスへの認証試行
5. [Persistence] Valid Accounts (T1078)
a. 有効なアカウントに基づく持続的アクセス
b. 侵害されたインスタンスとの継続的な相互作用
6. [Defense Evasion] Indicator Removal on Host (T1070)
a. フォレンジック痕跡の削除
b. 収集データの暗号化
7. [Collection] Data from Information Repositories (T1213)
a. 構成ファイルの収集
b. 侵害システムデータへのアクセス
8. [Command and Control] Non-Application Layer Protocol (T1095)
a. TFTP を基盤としたデータ転送
b. 侵害サーバーを用いたプロキシ活用

25) SectorC08 exploited WinRAR Vulnerability in Phishing Campaign (2025-12-05)

https://cti.nshc.net/events/view/20782

攻撃対象産業群: 政府・行政、軍事機関

2025 年にウクライナ政府部門を対象とした精巧なサイバー攻撃キャンペーンが進行中である。このキャンペーンは WinRAR の CVE-2025-8088 と名付けられた脆弱性を利用してスピアフィッシング攻撃を実行する。脅威行為者はスピアフィッシングメールを使用して特別に作成された RAR アーカイブを配布し、ディレクトリトラバーサルの欠陥を悪用して解凍時に悪性ペイロードを配布する代替データストリームを使用する。この初期攻撃は、ユーザーログイン時に実行を通じて持続性を確保するスタートアップディレクトリ内 HTA ファイルの静かな生成を引き起こす。その後、HTA は mshta.exe プロセスを使用して PDF 文書に偽装した追加スクリプトを検索し実行するダウンローダーとして機能する。これらのスクリプトは主に VBScript で、文字置換と Base64 エンコーディングを通じて非常に難読化され、検出を複雑にする。スタートアップディレクトリの使用に加えて、この攻撃は合法的なサービスを模倣したスケジュールされたタスクを通じて持続性を確立する。このキャ

ンペーンは多層的持続性戦略と、秘密裏の情報収集およびデータ流出活動を保証する強力な C2 通信を特徴とする。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. スピアフィッシングメールの送信
   b. 悪性 RAR アーカイブの添付
2. [Execution] User Execution: Malicious File (T1204.002)
   a. RAR アーカイブの解凍
   b. 開始ディレクトリ内への HTA ファイル生成
3. [Persistence] Boot or Logon Autostart Execution: Startup Folder (T1547.001)
   a. スタートアップディレクトリへの HTA ファイル配置
   b. ユーザーログイン時の自動実行
4. [Execution] Command and Scripting Interpreter: VBScript (T1059.005)
   a. HTA ベースのダウンローダー実行
   b. mshta.exe を通じたスクリプト実行
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. VBScript 文字置換による難読化
   b. Base64 エンコーディングの使用
6. [Persistence] Scheduled Task/Job: Scheduled Task (T1053.005)
   a. 予約タスクの作成
   b. 正規サービスへの偽装
7. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. ハードコードされた C2 ドメインとの通信
   b. 複数 C2 アドレスの活用

26) SectorC13 used Phishing Emails to Exploit Microsoft Office Vulnerability (2025-12-19)

https://cti.nshc.net/events/view/21150

攻撃対象産業群: 政府・行政、通信、建設

2025 年初、精巧なサイバー脅威がロシアとベラルーシのいくつかの産業を対象とした。これらの産業には、通信、建設、政府、工場が含まれる。攻撃は DOC(X)添付ファイルが含まれたフィッシングメールを通じて開始された。これらの添付ファイルは開かれると、悪性 RTF ファイルをダウンロードし、Microsoft Office Equation Editor の CVE-2018-0802 を悪用して HTML アプリケーション(HTA)ファイルを実行した。感染チェーンは VBShower、PowerShower、VBCloud のようなイン

プラントを含んでいた。VBShower はバックドアを配布し、追加のペイロードをインストールし、システムデータを収集するプロセスを開始した。これは予約されたタスクを生成し、スクリプトを使用して感染したシステムから情報を抽出した。このグループは VLC メディアプレーヤーを活用して DLL ハイジャック技法を実行し、バックドアをインストールした。VBCloud と PowerShower はそれぞれ独立したバックドアとして動作し、クラウドサービスを利用してコマンド＆コントロール通信、データ窃盗、追加ペイロード配布を行った。両バックドアは検出を避け、攻撃者のコマンドを実行するために複雑な暗号化および復号化技法を使用した。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
a. DOC(X) 添付ファイルを含むフィッシングメールの配信
   b. 悪意のある RTF ファイルのダウンロード誘導
2. [Execution] Exploitation for Client Execution (T1203)
   a. Equation Editor 脆弱性 (CVE-2018-0802) 悪用
   b. HTA ファイル実行
3. [Execution] Command and Scripting Interpreter: VBScript (T1059.005)
a. VBShower スクリプト実行
   b. 追加ペイロードロード
4. [Persistence] Scheduled Task/Job: Scheduled Task (T1053.005)
   a. 予約タスクの作成
   b. バックドア自動実行維持
5. [Persistence] Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
   a. VLC Media Player DLL ハイジャッキング
b. Malware DLL ロード
6. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. ペイロード暗号化
   b. 暗号化および復号化ルーチンの適用
7. [Credential Access] Credentials from Password Stores: Web Browsers (T1555.003)
   a. ブラウザ保存資格情報窃取
   b. クッキーおよびパスワード収集
8. [Discovery] System Information Discovery (T1082)
   a. システムプロセス情報収集
   b. プロキシ設定確認
9. [Collection] Data from Local System (T1005)
   a. ローカルファイル収集
   b. ネットワークドライブファイルアクセス

10. [Command and Control] Web Service: Bidirectional Communication (T1102.002)
    a. クラウドサービス基盤 C2 通信
    b. ペイロードおよびコマンド交換
11. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. データ収集の送信
    b. HTTP POST ベースの流出

27) SectorC14 used AiTM JavaScript for Phishing ProtonMail Logins (2025-12-03)

https://cti.nshc.net/events/view/20741

攻撃対象産業群: 国防、軍事機関、非政府組織(NGO)、シンクタンク

2025 年 5 月と 6 月の間に、ロシアと連携したサイバー侵入グループがウクライナを支援する戦略的部門を狙い、複数の機関を対象にスピアフィッシング攻撃を実行しました。特に、彼らはフランスのある非政府組織(NGO)と他の機関を対象に、添付ファイルがない合法的に見える ProtonMail アドレスからメールを送り、被害者がファイルを要求するよう誘導する戦術を使用しました。これは、被害者が損傷したサイトに接続するリンクが含まれた 2 次メールを受け取り、ProtonDrive URL に接続するマルウェア PDF をダウンロードさせるものでした。これらの PDF は、被害者を損傷したウェブサイトにホスティングされたリダイレクターを通じてフィッシングキットに案内しました。フィッシングキットは Adversary-in-The-Middle 手法と JavaScript 注入を使用して ProtonMail のログインページを改ざんし、ログイン資格情報を捕捉し、二要素認証プロセスを処理しました。フィッシングインターフェースのエラーにもかかわらず、資格情報の捕捉に成功し、非認可ログインが行われました。Namecheap と Regway を通じて登録されたドメインとサーバーは脅威行為者と関連し、ロシアの利益に反する機関を狙うグループの過去の戦術と一致するパターンを明らかにしました。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
    a. ProtonMail アドレスを利用した一次メールの送信
    b. リダイレクタリンクを含む二次メールの転送
2. [Execution] User Execution: Malicious File (T1204.002)
    a. ProtonDrive の URL を通じた悪性 PDF のダウンロード
    b. PDF 閲覧時にフィッシングサイトへの遷移
3. [Credential Access] Adversary-in-the-Middle (T1557.002)
    a. ProtonMail ログインページへの JavaScript 注入
    b. アカウント資格情報および 2FA トークンの奪取
4. [Command and Control] Web Service: Bidirectional Communication (T1102.002)
    a. 侵害された Web サイトをリダイレクターとして使用

b. API エンドポイントを通じた資格情報の伝達

5. [Exfiltration] Exfiltration Over Web Service (T1567.002)
   a. 奪取された資格情報を外部サーバーへ送信
   b. 攻撃者が制御するインフラへのデータ送信

28) SectorC21 used Custom Backdoor and Loader Malware (2025-11-28)

https://cti.nshc.net/events/view/20601

攻撃対象産業群: 政府・行政、外交

2025 年初、政治および外交的目標を狙った外務省と政府間機関に対する精巧なサイバー脅威が発生した。攻撃は、事務文書に偽装したパスワードで保護されたアーカイブを含むフィッシングメールを使用して感染を開始した。実行時、これらのファイルは Rust、Go、C/C++、Python といった言語で書かれた複数のインプラントを配布した。これらのインプラントはリモートシェルアクセスを可能にし、AdaptixC2 や Havoc のような事後搾取フレームワークをダウンロードするために使用され、オペレーションの柔軟性と難読化を強化した。主要な戦術には、Telegram や Discord のような公共プラットフォームをコマンド＆コントロール通信に使用し、悪意のある活動を合法的なネットワークトラフィックに偽装して検出を回避することが含まれていた。リバースシェルはシステムデータを収集し、コマンドをリモートで実行し、Tomiris ReverseShells や FileGrabber のようなカスタムツールを含め、持続性とデータ窃取のための追加プロセスを配布した。多言語マルウェアモジュールに重点を置いた攻撃は、検出回避と持続性を維持するための戦略的変化であり、特に公共 C2 チャンネルを活用してより大きな慎重さを図ることに重点を置いている。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. パスワードで保護されたアーカイブを添付したメールの送信
   b. 文書に偽装された実行ファイルの配布
2. [Execution] User Execution: Malicious File (T1204.002)
   a. 二重拡張子を用いた実行ファイルの実行
   b. インプラント初期ローダーの実行
3. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. PowerShell スクリプトの実行
   b. 追加命令およびペイロードのロード
4. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder (T1547.001)
   a. Run レジストリキーへの登録
   b. ブート後の自動実行の維持

5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. PyArmor を基盤としたコード難読化
   b. 長いファイル名および拡張子による偽装
6. [Discovery] System Information Discovery (T1082)
   a. システム情報の収集
   b. ネットワーク構成の確認
7. [Collection] Data from Local System (T1005)
   a. 特定拡張子ファイルの探索
   b. ファイルパスリストの収集
8. [Command and Control] Web Service: Bidirectional Communication (T1102.002)
   a. Telegram を基盤とした C2 通信
   b. Discord を基盤とした C2 通信
9. [Exfiltration] Exfiltration Over Web Service: Cloud Storage (T1567.002)
   a. 収集データの Discord 送信
   b. HTTP POST を用いたデータ漏洩
10. [Lateral Movement] Proxy: Internal Proxy (T1090.001)
    a. リバース SOCKS プロキシの構成
    b. プロキシトラフィックを通じた内部移動

29) SectorC30 used OAuth Phishing disguised as Security Events (2025-12-04)
https://cti.nshc.net/events/view/20783

2025 年初頭、サイバー脅威行為者たちが Microsoft 365 OAuth とデバイスコード認証を悪用してユーザーアカウントを奪取するキャンペーンを開始し、精巧なフィッシング手法を通じて複数の機関を標的にしました。ベオグラード安全保障会議とブリュッセルインド-太平洋対話を含む国際セキュリティイベントを模倣した偽のウェブサイトが、ユーザー資格情報を取得するための口実として作成されました。攻撃は OAuth ワークフローに接続されるリンクを含むスピアフィッシングメールを含み、被害者が知らないうちに OAuth トークンを共有するよう要求しました。ある事件では、攻撃者が WhatsApp を通じて被害者に連絡し、信頼を築いた後にフィッシングを試みました。資格情報の奪取に成功した後、脅威行為者たちは様々なデータにアクセスし、合法的なユーザーデバイスを模倣した詐欺デバイスを登録して持続性を維持しました。キャンペーンは奪取されたアカウントを使用して追加の標的をフィッシングすることでさらに拡大しました。この作戦はメッセージングアプリを通じた長期的な関与戦術と精巧に作成されたフィッシングサイトを活用し、2025 年に活発に標的を奪取する資源が豊富で熟練した脅威行為者を示しています。

[Attack Flow]

30) SectorD02 used Backdoor Malware disguised as Snake Game (2025-12-02)

https://cti.nshc.net/events/view/20722

攻撃対象産業群: 製造、技術、学界 - 大学、政府・行政、運送、工学

最近のサイバー諜報キャンペーンでは、脅威行為者は主にイスラエルの組織を標的にし、エジプトで1件の事件が発生しました。この作戦は、検出回避と持続性を強化するために、以前に文書化されていないツールセットを配布することを含んでいました。主要なツールには、MuddyViperというC/C++バックドアを実行するFooderローダーがあり、これはSnakeゲームに偽装しています。このローダーは、検出を避けるためにカスタム遅延関数などの洗練された技術を使用します。MuddyViperは、データ収集、コマンド実行、Windowsログイン資格情報およびブラウザーデータの漏洩を容易にします。このキャンペーンはまた、CE-NotesやLP-Notesのような資格情報窃取ツールと、go-socks5のようなリバーストンネリングツールを使用しました。攻撃者は暗号化のためにCNGという次世代Windows暗号化APIを使用する高度な技術を採用しており、これは類似の脅威行為者の間では珍しいことです。キャンペーンのインフラは、AmazonやDigitalOceanのようなプラットフォームにホスティングされたステージングおよびコマンド制御サーバーを含み、以前のキャンペーンに比べて攻撃の洗練度を大幅に向上させました。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 文書に偽装したマルウェア添付ファイルの配布
   b. メールを通じたユーザー実行の誘導
2. [Execution] User Execution: Malicious File (T1204.002)
   a. Snakeゲームに偽装したローダーの実行
   b. Fooderローダーを通じたMuddyViperのロード
3. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.003)
   a. システムコマンドの実行
   b. 後続コマンドの処理
4. [Persistence] Boot or Logon Autostart Execution: Scheduled Task (T1053.005)
   a. 予約タスクの作成
   b. 再起動後の自動実行維持
5. [Privilege Escalation] Access Token Manipulation (T1134)
   a. アクセストークンの偽装
   b. DuplicateTokenEx APIの使用
6. [Defense Evasion] Obfuscated Files or Information (T1027)

a. 文字列の難読化
b. リフレクティブローディング方式の使用
7. [Credential Access] Input Capture (T1056)
a. 偽の Windows セキュリティウィンドウの表示
b. ログイン資格情報の収集
8. [Discovery] System Information Discovery (T1082)
a. 実行中プロセスの列挙
b. セキュリティ製品の存在確認
9. [Collection] Data from Local System (T1005)
a. ブラウザデータの収集
b. 資格情報のローカル保存
10. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
a. HTTPS を基盤とした C2 通信
b. CNG を基盤とした暗号化通信
11. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. HTTPS を通じたデータ流出
b. go-socks5 を利用したリバーストンネリング

31) SectorD02 delivered UDPGangster Malware via Phishing Lures (2025-12-04)
https://cti.nshc.net/events/view/20785

UDP ベースのバックドア型マルウェアである UDPGangster に関連するサイバー脅威事案が、トルコ、イスラエル、アゼルバイジャンの Microsoft
Windows 利用者を標的として発生した。本マルウェアは、主に VBA マクロを含む悪意のある Microsoft
Word 文書を添付したフィッシングメールを通じて配布され、感染したシステムに対する遠隔操作を可能にする。これらのフィッシングメールは、北キプロス・トルコ共和国外務省を装い、「大統領選挙とその結果」をテーマとしたセミナー招待を装った内容となっている。受信者が文書内のマクロを有効化するとマルウェアが実行され、持続性を確立した上で、コマンド実行、ファイル流出、追加ペイロードの配布といった機能を UDP 通信を通じて実行する。UDPGangster は、デバッガ、仮想マシン、サンドボックス環境の検出などを含む高度な解析回避技術を実装しており、検知を回避する設計となっている。本キャンペーンにおいて確認されたマクロベースのドロッパーの一貫した使用と、広範な検知回避ルーチンの実装は、高度な脅威アクターの関与を示唆するものであり、本マルウェアは攻撃者に対してシステム制御および情報収集能力を提供し、スパイ活動や後続攻撃を容易にする。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 外務省主催セミナー招待を装ったフィッシングメールの送信
   b. VBA マクロを含む Word 文書の添付
2. [Execution] User Execution: Malicious File (T1204.002)
   a. 「コンテンツの有効化」クリックによるマクロ実行
   b. マクロを通じた UDPGangster ローダーの実行
3. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Base64 を基盤としたペイロードのデコード
   b. デバッガ・仮想環境・サンドボックスの検出
4. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
   a. レジストリ Run キーへの登録
   b. スタートアップフォルダへのマルウェア配置
5. [Command and Control] Application Layer Protocol: Non-Standard Protocol (T1071.004)
   a. UDP ベースの C2 通信の使用
   b. コマンド受信および実行結果の送信
6. [Collection] Data from Local System (T1005)
   a. システム情報の収集
   b. ローカルファイルの収集
7. [Exfiltration] Exfiltration Over Alternative Protocol (T1048)
   a. UDP チャネルを通じたデータ流出
   b. エンコードされたデータの転送

32) SectorD05 used Exchange ProxyShell for Diplomatic Espionage (2025-11-22)

https://cti.nshc.net/events/view/20398

攻撃対象産業群: 政府・行政、通信、エネルギー、外交

2025 年 10 月、流出した内部文書により、組織化されたサイバー作戦部隊が広範な諜報活動に関与している実態が明らかになった。当該部隊は、官僚的な軍事体系の内部に位置付けられた正式なワークフローを特徴としていた。この部隊は主に、中東およびアジアの一部地域における外交機関、政府機関、企業ネットワークへの侵入を目的として、Exchange の脆弱性を悪用する一貫したサイバー攻撃手法に注力していた。作戦は月次の成果レビューを通じて詳細に文書化されており、フィッシング成功率や脆弱性悪用指標が精緻に記録され、資格情報の収集および情報抽出の状況を追跡する包括的な報告書として整理されていた。部隊内部では、脆弱性開発、資格情報の再利用、フィッシングキャンペーンの実施、侵害されたメールボックスのリアルタイム監視といった機能ごとに専門チームが分離されていた。2022 年 5 月に開始された重要なキャンペーンでは、広範な偵察活動と標的指向の事

後悪用を組み合わせ、グローバルアドレス一覧（GAL）の収集、フィッシングに用いる連絡先の武器化、長期的な情報収集の維持が行われていた。これらの文書には、機会主義的な攻撃ではなく、戦略的な情報収集を重視する体系的なサイバー作戦アプローチが明確に示されていた。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. Exchange サーバー脆弱性の悪用
   b. 管理者エンドポイントへのアクセス
2. [Persistence] Server Software Component: Web Shell (T1505.003)
   a. ASP.NET Web シェルのアップロード
   b. 予測可能なパスへの Web シェル配置
3. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. PowerShell スクリプトの実行
   b. リモートコマンドの実行
4. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
   a. システム権限昇格脆弱性の悪用
   b. LSASS メモリへのアクセス
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. スクリプト置換によるエンコーディング
   b. 正規サービスへの偽装
6. [Credential Access] OS Credential Dumping (T1003)
   a. LSASS ダンプの生成
   b. 資格情報の抽出
7. [Discovery] System Network Connections Discovery (T1049)
   a. 内部ネットワーク接続の確認
   b. 側面移動対象の探索
8. [Lateral Movement] Remote Services (T1021)
   a. RDP セッションの使用
   b. SMB 管理者共有へのアクセス
9. [Collection] Email Collection: Local Email Collection (T1114.001)
   a. GAL アドレス帳の収集
   b. メールボックス内容の収集
10. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
    a. HTTP(S)を基盤とした C2 通信
    b. ヘッダーフィールドを利用したコマンド受信
11. [Exfiltration] Exfiltration Over Web Service: Cloud Storage (T1567.002)

a. 暗号化された圧縮ファイルの生成
b. クラウドストレージを用いたデータ転送

33) SectorD05 used Phishing Pages with Western University Branding (2025-12-16)

https://cti.nshc.net/events/view/21099

攻撃対象産業群: 国防

Sophisticated cyber threat incidents reveal how state-sponsored groups organize cyber espionage and sabotage activities through meticulous administrative procedures similar to official government operations, rather than traditional hacker groups. 政治的動機で知られるこのグループは、主にイスラエル機関を対象に、諜報と心理戦術を組み合わせて攻撃します。 Episode 4 と名付けられたこの事件は、調達および運用物流を詳細に説明するスプレッドシートを通じて広範なインフラを明らかにし、Cryptomus を通じたビットコインのような暗号通貨を使用して密かに作戦を資金調達します。 このグループは、ヨーロッパのリセラーを通じて低コストの VPS ホスティングを取得し、ProtonMail を通じて使い捨てのメール ID を生成し、フィッシングおよび影響力作戦を目的としたドメインを登録する多層的アプローチを使用します。 これらのドメインとインフラは、活動を隠蔽するために合法的な機関を模倣します。 これらの暴露は、高度な技術的即興性よりも行政的規律と官僚的システムに依存するグループの姿を強調し、もっともらしい否認可能性の下で諜報を支援する組織的な構造を示しています。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. 求職・採用関連内容を装ったフィッシングページの配信
   b. 正規機関を詐称したドメインによるユーザー誘導
2. [Execution] User Execution (T1204)
   a. フィッシングページ上でのユーザー操作の誘導
   b. 資格情報入力プロセスの発生
3. [Credential Access] Valid Accounts (T1078)
   a. 窃取されたアカウント情報の使用
   b. 電子メールおよび各種サービスアカウントへのアクセス
4. [Persistence] Account Manipulation (T1098)
   a. 侵害されたアカウントの継続的な使用
   b. アクセス維持を目的としたアカウント管理
5. [Defense Evasion] Masquerading (T1036)
   a. 正規機関・採用ブランドへの偽装
   b. 正常なサービスおよびドメイン形態の模倣

6. [Collection] Email Collection (T1114)
   a. メールボックスへのアクセス
   b. 内部メールデータの収集
7. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. VPS を基盤とした C2 サーバーの運用
   b. HTTP(S)通信の使用
8. [Exfiltration] Exfiltration Over Web Service: Cloud Storage (T1567.002)
   a. 外部 Web サービスへのデータ転送
   b. 収集情報の外部インフラへの移転
9. [Impact] Defacement / Psychological Operations (T1491)
   a. 情報公開サイトの運営
   b. 心理的圧迫を目的とした露出活動

34) SectorD09 used Foudre malware disguised as Excel files (2025-12-18)

https://cti.nshc.net/events/view/21188

攻撃対象産業群: 政府・行政、非政府組織(NGO)、社会運動団体

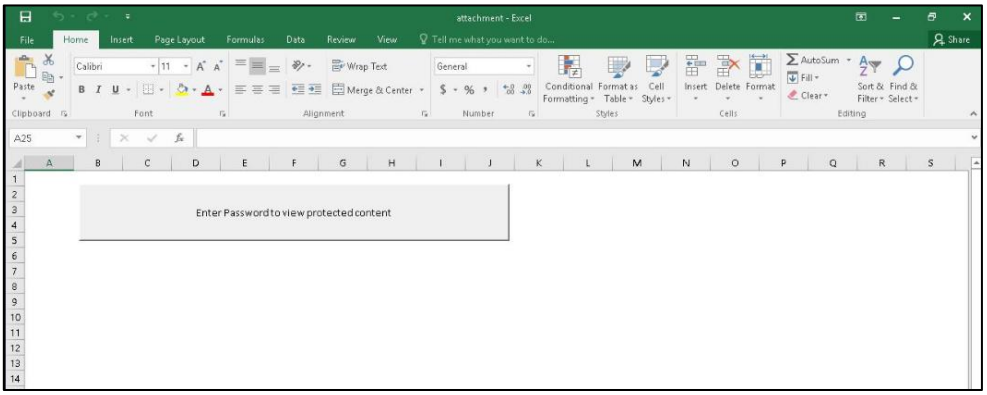
国家支援を受ける脅威行為者が数年間、主に様々な Malware を使用してグローバルネットワークと重要インフラ、そしてイラン反体制派を標的にしてきた。2000 年代初頭から活動してきたこのグループは、複数の名前で呼ばれ、最近では運用セキュリティと技術的能力を強化して再登場した。最新の研究は過去 3 年間の活動に関する重要な情報を明らかにし、広範な Malware 使用とコマンド＆コントロール（C2）インフラを示している。2016 年以降、複数のキャンペーンが様々な Malware 変種、特に Foudre と Tonnerre を使用して識別された。最近のキャンペーンには、C2 サーバーと通信するドメイン生成アルゴリズム（DGA）を使用する少なくとも 3 つのアクティブな変種が含まれる。新たに識別された Tonnerre 変種は、C2 指示を Telegram ボット API を通じてリダイレクトし、以前のプロトコルを置き換える高度な搾取技術を示唆している。分析者たちは、被害者データと通信ログのための特定のディレクトリを含むグループの広範な C2 サーバーインフラを発見した。Malware 偽装、データ窃取、C2 運用の高度な技術はグループの適応力を示している。これらの作戦は目立たないように隠されており、彼らの持続的な関連性と脅威を強調している。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. マクロを含む Excel 文書をメールに添付
   b. ドキュメント内に実行ファイルを含有
2. [Execution] User Execution: Malicious File (T1204.002)
   a. Excel ドキュメントの閲覧

b. 埋め込み実行ファイルの実行

3. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
   a. レジストリ自動実行キーへの登録
   b. 再起動後のマルウェア自動実行
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. MP4 ファイルへの偽装
   b. 暗号化された SFX ファイルの使用
5. [Discovery] System Information Discovery (T1082)
   a. システム GUID の収集
   b. ユーザー名およびホスト名の収集
6. [Collection] Data from Local System (T1005)
   a. 被害者ファイルの収集
   b. ローカルデータの整理および準備
7. [Command and Control] Web Service: Bidirectional Communication (T1102.002)
   a. Telegram Bot API を通じたコマンド受信
   b. DGA を基盤としたドメインを通じた C2 接続
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 収集データの C2 サーバー転送
   b. サーバー内指定ディレクトリへの保存
9. [Impact] Data Destruction (T1485)
   a. 削除コマンドの実行
   b. プロセス終了およびファイルの削除



[図 3: SectorD09 グループが活用したミキ文書]

35) SectorE01 used StreamSpy Malware disguised as PDF files (2025-12-02)

https://cti.nshc.net/events/view/20720

攻撃対象産業群: 産業、政府・行政、軍事機関、電気、外交

アジア地域を主に標的とするサイバースパイキャンペーンが識別されており、長期間活動している脅威グループと関連する StreamSpy というトロイの木馬を活用します。このグループは WebSocket および HTTP プロトコルのようなリモート通信チャネルを悪用し、「stream」を含むサーバーインターフェースと WebSocket 接続を設定し、結果を実行および受信します。トロイの木馬は PDF 文書に偽装した ZIP ファイルを通じて配布され、ユーザーがマルウェアを実行するよう誘導します。実行時、StreamSpy はネットワーク、アイデンティティ、および持続性の詳細を含む構成データを解読し、「www.mydropboxbackup[.]com」と接続された C2 サーバーと接続されます。このマルウェアはホスト名、オペレーティングシステムバージョン、およびハードウェア識別子を含むシステム詳細を収集し、C2「/[prefix]/auth"呈」に送信される固有デバイス識別子に統合します。持続性のために、スケジュールされたタスク、レジストリの修正、またはスタートアップディレクトリの LNK ファイルの生成などを通じて組み込まれます。特に、StreamSpy の C2 との相互作用は、定期的なハートビートアップデートとエンコードされた WebSocket ストリームを通じたコマンド実行を含み、リモートコマンド実行およびファイル転送を可能にします。これはグループの以前のマルウェアと機能が類似しており、脅威行為者間の継続的な進化とリソース共有を示しています。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. PDF 文書に偽装した ZIP ファイルをメールに添付
   b. ユーザー実行誘導を通じたマルウェアファイルの配布
2. [Execution] User Execution: Malicious File (T1204.002)
   a. PDF アイコンに偽装した実行ファイルの実行
   b. StreamSpy 初期ローダーの実行
3. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
   a. 予約タスクの作成
   b. レジストリ Run/RunOnce キーの修正
   c. スタートアップフォルダへの LNK ファイル生成
4. [Defense Evasion] Masquerading (T1036)
   a. 正規 PDF ファイルに偽装した実行ファイルの使用
   b. ファイルアイコンおよび名称の偽装
5. [Discovery] System Information Discovery (T1082)
   a. ホスト名およびオペレーティングシステム情報の収集
   b. WMI を基盤としたハードウェア識別子の収集
6. [Collection] Data from Local System (T1005)

a. システムおよび環境構成情報の収集
b. デバイス固有識別子の生成
7. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
a. WebSocket を基盤とした命令受信および実行
b. HTTP を基盤としたファイル転送
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. デバイス識別子および収集情報の C2 送信
b. コマンド実行結果の WebSocket ストリームによる返却

36) SectorE04 used DLL Side-Loading disguised as Income Tax Portals (2025-12-19)

https://cti.nshc.net/events/view/21219

攻撃対象産業群: 健康、소매

最近、精巧なサイバースパイキャンペーンがインド所得税部門を装い、インドの機関を標的にしました。この攻撃は主にサービス、小売、通信、医療部門のアジア企業を集中的に狙いました。脅威行為者は合法的な Microsoft Defender バイナリを使用した DLL サイドローディング技法を活用して検出を回避しました。評判ベースの防御を回避するために、公共クラウドストレージと URL 短縮器を使用しました。フィッシングメールは被害者を偽の「所得税」サイトに誘導し、Malware を配信しました。このキャンペーンは Malware ペイロードの実行に合法的なバイナリを使用し、検出の試みを複雑にしました。Malware はハイジャックされた DLL を反射的にロードしてメモリで実行され、ファイルスキャンを回避しました。ジオフェンシングを使用して南アジアのタイムゾーンのシステムのみを標的にしました。この作戦は信頼できるバイナリと公共インフラをコマンド＆コントロールに活用し、高度な回避技術を示しており、精巧な行為者によって重要な部門に持続的な脅威を提起していることを示しています。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
a. インド所得税部門を装ったフィッシングメールの送信
b. URL 短縮サービスを通じた悪性 ZIP ファイルのダウンロード誘導
2. [Execution] User Execution: Malicious File (T1204.002)
a. Inspection.zip の解凍
b. 正規の Microsoft Defender 実行ファイル（SenseCE.exe）の実行
3. [Defense Evasion] Signed Binary Proxy Execution (T1218)
a. Microsoft Defender バイナリの悪用
b. MpGear.dll のサイドローディングによる悪性 DLL のロード
4. [Defense Evasion] Masquerading: Match Legitimate Name or Location (T1036.005)

a. 正規セキュリティ構成要素への偽装
b. メモリ内でのリフレクティブ DLL ローディング
5. [Defense Evasion] Virtualization/Sandbox Evasion: Time Based Evasion (T1497.003)
a. 解析回避を目的とした実行遅延
b. 仮想環境および解析ツールの検出
6. [Discovery] System Information Discovery (T1082)
a. システムプロセス情報の収集
b. 外部 API を通じたタイムゾーンの確認
7. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
a. 外部 IP アドレスへの C2 接続
b. 追加ローダーおよびシェルコードの受信
8. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
a. 常駐エージェント（mysetup.exe）の登録
b. 設定ファイルを基盤とした自動実行の維持
9. [Command and Control] Ingress Tool Transfer (T1105)
a. 追加ペイロードのダウンロード
b. 正規ツール通信プロトコルに偽装したビーコン通信

37) SectorH03 used .desktop Phishing Files to Target Indian Government (2025-11-29)

https://cti.nshc.net/events/view/20701

攻撃対象産業群: 政府・行政

インド政府機関で使用される Linux 基盤 BOSS 環境を対象とした協力されたサイバースパイキャンペーンが識別された。侵入は合法的に見えるように設計された.desktop ファイルを含むスピアフィッシングメールで始まり、これはバックグラウンドで悪性コマンドを実行する。これらのファイルは"lionsdenim[.]xyz"ドメインと IP アドレス"185.235.137[.]90"にホスティングされた悪性インフラから追加ペイロードをダウンロードする。脅威行為者たちはこのインフラを活用して ELF バイナリとシェルスクリプトを取得し、コマンドを実行し、持続性を確立する。特に、Malware は.desktop ファイルを使用して自身の作業を隠し、システムレベルの実行権限を活用し、データ流出を容易にする。このキャンペーンは持続性のために systemd サービスを使用するなどの高度な技術と重要なインフラに長期的にアクセスするためのマルチプラットフォーム戦略を活用することを示している。これは土着の運用環境を悪用する精巧で国家と連携したサイバー脅威に対する警戒と強力な防御の必要性を強調する。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 政府文書に偽装した spear phishing email 配信
   b. 悪性 .desktop ファイル添付
2. [Execution] Command and Scripting Interpreter: Unix Shell (T1059.004)
   a. .desktop ファイル 実行 時 バックグラウンド コマンド 実行
   b. Base64 デコードされたシェルスクリプト実行
3. [Execution] User Execution: Malicious File (T1204.002)
   a. ユーザーによって .desktop ファイル実行
   b. リモートインフラから ELF バイナリをダウンロードおよび実行
4. [Persistence] Create or Modify System Process: Systemd Service (T1543.002)
   a. systemd サービス生成
   b. ブート時の自動実行設定
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Base64 エンコーディングでスクリプト隠蔽
   b. PyInstaller パッケージングを通じたコード偽装
6. [Discovery] System Information Discovery (T1082)
   a. オペレーティングシステムおよびユーザー情報の収集
   b. ファイルシステム構造確認
7. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. HTTP POST 基盤 C2 通信
   b. ホスト識別用ユニーク ID 送信
8. [Collection] Screen Capture (T1113)
   a. 画面キャプチャ実行
   b. 画像ファイル生成
9. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 収集データ HTTP POST 送信
   b. ファイルアップロードを通じた外部流出

38) SectorS01 used Caminho Malware disguised as Colombian Judicial Web Portal (2025-12-16)

https://cti.nshc.net/events/view/21105

攻撃対象産業群: 政府・行政

最近のサイバー脅威キャンペーンは、フィッシングメールを利用して組織を対象に攻撃を行いました。このキャンペーンは、損傷したメールアカウントを使用して見た目には合法的なメッセージを送信

しました。これらのメールはコロンビア司法システムの法的通知を装っており、Base64 でエンコードされた HTML ページが含まれた SVG 画像を含んでいました。このページは公式ポータルのように見え、アクセス時にファイルレス攻撃チェーンを開始する JavaScript ファイルを配信しました。この攻撃チェーンは、JavaScript と PowerShell コマンドを使用して複数段階の難読化プロセスを経ました。攻撃の主要な構成要素は、画像ファイルをダウンロードし、Base64 でエンコードされたペイロードを抽出して Caminho という.NET アセンブリにロードすることでした。Caminho は Malware ダウンローダーとして、Discord からテキストファイルを取得し、MSBuild.exe を使用したプロセスハロウィングを通じて実行し、最終ペイロードである DCRAT、すなわちリモートアクセス型トロイの木馬を配信しました。DCRAT の機能は、キーロギングやディスクアクセスを含み、検出を回避するために暗号化を使用します。このキャンペーンは、Discord とさまざまな難読化技法を活用して、高度で隠密な特性を強調しました。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
   a. 司法機関の通知を装ったフィッシングメールの送信
   b. SVG 画像のクリック誘導
2. [Execution] User Execution (T1204)
   a. SVG 内部の HTML ページのロード
   b. JavaScript 実行のトリガー
3. [Execution] Command and Scripting Interpreter: JavaScript (T1059.007)
   a. 難読化された JavaScript の実行
   b. 多段階デオブフスケーションの実行
4. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. PowerShell コマンドの実行
   b. WMI を基盤としたプロセス生成
5. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. Base64 エンコーディングの使用
   b. コメントおよび文字置換を用いた難読化
6. [Defense Evasion] Signed Binary Proxy Execution: MSBuild (T1218.011)
   a. MSBuild.exe の悪用
   b. .NET アセンブリを用いたプロセスホロウイング
7. [Defense Evasion] Impair Defenses: Disable or Modify Tools (T1562.001)
   a. AMSI の回避
   b. セキュリティ検出の回避
8. [Defense Evasion] Virtualization/Sandbox Evasion (T1497)
   a. デバッガーの検出

b. 仮想環境の確認

9. [Credential Access] Input Capture: Keylogging (T1056.001)
   a. キー入力の収集
   b. ユーザー活動の記録
10. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. Discord を通じた C2 通信
   b. テキストファイルを基盤とした命令受信
11. [Command and Control] Encrypted Channel (T1573)
   a. AES を基盤とした暗号化通信
   b. C2 サーバー認証の適用

39) SectorT01 used Macro-Exploited Docs with Dynamic Captcha Evasion (2025-12-05)

https://cti.nshc.net/events/view/21055

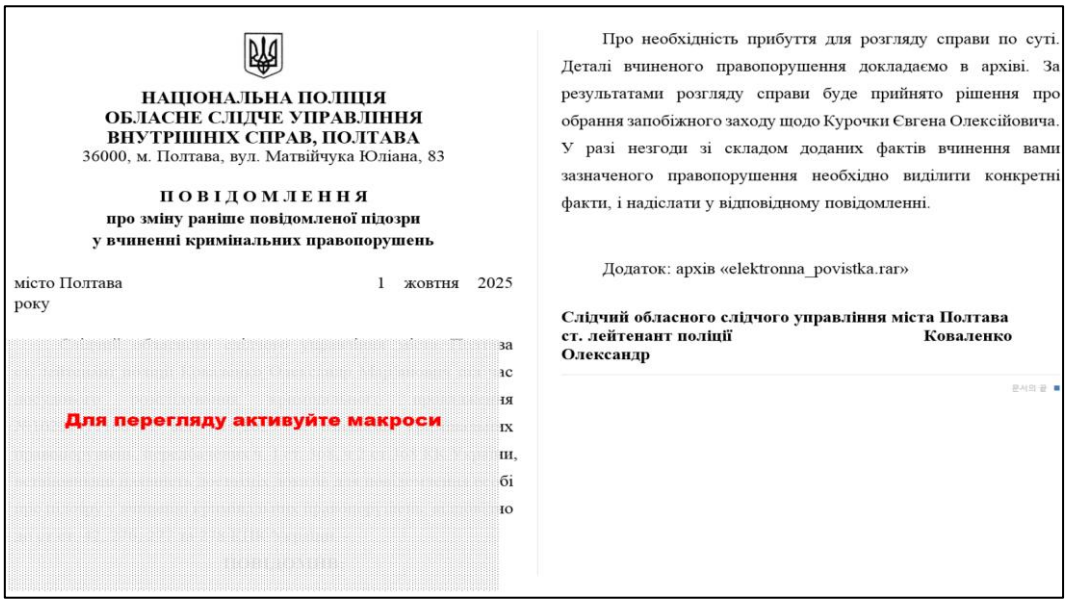
この事件は "Лист мадопомога.doc"という文書を利用した精巧なフィッシング作戦を含んでいる。この文書は分析と検出を回避するために動的 CAPTCHA を生成するローカルマクロを使用する。このフィッシング試みは文書を開くときにコードを実行し、セキュリティ対策を回避しようとする。正しい CAPTCHA 入力時に、文字列が伝達され文書の保護が解除され特定の関数が実行される。マクロはその後、餌を明らかにし、DLL ファイルを断片化して実行し、言語モデルによって自動生成されたと思われるエンコードされた詳細を含む。"EdgeService.dll"という DLL は特定のドメインに信号を送り、これは潜在的なマルウェアコマンド＆コントロール通信を示す。この攻撃はまたウクライナを狙った文書およびファイル名を使用し、マクロを活用して追加のマルウェアペイロードを実行するパターンを示している。ポーランドを狙った以前の攻撃との関連が発見され、これは他のドメインに信号を送るペイロードを含む PDF ファイルを操作したものである。この作戦は複数の地理的対象を狙った高度な難読化および分析防止技術を反映している。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. ウクライナ関連内容を装ったマルウェア文書の配布
   b. 動的 CAPTCHA を含む Word 文書の添付
2. [Execution] Command and Scripting Interpreter (T1059)
   a. ドキュメントを開く際にマクロが自動実行
   b. CAPTCHA 入力条件を満たした後に後続コードを実行
3. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. 難読化されたマクロコードの使用

b. エンコードされた MZ ヘッダーベースの DLL フラグメントを含有

4. [Defense Evasion] Deobfuscate/Decode Files or Information (T1140)
   a. CAPTCHA 検証を通じた保護解除
   b. エンコードされた文字列の復号
5. [Execution] User Execution: Malicious File (T1204.002)
   a. EdgeService.dll のロードおよび実行
   b. 分割された DLL を再結合した後に実行
6. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. agelessinvesting.xyz ドメインへのビーコン送信
   b. 追加の攻撃者制御ドメインとの通信
7. [Collection] Data from Local System (T1005)
   a. システムおよびユーザーデータの収集
   b. 追加ペイロード実行のための準備
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 収集データを外部 C2 サーバーへ送信
   b. 追加文書および PDF ベースのペイロード配布との連携


НАЦІОНАЛЬНА ПОЛІЦІЯ
ОБЛАСНЕ СЛІДЧЕ УПРАВЛІННЯ
ВНУТРІШНІХ СПРАВ, ПОЛТАВА
36000, м. Полтава, вул. Матвійчука Юліана, 83

ПОВІДОМЛЕННЯ
про зміну раніше повідомленої підозри
у вчиненні кримінальних правопорушень

місто Полтава 1 жовтня 2025 року

Для перегляду активуйте макроси

Про необхідність прибуття для розгляду справи по суті. Деталі вчиненого правопорушення докладаємо в архіві. За результатами розгляду справи буде прийнято рішення про обрання запобіжного заходу щодо Курочки Євгена Олексійовича. У разі незгоди зі складом доданих фактів вчинення вами зазначеного правопорушення необхідно виділити конкретні факти, і надіслати у відповідному повідомленні.

Додаток: архів «elektronna_povistka.rar»

Слідчий обласного слідчого управління міста Полтава
ст. лейтенант поліції Коваленко Олександр

[図 4: SectorT01 グループが悪用した文書]

40) SectorT01 used CAPTCHA Macro in Malicious Word Document (2025-12-08)

https://cti.nshc.net/events/view/20912

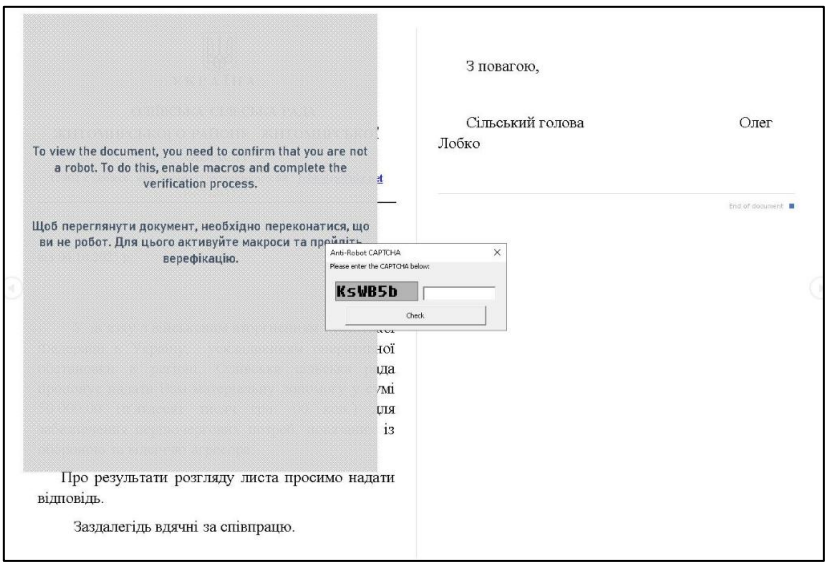
ベラルーシの脅威行為者がウクライナジトミール地域を対象に新しい"CAPTCHA マクロ"社会工学手法を使用しました。マクロが含まれた Malware Word 文書を使用し、マクロが有効化されると、ユ

ーザーは人間の相互作用を確認するための偽の CAPTCHA を見ることになります。確認後、ウクライナ政府テーマの内容が表示された餌文書が現れ、その間にバックグラウンドで悪性活動が進行します。これらの活動には、%LOCALAPPDATA%¥EReciver¥EdgeService.dll に位置する.NET DLL ファイルの配布が含まれ、これは regsvr32.exe を通じて実行されます。この DLL は約 1 分ごとにコマンド＆コントロールサーバーに HTTP POST リクエストを送り、感染したシステムに関するエンコードされた情報を送信します。この攻撃は社会工学と技術的回避戦術を活用し、リモートサーバーとの隠密な実行および継続的な通信を維持します。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. ウクライナ政府文書に偽装した Word ファイルの配布
   b. マクロ有効化を促すためのソーシャルエンジニアリング文句を含む
2. [Execution] User Execution: Malicious File (T1204.002)
   a. マクロ使用クリック
   b. 偽の CAPTCHA 入力誘導
3. [Execution] Command and Scripting Interpreter(T1059)
   a. CAPTCHA 確認後、マクロコード実行
   b. バックグラウンドで Malware ロジックを実行
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. マクロコード難読化
   b. 誘導文書表示によるユーザー認識回避
5. [Execution] Signed Binary Proxy Execution: Regsvr32 (T1218.010)
   a. EdgeService.dll ロード
   b. regsvr32.exe を通じた DLL 実行
6. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys (T1547.001)

a. DLL 自動実行のためのレジストリ設定
   b. ユーザー環境に基づく持続的実行
7. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. 約 1 分周期の HTTP POST 通信
   b. エンコードされたホスト情報の送信



[図 5: SectorT01 グループが悪用したマルウェア文書]

2. サイバー犯罪(Cyber Crime) ハッキンググループ活動

1) SectorJ21 used RedLoader Malware via Fake Recruitment Resumes (2025-12-05)

https://cti.nshc.net/events/view/20864

攻撃対象産業群: 製造, 小売, 技術

2024 年 2 月から 2025 年 8 月の間にカナダの組織を対象とした約 40 件のサイバー侵入が発生し、これは脅威行為者グループによって実行された。このグループは攻撃の 80%をカナダに集中した。元々サイバースパイ活動で知られていたこのグループは、データ脱取と選択的ランサムウェア配布を組み合わせた作戦に進化した。彼らは従来のフィッシングメールから脱却し、Malware 履歴書を配信するために採用プラットフォームを活用する。彼らの体系的なアプローチは、Indeed や JazzHR のようなプラットフォームを悪用して求職者を装い、Malware に改ざんされた PDF ファイルを配信して多段階感染チェーンを開始し、最終的に QWCrypt というカスタムランサムウェアを配布するものである。攻撃の順序は多段階で構成された洗練された RedLoader Malware 配信チェーンを含み、採用プラットフォームを通じた初期実行、二次ペイロード配布、そして潜在的な全体 Malware インストール実行を含む。彼らは検出を回避するためにカスタム BYOVD チェーンのような方法を使用し、プロキシツールを通じて C2 通信を転換する。これらの攻撃方法は典型的な金銭的動機を超えた専門的な作戦への転換を示し、洗練された回避および持続性戦略を含む。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 採用プラットフォームを通じた悪性履歴書(PDF)の提出

b. 求職者のなりすましアカウントで採用担当者にアクセス
2. [Execution] User Execution: Malicious File (T1204.002)
a. 履歴書 PDF 閲覧
b. RedLoader 初期ペイロード実行
3. [Execution] Command and Scripting Interpreter (T1059)
a. 後続スクリプト実行
b. 多段階ローダーチェーン動作
4. [Defense Evasion] Bring Your Own Vulnerable Driver (BYOVD) (T1068)
a. 脆弱なドライバーのロード
b. セキュリティ製品無力化
5. [Defense Evasion] Obfuscated Files or Information (T1027)
a. RedLoader 難読化
b. 多段階ペイロード隠匿
6. [Command and Control] Proxy (T1090)
a. プロキシツールを通じた C2 転換
b. C2 通信経路隠匿
7. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. 内部データ外部転送
b. C2 チャネル活用
8. [Impact] Data Encrypted for Impact (T1486)
a. QWCrypt ランサムウェア 実行
b. オプションのファイル暗号化

2) SectorJ39 used SocGholish JavaScript as Fake Software Updates (2025-11-25)

https://cti.nshc.net/events/view/20537

攻撃対象産業群: 工学

2025 年にウクライナと関連したアメリカ基盤の会社がサイバー脅威行為者の標的となり、SocGholish Malware を配布しました。この Malware は損傷した合法的なウェブサイトを通じて RomCom ローダーを配信しました。サイトに注入された悪意のある JavaScript はユーザーを偽のアップデートプロンプトに誘導し、リモートアクセスと追加ペイロードの配信を可能にする Malware をダウンロードさせました。SocGholish は初期アクセスブローカーとして活動する金銭的動機を持つグループによって運営され、損傷したシステムをランサムウェア運営者と接続しました。RomCom ローダーは初期感染後 30 分以内に配信され、難読化された JavaScript とコマンド＆コントロールサーバーとの通信を使用して実行され、追加の搾取と潜在的なランサムウェア配布を可能に

しました。この活動は国家と連携したグループによって実行されたもので、世界中の組織に影響を与える広範な被害者群を持つ偶発的サイバー脅威の危険性を強調します。

[Attack Flow]

1. [Initial Access] Drive-by Compromise (T1189)
   a. 正規 Web サイトに悪性 JavaScript を挿入
   b. 訪問者のブラウザに対してスクリプトを配信
2. [Execution] User Execution: Malicious File (T1204.002)
   a. 偽のソフトウェア更新ポップアップを表示
   b. 「アップデート」クリック時に SocGholish をダウンロード
3. [Execution] Command and Scripting Interpreter: JavaScript (T1059.007)
   a. 難読化された JavaScript の実行
   b. 追加ペイロードのローディングロジックを実行
4. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. HTTP/HTTPS 基盤の C2 サーバー通信
   b. コマンド受信およびローダー制御
5. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. RomCom ローダーの実行
   b. 追加マルウェアモジュールのダウンロードおよび実行
6. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. JavaScript および PowerShell の難読化
   b. 文字列置換およびエンコーディングの使用
7. [Command and Control] Ingress Tool Transfer (T1105)
   a. RomCom を介した後続ペイロードの受信
   b. 追加マルウェア配布パスの維持

3) SectorJ109 used Trojans with Valid Digital Signatures for Malware Spread (2025-12-13)

https://cti.nshc.net/events/view/21383

最近のサイバー脅威事件は、デジタル署名されたファイルを活用して Malware を配布するグループと関連しています。攻撃者は検出を避けるために、特にオンラインサンドボックスプラットフォームを対象にアンチサンドボックスおよびアンチデバッグ技術を使用しました。Malware は外部の Amazon AWS S3 バケットと通信してペイロードをダウンロードおよび実行しました。この作戦には photo20251208698m.exe というファイルが含まれており、Shanxi Rongshengyuan Technology、Shandong Saibo Information、Kingston Technology といった複数の会社のデジタ

ル署名を持っていました。トロイの木馬はレジストリエントリ、仮想マシンプロセス、MAC アドレス、システム環境を検査するなど、広範なアンチ仮想マシン検査を使用して制御された環境での実行を回避しました。活性化されると、Malware は外部アドレスをデコードして特定のディレクトリに保存された追加の悪性ペイロードを取得しました。DataReport.log でデコードされたシェルコードは、メモリ内で実行される追加の悪性コンポーネントを明らかにしました。サンプルには、Automation された悪性活動に使用される埋め込まれた暗号化されたコマンドおよび制御アドレスが含まれた UPX パッキングファイルが含まれていました。Malware はまた、Windows サービスを生成するコマンドを含む持続性機能を示しました。デジタル署名と攻撃方法は、類似の戦術とネットワーク指標を含む以前のキャンペーンと関連した脅威活動との歴史的関連性を示唆しました。

[Attack Flow]

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

a. デジタル署名された実行ファイル添付

b. 写真・文書に偽装したファイル名使用

2. [Execution] User Execution: Malicious File (T1204.002)

a. photo20251208698m.exe 実行

b. 管理者権限要求を通じた実行フロー誘導

3. [Defense Evasion] Masquerading: Match Legitimate Name or Location (T1036.005)

a. 正常企業デジタル署名悪用

b. 合法ソフトウェアで偽装

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

a. UPX パッキング適用

b. 暗号化された C2 アドレス 含む

5. [Defense Evasion] Virtualization/Sandbox Evasion (T1497)

a. 仮想マシン・サンドボックス環境検査

b. デバッグ・分析ツール検出

6. [Discovery] System Information Discovery (T1082)

a. CPU・メモリ・アップタイム確認

b. システム環境変数点検

7. [Discovery] Process Discovery (T1057)

a. セキュリティソリューションプロセス確認

b. 仮想化関連プロセス確認

8. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)

a. AWS S3 バケットと通信

b. 外部アドレスデコード後接続

9. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.003)

a. DataReport.log でシェルコードロード
b. メモリ内 Malware 実行
10. [Persistence] Create or Modify System Process: Windows Service (T1543.003)
a. Windows サービス生成
b. サービスベースの自動実行維持
11. [Collection] Input Capture (T1056)
a. キー入力収集
b. 画面情報収集
12. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. 暗号化されたチャネルで収集データを送信
b. 外部 C2 インフラ活用
13. [Impact] Indicator Removal on Host (T1070)
a. Windows イベントログ削除
b. ブラウザデータの削除

4) SectorJ135 used resume-themed ZIP lures to deliver LNK malware (2025-12-16)
https://cti.nshc.net/events/view/21109

2024 年 3 月、サイバー攻撃は脅威行為者が履歴書誘引を含む偽の求職申請書を通じて初期アクセスを得ることで始まりました。このマルウェアキャンペーンは、実行時に一連の悪性活動を引き起こす.lnk ファイルをダウンロードすることを含んでいました。ここには Microsoft の ie4uinit.exe を悪用して悪性.inf ファイルをロードし、WMI を使用して DLL を配布し、コマンド＆コントロール目的の more_eggs Malware をインストールすることが含まれていました。探索コマンドが実行され、Cobalt Strike が配布されて足場を築きました。攻撃者はバックアップサーバーの脆弱性(CVE-2023-27532)を悪用してローカル管理者アカウントを作成することで横方向移動を進めました。彼らは RDP を使用して接続し、ランサムウェアに関連する以前の事件と関連付けられたホスト名を漏洩しました。SharpShares や Seatbelt のようなツールを使用して追加の環境列挙が行われました。彼らは Pyramid C2 を配布しようとしましたが、成功は限定的でした。バックアップサーバーで LSASS メモリにアクセスして資格情報を取得し、2 番目のサーバーを侵害しました。攻撃者は持続的なネットワークアクセスのために Cloudflared トンネルを設定しました。彼らの行動を隠蔽しようとする試みにもかかわらず、彼らの活動には試験実行、ツールのインストール、侵害されたシステムからの貴重なデータ抽出が含まれていました。攻撃は技術とインフラに最小限の変更しか加えずに、かなりの期間検出されずに持続しました。

[Attack Flow]
1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)

a. 求職申請書に偽装したフィッシングメールの配信
b. 悪性ファイル添付
2. [Execution] User Execution: Malicious File (T1204.002)
a. ユーザーが .lnk ファイルを実行
b. ie4uinit.exe 呼び出しで後続動作をトリガー
3. [Execution] Signed Binary Proxy Execution: Rundll32 (T1218.011)
a. 悪意のある .inf ファイルのロード
b. rundll32.exe を通じた DLL 実行
4. [Execution] Windows Management Instrumentation (T1047)
a. WMI を利用した DLL 配布
b. more_eggs Malware インストール
5. [Persistence] Scheduled Task/Job: Scheduled Task (T1053.005)
a. 予約タスクの作成
b. more_eggs 自動実行維持
6. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
a. more_eggs C2 通信
b. Cobalt Strike ビーコン 활성化
7. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
a. バックアップサーバーの脆弱性 (CVE-2023-27532) 悪用
b. ローカル管理者アカウント生成
8. [Credential Access] OS Credential Dumping: LSASS Memory (T1003.001)
a. LSASS メモリ アクセス
b. 資格情報ダンプ実行
9. [Discovery] System Network Configuration Discovery (T1016)
a. SharpShares を通じた共有リソース探索
b. Seatbelt でシステム情報収集
10. [Lateral Movement] Remote Services: Remote Desktop Protocol (T1021.001)
a. バックアップサーバーへの RDP 接続
b. 追加サーバーへの横方向移動
11. [Command and Control] Ingress Tool Transfer (T1105)
a. Cloudflared トンネル設定
b. 外部 C2 と持続接続維持
12. [Exfiltration] Exfiltration Over C2 Channel (T1041)
a. C2 チャネルを通じたデータ転送
b. トンネリング基盤トラフィック隠匿

5) SectorJ199 used RAR disguised as PDF to deploy PowerShell malware (2025-11-25)

https://cti.nshc.net/events/view/20577

攻撃対象産業群: 政府・行政

精巧なサイバーキャンペーンが企業および政府ネットワークを対象に隠密な情報窃取を目的として、データ流出、資格情報窃取、長期的なアクセス維持に重点を置いた。攻撃はユーザーが Bing で "belay"を検索することから始まり、これは潜在的に JavaScript で損傷された合法的なサイトに接続され、悪性の類似ドメインにリダイレクトされた。このドメインは PDF ブロシャーに偽装した RAR アーカイブを提供し、これを開くと MSC ファイルをドロップした。このファイルは Windows mmc.exe を通じてペイロードを実行し、TaskPad コマンドとエンコードされた PowerShell スクリプトを使用した。攻撃は段階的に進行した。最初の段階で PowerShell スクリプトは第二のスクリプトをダウンロードして実行し、これは C#コードをコンパイルして隠されたプロセスを実行し、餌の PDF を表示し、持続的なローダーを実行した。最後の段階ではバックドアや情報窃取型 Malware をインストールした可能性が高く、EncryptHub, SilentPrism, DarkWisp, Rhadamanthys のようなツールが含まれていた可能性があるが、C2 インフラが応答しないため正確な確認は不可能だった。

[Attack Flow]

1. [Initial Access] Drive-by Compromise (T1189)
   a. Bing 検索結果を介した悪性サイトへのリダイレクト
   b. JavaScript が挿入された正規サイト経由の誘導
2. [Execution] User Execution: Malicious File (T1204.002)
   a. PDF に偽装した RAR アーカイブの実行
   b. MSC ファイルの実行
3. [Execution] Signed Binary Proxy Execution: MMC (T1218.014)
   a. mmc.exe を介した MSC のロード
   b. TaskPad コマンドの実行
4. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. エンコードされた PowerShell スクリプトの実行
   b. 2 段階の PowerShell スクリプトのダウンロードおよび実行
5. [Execution] Command and Scripting Interpreter: Windows Command Shell (T1059.003)
   a. C#コードのコンパイル
   b. 隠蔽されたプロセスの実行
6. [Defense Evasion] Masquerading (T1036)
   a. PDF ブロシャーに偽装
   b. 偽装された PDF 画面の表示

7. [Persistence] Create or Modify System Process: Windows Service (T1543.003)
   a. ローダープロセスの反復実行
   b. サービスベースの永続性確保
8. [Collection] Data from Local System (T1005)
   a. システム情報の収集
   b. ユーザーデータの収集
9. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. 外部 C2 インフラへの接続試行
   b. コマンド受信および後続ペイロードの取得試行
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. 収集データの送信試行
    b. バックドアおよび情報窃取型マルウェアの活用

6) SectorJ230 used Gainsight Compromise in SaaS Supply-Chain Attack (2025-11-26)

https://cti.nshc.net/events/view/20594

この事件は攻撃者が Gainsight と Salesforce 間の OAuth 基盤統合を悪用し、非許可 IP アドレスから非認可 API 呼び出しを実行したものである。この過程で Tor 終了ノードやプロキシまたは VPN サービスのような一般的な匿名化インフラを使用した。この活動は OAuth トークンや統合資格情報を収集または損傷させることに重点を置いており、これにより Salesforce 自体の脆弱性を悪用せずに信頼できる Gainsight 接続アプリケーションを通じて Salesforce データにアクセスすることができた。これは効果的にサプライチェーンスタイルの妥協を生み出した。関連指標は SmokeLoader、Stealc、DCRat、Vidar のような一般的な Malware 系と共に頻繁に使用されるインフラとの重複を示しており、初期資格情報やトークン盗難が SaaS 統合悪用以前に Malware 基盤収集から生じた可能性を示唆する。

[Attack Flow]

1. [Initial Access] Valid Accounts (T1078)
   a. 盗まれた OAuth トークンの使用
   b. 統合アプリケーション資格証明の悪用
2. [Credential Access] Steal Application Access Token (T1528)
   a. OAuth 基盤 統合 トークン 再使用
   b. 既存の統合信頼関係の悪用
3. [Defense Evasion] Proxy (T1090)
   a. Tor 終了ノード使用
   b. プロキシ・VPN 基盤アクセス

4. [Discovery] Cloud Service Discovery (T1526)
a. Salesforce API エンドポイント探索
b. アクセス可能なオブジェクト・データ識別
5. [Collection] Data from Cloud Storage (T1530)
a. Salesforce データ 조회
b. 統合権限範囲内情報収集
6. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
a. Gainsight アプリケーションを通じた API 呼び出し
b. HTTPS 기반 SaaS API 通信
7. [Exfiltration] Exfiltration Over Web Service: Cloud Storage (T1567.002)
a. API 応答データ外部収集
b. 正常な統合トラフィックに偽装したデータ移転

7) SectorJ247 used CastleLoader Disguised as GitHub Tools for Attacks (2025-11-26)
https://cti.nshc.net/events/view/20572

2025 年 3 月から新しいサービス型マルウェア(Malware-as-a-Service, MaaS)運営者がアメリカを中心に活動している。この運営者は CastleLoader と CastleRAT という 2 つのカスタムマルウェアファミリーを使用してキャンペーンを実行する。CastleLoader は追加の悪性ソフトウェアをインストールするローダーマルウェアで、しばしば合法的なサービスを模倣するドメインを通じてユーザーを欺き、悪性スクリプトを実行させる。このマルウェアは検出を回避するためにコード難読化を使用し、CastleRAT を配信するメカニズムとして機能する。CastleRAT はリモートアクセス型トロイの木馬で、侵害されたシステムに対する広範な制御を可能にする。このグループのインフラは、さまざまなマルウェアのコマンド＆コントロールサーバーとして使用される IP アドレスとドメインを含む。2025 年 5 月までに CastleLoader は 469 台のデバイスを侵害した。Python ベースの CastleRAT 変種は、隠蔽技術を使用して最小限のアンチウイルス検出を示す。6 月にはこのマルウェアに関連する異常なネットワーク活動が観察され、ここには既知の悪性 IP との接続、スクリプトのダウンロード、内部偵察の試みが含まれる。高度なモニタリングモデルがこれらの活動を検出し、悪性接続を遮断する自動応答を誘導した。

[Attack Flow]
1. [Initial Access] Phishing: Spearphishing Link (T1566.002)
a. 合法サービスに偽装したドメイン接続誘導
b. Cloudflare セキュリティ確認画面を詐称したスクリプト配信
2. [Execution] User Execution: Malicious Script (T1204.002)
a. ユーザーの相互作用を通じた悪性スクリプトの実行

b. PowerShell コマンドを通じた CastleLoader 実行

3. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. コード難読化および無意味コード挿入
   b. パッキング技法を通じた静的分析回避
4. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
   a. レジストリ自動実行キー登録
   b. ローダー基盤の持続実行維持
5. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. HTTP 기반 C2 サーバー通信
   b. 多数の User-Agent を活用したトラフィック偽装
6. [Discovery] Network Service Scanning (T1046)
   a. 内部ネットワークサービススキャン
   b. 接続可能なエンドポイント識別
7. [Collection] Input Capture: Keylogging (T1056.001)
   a. キー入力情報収集
   b. ユーザー活動情報収集
8. [Exfiltration] Exfiltration Over C2 Channel (T1041)
   a. 収集データ外部 C2 送信
   b. 持続的な C2 チャネル活用

8) SectorJ247 used Malware via ClickFix phishing (2025-12-09)

https://cti.nshc.net/events/view/20902

攻撃対象産業群: 物流

2025 年 9 月、高度なサイバー脅威アクターが CastleLoader として知られるサービス型 Malware を活用した精巧な作戦が識別された。このアクターは少なくとも 2025 年 3 月から活動中のサイバー攻撃を遂行するために多様なインフラを使用している。脅威アクターは複数の個別クラスターを運営しており、特に物流会社や Booking[.]com のような主要ホスピタリティプラットフォームを装って CastleLoader およびその他の悪性ペイロードを配布する標的フィッシングキャンペーンを実行している。該当 Malware エコシステムは CastleRAT や Matanbuchus のようなカスタム開発された多様な悪性ツールを特徴としており、CastleRAT は C と Python バージョンの両方で存在し、柔軟で技術的に熟練した開発過程を示している。Malware は通常、巧妙に偽装されたメールや悪性広告を通じてシステムに侵入し、効果的なペイロード配布のために ClickFix のような技術を使用する。脅威アクターのインフラは持続的な作戦と強力な回避行動を支援し、プロセス注入や難読化を含め、損傷したシステムと合法的な貨物プラットフォームを活用してより広範囲と影響を与える。また、物流会社

を模倣するためにインフラが再登録された兆候があり、フィッシングの信頼性を高めている。調査は複数の活動とインフラクラスターが同一の脅威アクターに再び接続されることを示し、特に物流およびホスピタリティ部門で産業別脆弱性を悪用しようとする調整された努力を示唆している。報告された活動は現代サイバー脅威の複雑性と適応性が増加していることを強調し、精巧な防御で緩和されない限り、標的部門に対するリスクが増加していることを示している。

[Attack Flow]

1. [Initial Access] Phishing: Spearphishing Attachment (T1566.001)
   a. 物流業界およびホスピタリティ企業を詐称したフィッシングメールの配信
   b. Booking.com や物流企業名を装ったマルウェア添付ファイルの送信
2. [Execution] User Execution: Malicious File (T1204.002)
   a. ClickFix 手法を通じたユーザー実行の誘導
   b. マルウェア添付ファイルまたはスクリプトの実行
3. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. PowerShell コマンドの実行
   b. CastleLoader 初期ローダーの実行
4. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. PowerShell およびローダーコードの難読化
   b. 文字列エンコーディングおよび実行フローの隠蔽
5. [Defense Evasion] Masquerading: Match Legitimate Name or Location (T1036.005)
   a. 正規の物流・予約サービスを装った偽装
   b. 再登録されたドメインを利用した信頼性の偽装
6. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. HTTP/HTTPS 基盤の C2 通信
   b. RC4 暗号化によるトラフィック保護
7. [Command and Control] Ingress Tool Transfer (T1105)
   a. CastleRAT の追加ペイロード配信
   b. Matanbuchus などの二次マルウェアの配布
8. [Collection] Input Capture: Keylogging (T1056.001)
   a. キー入力の収集
   b. ユーザー活動情報の収集
9. [Collection] Screen Capture (T1113)
   a. 画面キャプチャの取得
   b. 視覚的なユーザー情報の収集
10. [Exfiltration] Exfiltration Over C2 Channel (T1041)
    a. 収集データの外部 C2 サーバーへの送信

b. 持続的な C2 チャネルを通じた情報流出

9) SectorJ249 used Velociraptor DFIR for Warlock ransomware deployment (2025-12-11)

https://cti.nshc.net/events/view/21075

攻撃対象産業群: 産業, 農業, 政府・行政, エネルギー, 小売, 自動車, 教育, 金融, IT, 技術

2025 年 3 月から 9 月の間、Microsoft SharePoint の脆弱性を悪用する精巧なグループによって一連のサイバー侵入が発生し、Warlock ランサムウェアが配布されました。これらの攻撃は農業、政府、エネルギーなどの複数の分野で発見され、ToolShell として知られるゼロデイ脆弱性セットを悪用しました。主に SharePoint を通じて初期アクセスを得た後、攻撃者は Mimikatz や Velociraptor のようなツールを使用して持続性と資格情報アクセスを確保しました。彼らは管理者アカウントを作成し、Velociraptor ツールを使用して攻撃を準備し、これは制御ドメインからダウンロードしてトンネルがアクティブな状態で Visual Studio Code を実行する戦略を含みました。特に VMTools のようなアンチウイルスおよびエンドポイント検出と EDR キラーの使用は、セキュリティ検出を回避する高度なアプローチを示しています。また、このグループは脆弱なドライバーを直接持ち込む攻撃(BYOVD)と DLL サイドローディングを使用した可能性があります。配布されたランサムウェアの変種には Warlock、LockBit、Babuk が含まれ、カスタムランサムノートや qTox ID および Protonmail を通じた独特な通信チャネルなどのユニークな侵入特性を示しました。これらの侵入は財政的動機があると見られ、中国を拠点とする起源を示唆するつながりがありますが、政府の関与を裏付ける明確な証拠はありません。それにもかかわらず、標的とされた分野は諜報目的との潜在的な重複を示唆しています。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
   a. Microsoft SharePoint 脆弱性 悪用
   b. ToolShell ゼロデイ脆弱性チェーン活用
2. [Execution] Command and Scripting Interpreter (T1059)

a. SharePoint 環境内のリモートコマンド実行
   b. 後続ペイロード実行のための命令伝達
3. [Persistence] Valid Accounts (T1078)

a. 新規管理者アカウント生成

b. 生成されたアカウントを通じた持続的アクセス維持

4. [Command and Control] Application Layer Protocol (T1071)
   a. Velociraptor 配布および C2 チャネル構成

b. Visual Studio Code 実行およびトンネル機能 활성化

5. [Privilege Escalation] Exploitation for Privilege Escalation (T1068)
a. BYOVD(脆弱なドライバーの直接ロード)攻撃の活用
b. DLL Side-Loading の可能性
6. [Defense Evasion] Impair Defenses: Disable or Modify Tools (T1562.001)
a. VMTools 등セキュリティエージェントキラー使用
b. EDR/アンチウイルス プロセス 無効化
7. [Credential Access] OS Credential Dumping (T1003)
a. Mimikatz を利用した資格情報ダンプ
b. 管理者・ドメインアカウント情報収集
8. [Command and Control] Application Layer Protocol (T1071)
a. qTox 기반 통신 식별자 사용
b. ProtonMail アカウントを通じた攻撃者通信
9. [Impact] Data Encrypted for Impact (T1486)
a. Warlock ランサムウェア 配布
b. LockBit 및 Babuk ランサムウェア 変種 実行

10) SectorJ266 used Hybrid Phishing Kit blending Salty2FA and Tycoon2FA (2025-12-02)

https://cti.nshc.net/events/view/20706

2025 年 10 月末、フィッシングキット Salty2FA と Tycoon2FA の活動に注目すべき変化が発生する。Salty2FA を使用するフィッシングキャンペーンは、週に数百件のアップロードから数十件へと急激に減少する。その後、Salty2FA と Tycoon2FA の要素を組み合わせた新しいハイブリッドペイロードが登場する。分析の結果、重複する指標と共有されたコードが発見され、オペレーター間のインフラ統合や運営協力がある可能性を示唆する。これらの重複は Salty2FA の運営問題を示しており、DNS 失敗により Tycoon2FA ホスティングへの代替が発生し、両フレームワークの背後に統合された敵対勢力が存在する可能性を提起する。この状況は、行動ベースの指標に重点を置いた更新された検出能力とハイブリッドフィッシング活動の包括的な追跡の必要性を強調する。これらの進展は、キット別検出戦略を複雑にし、脅威行為者が防御措置に対する適応力と回復力を強化していることを示唆する。

[Attack Flow]

1. [Initial Access] Spearphishing Link (T1566.002)
a. Salty2FA および Tycoon2FA 基盤のフィッシングページ配信
b. ハイブリッド型フィッシングキットの誘導リンクを使用
2. [Execution] User Execution (T1204)

a. 被害者によるログインページとの相互作用
b. 基本インフラ障害時における代替 URL への自動切り替え
3. [Credential Access] Adversary-in-the-Middle (T1557.002)
a. リアルタイムでの資格情報および 2FA コードの中継
b. 認証セッションのハイジャック
4. [Defense Evasion] Obfuscated Files or Information (T1027)
a. Base64 および XOR を組み合わせた難読化
b. 分析および自動化回避ロジックの適用
5. [Command and Control] Web Service (T1102.002)
a. Tycoon2FA 基盤ホスティングを利用したフェイルオーバー
b. Fast-flux および DNS エラー（SERVFAIL）への対応
6. [Collection] Credentials from Web Browsers (T1555.003)
a. ユーザーアカウント情報の収集
b. セッショントークンおよび認証データの取得

11) SectorJ267 used Gigaflower Malware disguised in Banking Apps (2025-12-03)

https://cti.nshc.net/events/view/20743

攻撃対象産業群: 銀行

2024 年初頭、アジア太平洋地域のユーザーを対象とした精巧なモバイル詐欺キャンペーンが高級バンキングトロイの木馬を使用して発生する。脅威行為者は Android および iOS モバイル Malware を使用し、合法的なバンキングアプリを模倣し、Frida、Dobby、Pine のような公開フレームワークを悪用して Malware を注入する。主要な感染ベクターは社会工学的戦術を含み、攻撃者は政府サービスを装って被害者のデバイスに偽のアプリをインストールする。この攻撃は主にベトナム、インドネシア、タイのユーザーに影響を与え、インドネシアだけで 2,200 件以上の感染が確認された。Gigaflower のような修正されたアプリは、テキスト認識および身分証明書の QR コードスキャンを含む強化された機能を示す。攻撃者はフィッシングとスミッシングを活用して APK を合法的なアプリに偽装し、アプリストアの防御を回避して Malware を配布する。この作戦は WebRTC を使用してリアルタイムデバイス制御を実行し、リモートアクセス、データ窃取、アプリロジックの修正といった主要な問題に集中し、伝統的なセキュリティシステムを回避するための技術的能力を活用する。

[Attack Flow]

1. [Initial Access] Spearphishing Link (T1566.002)
a. 政府サービスを装ったメッセージの配布
b. 合法アプリに偽装した APK インストール誘導
2. [Execution] Native API (T1636)

a. モバイル OS ネイティブ API 悪用
b. Malware ランタイム注入
3. [Execution] Command and Scripting Interpreter (T1059)
a. Frida·Dobby·Pine フレームワーク 使用
b. アプリロジックフッキングおよびコードインジェクション
4. [Persistence] Modify System Partition (T1409)
a. 正常なアプリを改ざん後、再パッケージング
b. Malware 機能内蔵アプリ維持
5. [Credential Access] Input Capture (T1056)
a. 画面テキスト認識
b. 認証・金融情報入力の窃取
6. [Collection] Data from Information Repositories (T1213)
a. 身分証明書イメージ収集
b. QR コード情報抽出
7. [Command and Control] Application Layer Protocol (T1071)
a. WebRTC 基盤のリアルタイム制御
b. リモートコマンドおよびセッション維持
8. [Defense Evasion] Obfuscated Files or Information (T1027)
a. アプリストア検証回避
b. セキュリティソリューション回避ロジック適用

12) SectorJ268 used Spyware Extension disguised as Productivity Tools (2025-12-01)

https://cti.nshc.net/events/view/20707

サイバー脅威行為者が 7 年にわたり、精巧で多段階のキャンペーンを実施し、Chrome と Edge ブラウザを悪性拡張プログラムを通じて攻撃した。初期には、背景画や生産性アプリに偽装した 145 個の拡張プログラムが配布され、ユーザーブラウジングデータを記録し、コミッションを得るアフィリエイト詐欺を行った。これは Infinity V+のような拡張プログラムを通じた検索ハイジャッキングに発展し、検索をリダイレクトし、クッキーデータを流出させた。2018-2019 年までに拡張プログラムは信頼できる状態を得た後、リモートコード実行および中国サーバーへのデータ流出を含むより深刻な作業のために武器化された。いくつかの拡張プログラムが削除されたにもかかわらず、400 万人以上のユーザーに影響を与える重要なスパイウェア作戦が進行中であり、主に WeTab 拡張プログラムを通じて URL、検索クエリ、マウスクリックに関するデータ収集が行われている。これらの作戦はブラウザ自動更新メカニズムを悪用して静かに Malware を配布し、信頼に基づくブラウザ拡張プ

ログラムエコシステムの結果を示している。この脅威は静的レビュープロセスよりも継続的なモニタリングの必要性を強調する。

[Attack Flow]

1. [Execution] Command and Scripting Interpreter: JavaScript (T1059.007)
   a. ブラウザ拡張コンテキスト内での JavaScript コード実行
   b. リモートサーバーから配信されたスクリプトの定期的実行
2. [Persistence] Event Triggered Execution: Browser Extensions (T1546.008)
   a. ブラウザ拡張の自動アップデートメカニズムの悪用
   b. 信頼確保後における機能の段階的な武器化
3. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. JavaScript コードの難読化
   b. 分析環境に応じた動作分岐
4. [Discovery] System Information Discovery (T1082)
   a. ブラウザ種別およびバージョンの識別
   b. ユーザー環境に基づく識別子の生成
5. [Collection] Data from Local System (T1005)
   a. 訪問 URL およびブラウジング履歴の収集
   b. 検索クエリおよびユーザー操作情報の収集
6. [Collection] Input Capture (T1056)
   a. 検索入力およびクリックイベントの収集
   b. マウス操作およびページ相互作用の追跡
7. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. HTTP/HTTPS ベースのリモートサーバー通信
   b. ブラウザトラフィックに混在した C2 通信
8. [Exfiltration] Exfiltration Over Web Service (T1567.002)
   a. 収集されたユーザーデータの外部サーバー送信
   b. 暗号化チャネルを介した情報流出
9. [Impact] Data Manipulation (T1565)
   a. 検索結果のリダイレクト
   b. アフィリエイト追跡コード挿入によるトラフィック操作

13) SectorJ269 used DLL sideloading for security tool evasion (2025-12-09)

https://cti.nshc.net/events/view/20963

金銭的動機を持つ脅威行為者が初期アクセスブローカーから高度な事後搾取エンティティへと発展し、DLL サイドローディングを通じて合法的なエンドポイント検出および対応(EDR)システムを標的にしてマルウェア活動を隠します。この行為者はサービス型ランサムウェア(RaaS)運営に関与したことで知られており、元々は大量フィッシングを使用していましたが、現在ではドメインスプーフィング、ファイルレス実行、SentinelOne のような合法的なセキュリティツールのサイドローディングを含む高度な技術を使用して防御を回避します。攻撃は社会工学戦術で始まり、被害者を説得して Windows 実行ダイアログを通じてエンコードされた悪性コマンドを実行させます。主要な攻撃段階には、スプーフィングされた Microsoft ドメインの下に偽装された悪性スクリプトを取得し、PowerShell コマンドをメモリ内で直接実行して検出を回避し、信頼できるソフトウェアプロセスを使用して隠密なコマンドおよび制御チャネルを構築して安全な通信を行うことが含まれます。これらの方法は検出にかなりの困難を引き起こし、正常な運用からの逸脱を発見するために高度な行動モニタリングが必要です。これらの事前準備されたアプローチをランサムウェアアフィリエイトに販売することで、ランサムウェア攻撃の迅速な展開を容易にし、産業全体にわたる警戒強化と事前脅威検出戦略の必要性を強調します。

[Attack Flow]

1. [Initial Access] Spearphishing Link (T1566.002)
   a. Windows の実行（Run）ダイアログを利用したソーシャルエンジニアリング誘導
   b. エンコードされたコマンドの実行をユーザーに直接指示
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
   a. curl.exe を利用したリモートスクリプトのダウンロード
   b. ファイルを生成せずにメモリ内で PowerShell を実行
3. [Defense Evasion] Hijack Execution Flow: DLL Side-Loading (T1574.002)
   a. マルウェア DLL のサイドローディング
   b. SentinelAgentWorker.exe プロセスの悪用
4. [Defense Evasion] Signed Binary Proxy Execution (T1218)
   a. curl.exe など署名済み Windows ユーティリティの悪用
   b. 信頼されたバイナリコンテキストでのコマンド実行
5. [Discovery] System Information Discovery (T1082)
   a. MachineGuid などのシステム識別子の照会
   b. reg.exe を通じた OS および環境情報の収集
6. [Persistence] Boot or Logon Autostart Execution: Registry Run Keys (T1547.001)
   a. レジストリの Run キーの改変
   b. 信頼された実行パスに基づく自動実行の維持
7. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. HTTP/HTTPS 基盤の暗号化された C2 通信

b. 正規プロセスのコンテキストを利用した通信
8. [Command and Control] Dynamic Resolution (T1568)
a. Microsoft 関連ドメインを模倣した C2 ドメインのローテーション
b. 弾力的な C2 エンドポイントの解決

14) SectorJ270 used VolkLocker Ransomware with Telegram Automation (2025-12-10)

https://cti.nshc.net/events/view/20968

脅威行為者が 2025 年 8 月、休眠期間後に VolkLocker というランサムウェアサービスを使用して攻撃を開始する。この作戦は自動化と通信のために Telegram を活用する。Linux と Windows システムを対象とする VolkLocker ペイロードは Golang で作成されており、基本的な難読化機能がないため、アフィリエイトが UPX を使用してパッキングするよう誘導する。攻撃は"ms-settings" UAC 回避技法を通じた権限昇格を含み、MAC アドレスとレジストリ項目を使用して仮想環境を確認する。ランサムウェアは AES-256 GCM モードでファイルを暗号化し、%TEMP%フォルダに暗号化キーの平文バックアップを保管するが、これは注目すべき設計上の欠陥である。持続性はセキュリティツールを無効化するためにシステムポリシーを修正し、複数の場所にランサムウェアのコピーを生成することで達成される。ペイロードはカウントダウンタイマーがある身代金要求書を使用し、無断復号化試行にシステムファイル削除と BSOD を結びつける。CyberVolk はすべての作業に Telegram を使用し、RAT およびキーロガーツールを含む拡張されたサービスを広告する。

[Attack Flow]

1. [Initial Access] Exploit Public-Facing Application (T1190)
a. 外部に公開されたサービスの侵害を通じた初期アクセス
b. RaaS パートナーを介したアクセス権の確保
2. [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)
a. PowerShell を利用したセキュリティ機能の無効化
b. 分析およびセキュリティツールプロセスの終了
3. [Privilege Escalation] Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
a. ms-settings プロトコルを利用した UAC 回避
b. レジストリキーのハイジャックによる権限昇格の実行
4. [Defense Evasion] Impair Defenses: Disable or Modify Tools (T1562.001)
a. Windows Defender およびセキュリティポリシーの無効化
b. システムセキュリティ設定の変更
5. [Defense Evasion] Virtualization/Sandbox Evasion (T1497)

   a. MAC アドレスに基づく仮想環境の判別
   b. 特定のレジストリ値に基づく分析環境の回避
6. [Defense Evasion] Obfuscated Files or Information (T1027)
   a. UPX パッキングによるバイナリの隠蔽
   b. 静的解析回避を目的とした難読化
7. [Persistence] Boot or Logon Autostart Execution (T1547)
   a. ランサムウェアコピーを複数のパスに生成
   b. 自動実行位置を通じた再実行の保証
8. [Discovery] System Information Discovery (T1082)
   a. システム構成および OS 情報の収集
   b. ローカル環境の識別情報の確認
9. [Impact] Data Encrypted for Impact (T1486)
   a. ファイルを AES-256-GCM 方式で暗号化
   b. 暗号化キーを TEMP ディレクトリに平文で保存
10. [Impact] Inhibit System Recovery (T1490)
   a. Volume Shadow Copy の削除
   b. 復旧妨害を目的としたシステム設定の変更
11. [Command and Control] Application Layer Protocol: Web Protocols (T1071.001)
   a. Telegram API 基盤の命令および状態通信
   b. 感染状態および実行結果の報

今月のサイバー脅威の特徴点

今月のサイバー攻撃事件は、脅威行為者の精巧さと適応力を反映しており、様々な技術的および戦術的特徴を示しています。攻撃は LummaC2 や OtterCookie のような情報窃取型 Malware、CastleRAT や UDPGangster のようなリモートアクセスツール、Warlock や VolkLocker のようなランサムウェアを含む様々な Malware ファミリーを使用します。これらの Malware タイプはしばしばフィッシングメールを通じて配信され、ソーシャルエンジニアリング戦術を利用して被害者が悪意のあるペイロードを実行するように欺きます。攻撃ベクターには、侵害されたウェブサイト、偽の求人応募書、悪意のある添付ファイルやリンクを含むスピアフィッシングメールが含まれます。感染経路はしばしばマクロを通じてペイロードを配布したり、CVE-2018-0802 のような脆弱性を悪用する悪意のある Word および RTF ファイルのような文書ベースのエクスプロイトを使用します。
今月観察された戦術、技術および手順（TTP）は、高度な回避および持続性メカニズムの使用を強調しています。脅威行為者は DLL サイドローディング、PowerShell 難読化、Visual Studio Code および AnyDesk のような正当なツールを使用した側面移動およびリモートアクセスのような技術を使

用します。持続性はしばしばスケジュールされたタスク、レジストリの変更、スタートアップディレクトリの使用を通じて達成されます。コマンドおよびコントロール（C2）通信は AES および HTTPS のような暗号化プロトコルを使用して保護されており、一部の行為者は Discord および Telegram のような公共プラットフォームを C2 チャネルとして活用します。
いくつかのキャンペーンは、WinRAR および Microsoft SharePoint のような広く使用されているソフトウェアの脆弱性を悪用して初期アクセスを得て Malware を配布することを示しています。ネットワークデバイスのゼロデイ脆弱性および誤った構成の使用は、脅威行為者が技術的弱点を悪用する能力をさらに強調します。また、偽の CAPTCHA プロンプトを使用したり、合法的なサービスを模倣して被害者を誘引するキャンペーンでは、技術的エクスプロイトとソーシャルエンジニアリングの統合が明白です。
これらの攻撃を支援するインフラはしばしば複雑で弾力的であり、脅威行為者はドメイン生成アルゴリズム（DGA）およびデータ漏洩および C2 作業のためのクラウドサービス使用のような技術を使用します。GitHub、Google Drive、AWS のような正当なインフラの使用は、検出および帰属の努力を複雑にします。さらに、商用 Malware とカスタム開発ツールの混合は、サイバー作戦に対するハイブリッドアプローチを示し、脅威行為者が変化する防御措置に迅速に適応できるようにします。
全体として、今月のサイバー脅威環境は高いレベルの技術的精巧さと戦略的計画が特徴であり、脅威行為者は高度な Malware、ソーシャルエンジニアリング、インフラ悪用の組み合わせを活用して彼らの目標を達成します。これらの脅威の持続的な特性と検出を回避し長期的なアクセスを維持する能力は、そのような攻撃に対抗する任務を負うサイバーセキュリティ専門家にとってかなりの挑戦を提起します。

今月のサイバー脅威の示唆点

最近観察されたサイバー脅威活動全般では、多様な攻撃主体が複合的な戦術と手段を活用する様相が確認される。該当活動では社会工学技法、Malware、ソフトウェア脆弱性悪用が結合された攻撃フローが観察され、APT 攻撃と関連した浸透方式が反復的に識別される。また、国家支援と財政的目的が混在した攻撃様相は、脅威行為者の活動動機が諜報収集、破壊行為、金銭的利益追求など様々な方向に分化されていることを示す。
一部の北朝鮮関連とされる活動では、サイバー犯罪的な攻撃が国家レベルの目的と結び付いているとみられる状況が観測されており、攻撃の目的と手段の間の境界が明確に区別されないという特徴が見られる。 さらに、特定 Malware 感染過程で攻撃者の運用インフラ一部が外部に露出した事例は、脅威行為者の運用方式とインフラ構成に対する制限的な観察情報を提供する。
一方、npm 生態系および OAuth 統合を狙った攻撃事例では、供給網を媒介とした侵入試みが確認され、第三者サービスが攻撃経路として活用される様相が見られます。これらの活動は、信頼関係を基盤とする外部サービスが侵害された場合、攻撃の影響範囲が広範囲に及ぶ可能性を示唆しています。また、CAPTCHA 回避マクロと求人手続きを悪用したフィッシング手法が観察され、社会工学に基

づく攻撃が継続的に活用されていることを示しています。これに加えて、WinRAR、Microsoft SharePoint など広く使用されているソフトウェアを対象とした脆弱性悪用事例が確認され、公開ソフトウェア環境全般が攻撃表面として活用されている様相が見られます。

BRICKSTORM および UDPGangster のような高級 Malware の配布は、持続性を維持し、検出を避けるために隠密な技術を使用する脅威行為者の進化する戦術を示している。Discord および Telegram のような合法的なサービスをコマンド＆コントロール通信に使用することは、検出の努力をさらに複雑にし、高度な行動モニタリングおよび異常検出システムの実装が必要である。Malware 配布およびコマンド＆コントロールのための公共クラウドインフラへの依存は、組織がクラウド環境に対する厳格なアクセス制御およびモニタリングを実装する必要性を強調している。

戦略的観点から、組織は脅威情報、事件対応および持続的なモニタリングを含む包括的なサイバーセキュリティ戦略の開発を優先すべきである。これは最新の脅威検出技術を備えた強力なセキュリティオペレーションセンター(SOC)を設立し、洗練された脅威を識別し対応できる熟練したアナリストを配置することを含む。産業の同僚との協力および情報共有イニシアチブに参加することにより、状況認識を向上させ、組織が新しい脅威に先んじることができるようにする。

これらの事件はまた、エネルギーおよび政府部門を対象としたキャンペーンで見られるように、重要なインフラセキュリティの重要性を強調している。これらの部門の組織は、外部および内部の脅威の両方に対して防御するために、階層化されたセキュリティ制御を含む深層防御アプローチを採用すべきである。ここにはネットワーク分割、侵入検出および防止システム、定期的なセキュリティ監査が含まれ、脆弱性を識別し修正する。

結論として、今月のサイバー脅威環境は、組織がサイバーセキュリティに対する積極的かつ包括的なアプローチを採用する必要性を強調している。高度な脅威検出および対応能力に投資し、ユーザー認識を高め、サプライチェーンおよび重要なインフラを保護することにより、組織は脅威行為者の洗練された進化する戦術に対してより良い防御ができる。これらの事件から得られた教訓は、戦略的計画に情報を提供し、将来の攻撃のリスクを軽減するためにサイバーセキュリティの実践の持続的な改善を推進すべきである。

今月に説明されたサイバー事件は、組織がサイバーセキュリティ態勢を強化する上で貴重な教訓を提供する。主要な教訓の一つは、強力な脅威情報能力を維持することの重要性である。偶発的な Malware 感染により北朝鮮国家支援作戦が露出したことは、敵の戦術、技術および手順(TTP)を理解する上で脅威情報の価値を強調している。組織は脅威情報プラットフォームに投資し、産業の同僚と協力して新しい脅威に関する洞察を得て防御を適切に調整すべきである。

もう一つの重要な教訓は、包括的なユーザー認識および教育プログラムの必要性である。CAPTCHA マクロや偽の求人申請書を含む洗練された社会工学技法の使用は、社会工学のリスクについて従業員を教育し、疑わしい活動を認識し報告する方法の重要性を強調している。定期的な教育セッションと模擬フィッシング演習は、良いサイバーセキュリティの実践を強化し、成功する攻撃の可能性を減らすのに役立つ。

これらの事件はまた、タイムリーなパッチ管理および脆弱性評価プロセスの重要性を強調している。

WinRAR および Microsoft SharePoint のような広く使用されているソフトウェアの脆弱性悪用は、組織がシステムが最新のセキュリティパッチで更新されることを保証するために強力なパッチ管理プログラムを実装する必要性を強調している。定期的な脆弱性評価および

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

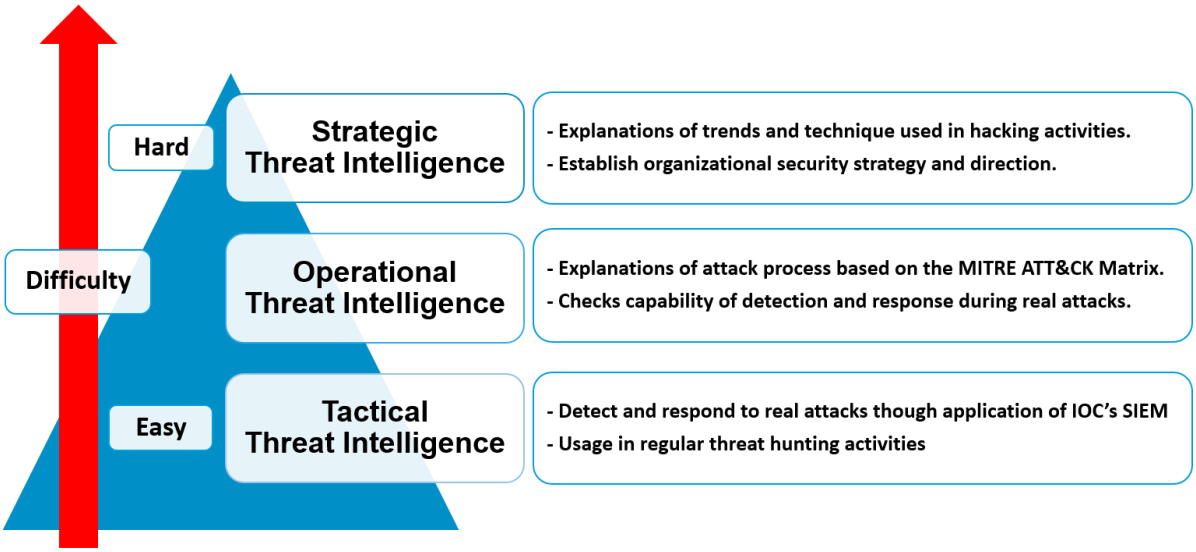
3. セキュリティ認識教育 (User Training)

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

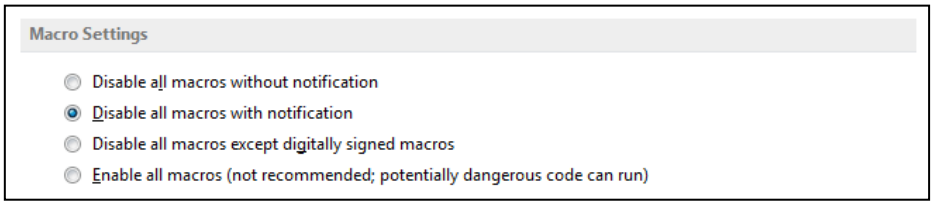
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

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.