NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI2025101302

月刊ハッキンググループの動向レポート

Monthly Threat Actor Group Intelligence Report

- twitter.com/nshcthreatrecon
- service@nshc.net

Nov 2025

NSHC PTE. LTD.

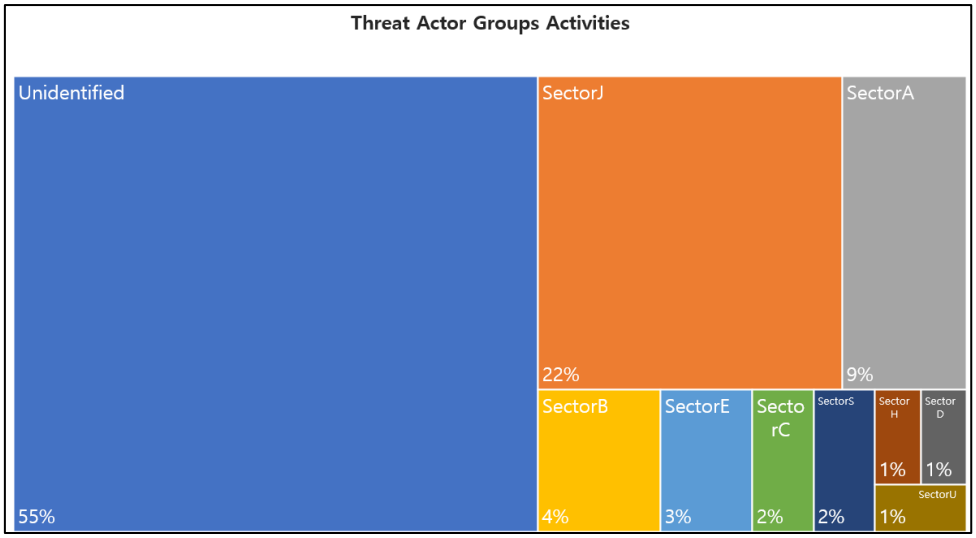
このレポートは 2025 年 8 月 21 日から 2025 年 9 月 20 日まで見つけた政府支援のハッキンググループ活動と関係あるイッシューを説明し、それに伴う侵害事故の情報と ThreatRecon Platform 内のイベント情報を含む。

Table of Contents

エグゼクティブサマリー

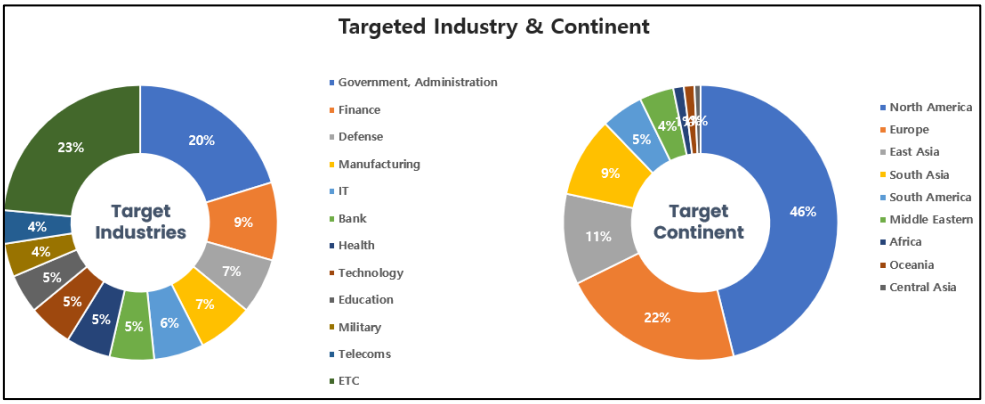
2025 年 8 月 21 日から 2025 年 9 月 20 日までの間に NSHC 脅威分析研究所（Threat Research Lab）が収集したデータと情報に基づいて分析したハッキンググループ（Threat Actor Group）の活動を要約した内容です。

今回の 9 月には、合計 92 のハッキンググループの活動が確認されており、確認されていない未識別（Unidentified）グループが 55%で最も多く、SectorJ、SectorA グループの活動がそれに続きました。



[図 1: 2025 年 9 月に確認されたハッキンググループ別活動統計]

今年 9 月に発見されたハッキンググループのハッキング活動は、政府機関や金融業界に従事する関係者またはシステムを対象に最も多くの攻撃を行い、地域別では北アメリカとヨーロッパに位置する国々を対象としたハッキング活動が最も多いことが確認されています。



[図 2: 2025 年 9 月に攻撃対象となった産業分野と国の統計]

SectorA グループのハッキング活動を分析すると、主にソーシャルエンジニアリング技術と精巧なマルウェアを組み合わせた攻撃を主導していると判断されます。BeaverTail や InvisibleFerret のようなマルウェアは、暗号通貨および小売業部門のマーケティング・取引担当者をターゲットにしており、偽の求人ウェブサイトを通じて配布されます。攻撃者は ClickFix 技術を使用して、被害者がコンパイルされた実行ファイルを直接実行するよう誘導し、スクリプトベースの配布から実行ファイル配布に切り替えた状況が見られます。内部調整には Slack を活用し、インフラを迅速に交換して高い被害者参加度を維持しようとする活動が観察され、分散されたコマンド構造と迅速なインフラ転換を好む傾向が明らかになります。Windows と macOS を狙ったケースでは、Nvidia アップデートに偽装した悪意のあるソフトウェアを配布し、心理的信頼を利用してインストールを誘導します。また、Chrome ゼロデイ脆弱性を悪用したスパイウェア事件では、PondRAT と ThemeForestRAT がファイル操作およびシステム情報収集に使用され、国家情報および学術部門を対象としたフィッシングでは、LNK ファイルが PowerShell スクリプトを実行して追加ペイロードを配布し、マルウェアはクラウドサービスを通じて C2 を実行します。全体的にデータ窃取とリモートアクセスを目的としており、検出回避性と持続性を強調します。特に AI 生成スピアフィッシングは、高度な偽装で従来の防御を困難にします。

SectorB グループは、多層的な戦術と高度に洗練された Malware の開発を中心に活動しています。スピアフィッシング、ドメイン登録、ソフトウェアアップデートの乗っ取りなど、さまざまな手法でアプローチし、Visual Studio Code Remote Tunnels のようなツールを用いてリモートアクセスを持続させ、検出を回避する事例が報告されています。Python ローダーWhirlCoil を通じた攻撃実行が特徴であり、データ流出は主にクラウドサービスを通じて行われます。ネットワークインフラの脆弱性を利用して長期的なアクセスを維持し、ルーター設定の変更やトラフィックミラーリングなどで検出を回避する点が際立っており、プロトコルベースの回避と認証メカニズムの無力化を通じて持続性を確保します。Malware は情報窃取、リモートアクセス、バックドア機能を複合的に実行し、ToneShell は DLL サイドローディングや偽の TLS 通信を、SnakeDisk は USB 伝播を通じて地域 IP ベースの標的動作を行います。コード難読化、マシン ID、GUID ベースのホスト識別などでセキュリティシステムの回避を試みる様子が観察され、分析妨害を目的として AI プラットフォームからコピーしたテキストを含む事例も確認されています。

SectorC グループは、ウクライナの軍事・行政構造を主要なターゲットとし、高度な技術を駆使して複合攻撃を行います。スピアフィッシングを通じて Signal を媒介にし、マルウェアを含む Office 文書を配布し、マクロは COM ハイジャックを利用して DLL をロードし、PNG に隠されたシェルコードを抽出して Covenant の GruntHTTPStager を実行し、Koofr クラウドインフラを通じて通信チャネルを構築します。BeardShell 配信段階では icedrive を C2 として使用し、SlimAgent インプラントを通じてキーロギング・スクリーンショット機能が統合される可能性が指摘されています。

NotDoor バックドアは OneDrive.exe を悪用した DLL サイドローディングで VBA マクロをインストールし、暗号化された識別子とコマンドを含むメールで動作し、暗号化された PowerShell コマンドでデータの窃取・ファイルのアップロード・コマンドの実行を行います。Outlook イベントを利用

した持続性の維持とマクロ実行の保証技術も確認されており、PteroGraphin を通じた Kazuar の再起動およびウォータリングホールキャンペーンは、JavaScript 難読化・サーバーサイドリダイレクトでマルウェアインフラに誘導し、クラウドトンネルを通じてマルウェアトラフィックを合法的な暗号化トンネルに隠し、Dropbox を使用してデータの窃取を行います。カザフスタンのエネルギー部門をターゲットとしたケースでは、内部 IT 通信を装ったスピアフィッシングで多段階感染チェーンが運営されました。

SectorD グループは精巧で組織的な攻撃を行い、2025 年 8 月に検出されたフィッシングキャンペーンではオマーン外務省を装ってグローバルな外交機関を標的にしました。ハッキングされたメールアカウントを通じて悪意のある Word 文書を送信し、文書内のエンコードされたコンテンツは VBA マクロでデコードされ、sysProcUpdate マルウェアを配布しました。合法的なインフラの活用、エンコードされたペイロード・実行遅延メカニズムを通じた検出回避戦術を駆使し、収集した偵察データで目標システムを長期観察します。マルウェアはシステムメタデータの収集、一般ディレクトリの隠蔽、C2 通信を行い、インフラには VPN が使用されて地理的起源の隠蔽が確認され、ヨーロッパ、アフリカ、国際機関を同時に標的にしました。

SectorE グループは、GitHub を悪用してセキュリティ専門家や大企業を対象にマルウェアを配布することに注力しています。トロイの木馬をプロジェクトファイルに挿入し、コンパイル時に自動実行されるように設計し、プロセスインジェクション、DLL ホローイング、コード難読化を用いて検出を回避し、生産性ツール API を悪用してセキュリティ対策を迂回します。MSC ファイルと GrimResource を組み合わせた攻撃でパキスタンの機関を標的にし、フィッシングを通じて悪意のあるペイロードを配布します。南アジアの標的には、LNK ファイルを ZIP に入れて配布し、リモート URL スクリプトの実行を誘導して条件付きで追加のペイロードを復号・実行する多層難読化技法を使用します。モバイルと Windows のマルウェアを組み合わせた事例や、予約タスク・自動起動項目を利用した持続性の確保も観察されています。

SectorF グループは、高度な TTPs に基づく活動を示しており、発見されたマルウェア DLL はトロイの木馬ローダーとして機能します。動的 API 取得のためのハッシュ使用、Global¥MicrosoftMPI ミューテックスの生成による単一インスタンスの保証、コマンドラインパラメータ検査の回避、レジストリのスタートアップ項目を通じた持続性の確保を行います。反射型 DLL ローディング・動的 API アドレス検索などで初期化し、certmgr.dll の.text セクションコード置換を通じた DLL ホロウイングで RAT をロードする手法が使用されます。シェルコードの配布と環境特化開発ツールの使用は、過去の高度な脅威行為者と類似しており、持続的なアクセス維持に重点を置いています。

SectorH グループは、インド内の組織を標的にして Linux 環境を狙った独特な感染戦略を実行しています。武器化された.desktop ショートカットファイルを使用して検出を回避し、MeshAgent ペイロードでリモートアクセスを確保します。感染チェーンは、デコイ PDF で注意をそらしながらバックグラウンドで悪性ルーチンを実行し、多段階で進行します。攻撃は、デコイドキュメント・デコーダー・暗号化されたファイルのダウンロードを含み、Google Docs などのプラットフォームを活用して検出を避けるファイル作成技術を適用しています。最終ペイロードである MeshAgent は、活動

モニタリング・横方向移動・データ流出機能を提供し、インフラは AWS ホスティング C2 で追跡され、調整されたオペレーションが疑われます。2025 年 8 月に開始されたキャンペーンでは、悪性 ZIP 内に PDF に偽装した'.desktop'ファイルが含まれており、実行時に Google Drive から Go バイナリペイロードをダウンロードして実行し、アンチデバッグ・アンチサンドボックスチェックで検出を回避し、WebSockets で C2 接続を維持します。

SectorS グループは、コロンビア政府機関を中心に 2024 年から 2025 年まで、5 つの活動クラスターに分けられた作戦を実行しました。オープンソースやクラックされたリモートアクセス型トロイの木馬（AsyncRAT、DcRAT、REMCOS など）をスピアフィッシングで配布し、ステガノグラフィーで Malware を隠蔽し、GitHub や Discord のような合法的なプラットフォームを通じてペイロードを配信します。ドメイン生成アルゴリズム（DGA）と地理的検出回避を通じて持続性を確保し、インフラには VPN やリバースプロキシに見えるコンプロマイズされたシステムを含め、C2 や通信の隠蔽を試みます。キャンペーンは資格情報の窃取、スパイ活動、金融的な偽装を並行して行い、政府、金融、エネルギー、ヘルスケアを標的とします。

SectorJ グループは、電子商取引の決済情報の窃取（JavaScript インジェクション）、サプライチェーン攻撃、巧妙なフィッシングおよびランサムウェアの配布など、さまざまな手法を見せています。cc-analytics[.]com などのドメインを通じてスクリプトを配布し、検出回避を試みており、DeskSoft EarthTime に偽装したマルウェアファイルの事例、SectopRAT・SystemBC を利用した C2 接続および横方向移動、RDP・wmiexec を活用したドメインコントローラーの標的化が観察されています。金融を標的としたサプライチェーン攻撃では、msdtctm.dll を悪用したバックドア配布と AdaptixC2 の構築を通じて作戦を拡大し、Microsoft Teams を利用したソーシャルエンジニアリングでリモートアクセスソフトウェアのインストールを誘導し、DarkGate・Matanbuchus ローダーを配布しました。認証情報の窃取・リモートコード実行・暗号化された C2 通信を通じたデータ窃取が頻繁に行われており、Redis 設定の悪用を通じたクリプトジャッキングや QR コードベースのフィッシングで高価値の標的を狙う事例も報告されています。

詳細情報

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

1) SectorA01 used Malware disguised as Nvidia software for attacks (2025-08-28)

https://cti.nshc.net/events/view/18073

攻撃対象産業群: 金融

脅威行為者はソーシャルエンジニアリング技法、特に「ClickFix」手法を利用して、Windows および macOS システムを対象にサイバー攻撃を実行しました。この攻撃は、求職機会に偽装したフィッシング手法を使用して被害者を偽のインタビューウェブサイトに誘導しました。被害者はカメラの不具合を修正するよう指示され、Nvidia のアップデートに偽装したマルウェアをダウンロードして実行するよう誘導されました。この配布方法は、ClickFix-1.bat のような悪意のあるスクリプトを実行して、指定されたサーバーから有害なアーカイブをダウンロードさせるものでした。アーカイブが開かれると、複数のスクリプトが実行され、Node.js 環境を構築し、BeaverTail マルウェアを実行してプラットフォーム間でデータを窃取しました。Windows 11 では、追加のバックドア drvUpdate.exe が実行されました。このバックドアはコマンドを実行し、ファイルを操作でき、コマンド＆コントロールサーバーと通信します。macOS の亜種は、arm64 アーキテクチャツールに偽装したマルウェアをダウンロードして実行するためにシェルスクリプトを使用しました。このキャンペーンは、人間の心理を悪用して巧妙なマルウェアを複数のプラットフォームに配布する脅威行為者の依存性を示しています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 偽の求人機会でフィッシングメール送信
   b. 被害者を偽のインタビューウェブサイトに誘導
2. [実行] ユーザー実行 (T1204)
   a. Nvidia アップデートに偽装したマルウェアのダウンロードと実行
   b. ClickFix-1.bat スクリプトを実行してマルウェアアーカイブをダウンロード
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. Windows システムで drvUpdate.exe バックドアを実行
   b. macOS システムで plist ファイルを利用した持続性設定
4. [防御回避] 偽装 (T1036)
   a. Nvidia ソフトウェアアップデートにマルウェアを偽装
   b. arm64 アーキテクチャツールにマルウェアを偽装
5. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. コマンド＆コントロールサーバーと通信
   b. サーバーから命令を受信し、ファイル操作を実行
6. [収集] ローカルシステムからのデータ (T1005)
   a. Node.js 環境で BeaverTail マルウェアを実行
   b. プラットフォーム間でデータ窃取を実行
7. [流出] C2 チャネル経由のデータ流出 (T1041)
   a. 収集されたデータを C2 サーバーに送信
   b. BeaverTail を通じて継続的なデータ窃取を実行

2) SectorA01 used RATs disguised as trading company employee access (2025-09-01)

https://cti.nshc.net/events/view/18171

攻撃対象産業群: 金融

攻撃者は 2024 年に分散型金融分野を対象に高度なサイバースパイ活動を行いました。攻撃者は Telegram で取引会社の従業員を装い、偽のスケジュールウェブサイトを利用して被害者と接触を試みました。初期のアクセスは Chrome のゼロデイ脆弱性を通じて行われ、PondRAT、ThemeForestRAT、そしてその後にはより高度な RemotePE RAT が配布されました。
PondRAT は第一段階のペイロードとして使用され、攻撃者がファイルを読み書きし、コマンドを実行できるようにしました。これは Base64 でエンコードされ、XOR で暗号化されたメッセージを使用して C2 サーバーと通信しました。ThemeForestRAT は PondRAT と共に使用され、主にメモリ内で動作し、ファイル操作やシステム情報の検索などの拡張機能を提供しました。
攻撃は機密データを窃取し、Mimikatz のようなツールを活用して資格情報を収集し、PerfhLoader を使用した DLL ハイジャックを通じて持続性を維持しました。今回の事件は経済的動機と技術的な高度さを反映し、隠密性と持続性を優先しました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. Telegram で取引会社の社員を装う
   b. 偽のスケジュールウェブサイトを使用して被害者に接触
2. [実行] クライアント実行のためのエクスプロイト (T1203)
   a. Chrome ゼロデイ脆弱性の活用
   b. PondRAT の配布と実行
3. [持続性] DLL 検索順序ハイジャック (T1574.001)
   a. PerfhLoader を通じた持続性の維持
   b. SessionEnv サービス設定の修正
4. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. Mimikatz を使用して資格情報を収集
   b. ブラウザのクッキーおよび資格情報のダンプ
5. [発見] システムネットワーク構成の発見 (T1016)
   a. ネットワーク内の活動を探索
   b. システム情報の収集
6. [収集] スクリーンキャプチャ (T1113)
   a. スクリーンショットの収集

7. [収集] 入力キャプチャ: キーロギング (T1417.001)
   a. キーロギングを通じたユーザー活動の記録
8. [コマンドと制御] 暗号化チャネル (T1573)
   a. Base64 および XOR 暗号化を通じた C2 通信
   b. C2 サーバーとの定期的な通信の維持
9. [防御回避] ホスト上のインジケーター削除 (T1070)
   a. PondRAT および ThemeForestRAT の痕跡削除
   b. RemotePE のインストールと実行
10. [データ抽出] C2 チャネルを介したデータ抽出 (T1041)
   a. 盗まれたデータを C2 サーバーに送信
   b. 秘密裏にデータ漏洩を実行

3) SectorA01 used ClickFix social engineering for fraudulent job lures (2025-09-04)

https://cti.nshc.net/events/view/18265

攻撃対象産業群: 金融

攻撃者は 2025 年 1 月から 6 月の間にサイバー脅威インテリジェンスを監視し、攻撃戦略を改善しました。攻撃者は既存の資産が損傷した場合、迅速に新しいインフラを展開し、高い被害者の関与を維持しました。Slack を利用した調整や Validin、VirusTotal、Maltrail のようなソースを情報収集に活用し、分散された指令構造により大規模なインフラ変更を制限しました。攻撃ベクターには、暗号通貨分野の求人提案を装った社会工学的手法が含まれていました。ClickFix のような手法を使用して求職者にコマンド実行を要求し、フィッシングを通じてマルウェアを配布しました。グループのインフラは散発的なセキュリティ向上により検出可能であり、戦略的に運用準備状態を優先し、広範囲な修正よりもインフラの置き換えに機敏性を好みました。これは内部の競争圧力や分散された統制などの内部要因により、既存の資産を体系的に保護するよりもインフラを迅速に交換する傾向を反映しています。

[Attack Flow]

1. [偵察] 被害者の身元情報を収集 (T1589)
   a. 暗号通貨産業対象の求職者情報収集
2. [リソース開発] インフラストラクチャの取得 (T1583)
   a. 新しいインフラの配置
   b. 既存資産の損傷時の代替
3. [初期アクセス] フィッシング (T1566)
   a. 暗号通貨分野の求職提案に偽装
   b. ClickFix 技法の使用

4. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. 求職者にコマンド実行を誘導
   b. コマンド実行で Malware を伝達
5. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
   a. Slack を通じたチーム協力
   b. リアルタイムインフラ監視
6. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. インフラ変更の限定的適用
   b. 検出回避のための散発的変更
7. [収集] 情報リポジトリからのデータ (T1213)
   a. Validin、VirusTotal、Maltrail の活用
   b. インフラ関連情報の収集

4) SectorA01 used BeaverTail Malware disguised as job application site (2025-09-17)

https://cti.nshc.net/events/view/18656

攻撃対象産業群: 小売、マーケティング

2025 年 5 月末、国家主導の脅威行為者は、暗号通貨および小売部門のマーケティングおよびトレーダー役割をターゲットにしたキャンペーンを開始しました。この作戦は ClickFix の誘引策を使用して、BeaverTail および InvisibleFerret マルウェアを配布しました。脅威行為者は、Vercel プロジェクトにホスティングされた偽の求人ウェブサイト businesshire[.]top を構築し、求職者を欺きました。マルウェアはスクリプトではなく、コンパイルされた実行ファイルとして配布され、戦術的な変化を示しました。ウェブサイトは偽の就職機会と問題解決のアドバイスを提示し、ユーザーがこれらのマルウェアバイナリを実行するよう誘導しました。バックエンドインフラは nvidiasdk.fly[.]dev にホスティングされ、ブラウザから暗号通貨ウォレットデータにアクセスし、盗もうとしました。macOS、Windows、Linux の感染チェーンは、bash スクリプト、Python 依存関係、および JavaScript を活用して BeaverTail および InvisibleFerret を配布しました。マルウェアは暗号通貨拡張機能をターゲットにして、情報の窃取およびリモートアクセスを試みました。このキャンペーンは、より広範な目標のための戦略的変化を示唆し、潜在的な将来の作戦アプローチの適応可能性を示しています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 偽の採用ウェブサイトの構築
   b. 偽の就職機会を通じてユーザーを誘導
2. [実行] ユーザー実行 (T1204)

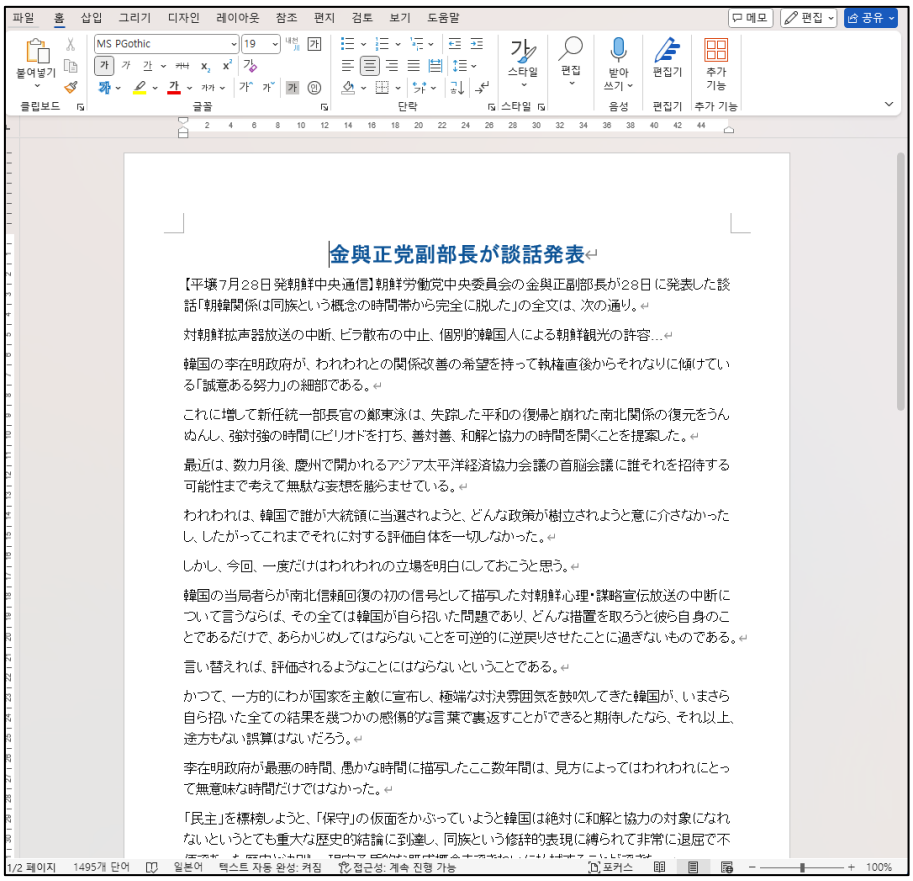
a. マルウェア実行ファイルへの誘導
b. 問題解決のアドバイスを提供してマルウェア実行を誘導
3. [防御回避] 偽装 (T1036)
a. コンパイルされた実行ファイルで配布して検出回避
b. ユーザーエージェントベースの動作で検出回避
4. [資格情報アクセス] 資格情報ダンピング (T1003)
a. ブラウザから暗号通貨ウォレットデータへのアクセス試行
b. システム資格情報の窃取
5. [データ流出] ウェブサービス経由のデータ流出 (T1567)
a. 窃取したデータをバックエンドサーバーに送信
b. 暗号通貨ウォレット情報の窃取および送信
6. [コマンド＆コントロール] ウェブサービス経由の C2 (T1102)
a. C2 サーバーへのデータ送信
b. リモート制御および情報収集

5) SectorA02 used LNK Malware disguised as a research newsletter (2025-08-29)

https://cti.nshc.net/events/view/18090

攻撃対象産業群: 政府・行政、学界 - 大学、シンクタンク

攻撃者は「国家情報研究会ニュースレター（第 52 号）」というタイトルの誘引文書を使用して、韓国の国家情報および学術機関を対象としたサイバー脅威キャンペーンを実施しました。攻撃者は PDF 文書に偽装した悪性 LNK ファイルを配布し、実行時に追加のペイロードのダウンロードを開始しました。この攻撃の目的はスパイ活動とデータ窃取であり、国家情報研究会に関連する人物を標的としました。攻撃は北朝鮮国家の支援を受けたグループによって実行され、精巧なスピアフィッシング技術が使用されました。感染チェーンは LNK ファイルの実行から始まり、これは追加のペイロードを抽出して実行するための PowerShell スクリプトを含んでいました。これらのスクリプトは難読化されており、ディスクに記録せずにメモリ内でペイロードを配布する多段階の実行を含み、従来の防御を回避しました。また、このキャンペーンは PowerShell を利用した反射的 DLL インジェクションを悪用し、韓国および周辺国の政府および研究部門を標的としました。マルウェアはクラウドサービスを含むリモートサーバーをコマンド＆コントロール（C2）として使用し、データ流出を容易にしました。感染したシステムでは合法的なブラウザベースの活動に偽装した隠密なデータ収集を行い、遅延および削除を通じて痕跡を整理しました。



金與正党副部長が談話発表

【平壌7月28日発朝鮮中央通信】朝鮮労働党中央委員会の金與正副部長が28日に発表した談話「朝韓関係は同族という概念の時間帯から完全に脱した」の全文は、次の通り。

対朝鮮拡声器放送の中断、ビラ散布の中止、個別的韓国人による朝鮮観光の許容…

韓国の李在明政府が、われわれとの関係改善の希望を持って執権直後からそれなりに傾けている「誠意ある努力」の細部である。

これに増して新任統一部長官の鄭東泳は、失踪した平和の復帰と崩れた南北関係の復元をうんぬんし、強対強の時間にピリオドを打ち、善対善、和解と協力の時間を開くことを提案した。

最近は、数カ月後、慶州で開かれるアジア太平洋経済協力会議の首脳会議に誰それを招待する可能性まで考えて無駄な妄想を膨らませている。

われわれは、韓国で誰が大統領に当選されようと、どんな政策が樹立されようと意に介さなかったし、したがってこれまでそれに対する評価自体を一切しなかった。

しかし、今回、一度だけはわれわれの立場を明白にしておこうと思う。

韓国の当局者らが南北信頼回復の初の信号として描写した対朝鮮心理・謀略宣伝放送の中断について言うならば、その全ては韓国が自ら招いた問題であり、どんな措置を取ろうと彼ら自身のことであるだけで、あらかじめしてはならないことを可逆的に逆戻りさせたことに過ぎないものである。

言い替えれば、評価されるようなことにはならないということである。

かつて、一方的にわが国家を主敵に宣布し、極端な対決雰囲気を鼓吹してきた韓国が、いまさら自ら招いた全ての結果を幾つかの感傷的な言葉で裏返すことができると期待したなら、それ以上、途方もない誤算はないだろう。

李在明政府が最悪の時間、愚かな時間に描写したここ数年間は、見方によってはわれわれにとって無意味な時間だけではなかった。

「民主」を標榜しようと、「保守」の仮面をかぶっていようと韓国は絶対に和解と協力の対象になれないというとても重大な歴史的結論に到達し、同族という修辞的表現に縛られて非常に退屈で不

[図 3: SectorA02 グループが利用した文書]

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. 誘引文書「国家情報研究会ニュースレター (52 号)」使用
   b. PDF に偽装したマルウェア LNK ファイル配布
2. [実行] コマンドとスクリプトインタープリター: PowerShell (T1059.001)
   a. PowerShell スクリプト実行で追加ペイロード抽出
   b. 難読化されたスクリプトでメモリ内実行
3. [防御回避] 難読化解除/ファイルまたは情報のデコード (T1140)
   a. PowerShell を通じたファイル難読化解除
   b. 反射的 DLL インジェクション技術使用
4. [資格情報アクセス] 入力キャプチャ: キーロギング (T1056.002)
   a. キー入力監視
   b. GUI 入力キャプチャ
5. [収集] オーディオキャプチャ (T1123)
   a. システムオーディオ録音
   b. 収集されたデータ送信準備
6. [データ流出] C2 チャネル経由のデータ流出 (T1041)

a. クラウドサービス経由のデータ流出
b. C2 サーバーへのファイルアップロード
7. [影響] システムシャットダウン/再起動 (T1529)
a. システム終了コマンド実行
b. マルウェア実行終了および削除

6) SectorA03 used APT NAKSOO Malware disguised via GitHub payloads (2025-09-16)

https://cti.nshc.net/events/view/18738

攻撃対象産業群: 国防、軍事機関、外交、貿易

攻撃者は 2018 年から活動を開始し、中国、北朝鮮、日本、シンガポールなどの東北アジア諸国を対象にサイバースパイ活動および機密情報の窃取を行ってきました。政治、外交、軍事、学界、貿易、人事部門を中心に攻撃を展開しました。攻撃者は主にスピアフィッシングとブラウザのゼロデイ脆弱性を利用して標的に侵入しました。最近では、NAKSOO というカスタムリモートコントロール Malware を活用しており、これはバージョン v3.1.14 に進化し、XOR および非標準 RC4 暗号化アルゴリズムを使用して通信していました。攻撃は「一帯一路」をテーマにしたフィッシングメールで始まり、検出を回避できる VHDX ファイルを活用しました。その後、攻撃チェーンはホワイトとブラックの手法を使用して予約タスクを設定し、COM レジストリ DLL ハイジャックを通じてリモートローダーを配布しました。このローダーは GitHub リポジトリに接続して暗号化されたペイロードをダウンロードすることで持続性を確保し、データ窃取やリモートコントロールなどのさまざまな悪意のある機能を実行しました。Malware は DLL インジェクションと暗号化された通信を通じて高い隠蔽性を示し、痕跡を隠し複雑な攻撃ベクトルを実行する上で高度な能力を強調しました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566.001)
a. 「一帯一路」をテーマにしたフィッシングメールの送信
b. VHDX ファイルの添付で検出回避
2. [実行] コマンドとスクリプトインタープリタ (T1059)
a. LNK ファイルを通じて gbash.exe を実行
b. bashcfg.txt を使用してコマンドを実行
3. [持続性] スケジュールされたタスク/ジョブ (T1053.005)
a. スケジュールされたタスクを通じて持続性を確保
b. COM レジストリ DLL ハイジャック
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. XOR および RC4 暗号化で通信を保護

b. 非標準アルゴリズムの使用

5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. DLL インジェクションで資格情報を窃取
   b. Powershell スクリプトで情報を収集
6. [探索] システム情報探索 (T1082)
   a. システム情報の収集と外部 IP アドレスの確認
   b. statcounter.com を活用した情報収集
7. [横移動] リモートサービス (T1021)
   a. リモートローダーを通じて GitHub からペイロードをダウンロード
   b. COM インターフェースの活用
8. [収集] ローカルシステムからのデータ (T1005)
   a. 主要ディレクトリのファイルを収集
   b. データ窃取プラグインの実行
9. [コマンドと制御] 暗号化されたチャネル (T1573)
   a. 非標準 RC4 アルゴリズムを使用した暗号化チャネル
   b. GitHub および C2 サーバーとの暗号化通信
10. [流出] C2 チャネルを介した流出 (T1041)
    a. NAKSOO を通じてデータを送信
    b. POST リクエストで C2 サーバーに結果を伝達

7) SectorA05 used Phishing Email disguised as NTS Notification (2025-08-25)

https://cti.nshc.net/events/view/18376

攻撃者は国税庁を装い、ネイバーアカウントの資格情報を盗むためのフィッシングキャンペーンを実施しました。フィッシングメールは国税庁から送信されたように偽装され、受信者に 9 月の税金申告に関連する電子文書が届いたというメッセージを伝え、2025 年 8 月 31 日までに確認するよう緊急性を持たせていました。メールは SPF、DKIM、DMARC、ARC 認証をすべて通過するよう巧妙に作成され、Mail.ru インフラを通じて送信されました。メールにはネイバーログインページを装ったマルウェアリンクが含まれており、リンクの URL は ROT13 とパーセントエンコーディングを通じて複雑に暗号化され、悪意のある意図を隠していました。フィッシング戦略は、受信者のメールアドレスを URL に含めて個別化された攻撃を行うことで、ユーザーの資格情報を収集するための巧妙な手段を示していました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 国税庁を装ったメール送信

b. 緊急性を強調し、電子文書の確認を要求
2. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. ROT13 およびパーセントエンコーディングの使用
b. SPF、DKIM、DMARC、ARC の通過
3. [認証情報アクセス] 認証情報収集 (T1110)
a. ネイバーのログインページに偽装
b. パーソナライズされた URL で受信者のメールを含む
4. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
a. TLSv1.3 暗号化の使用
b. ネイバーとの通信暗号化が正常に動作

8) SectorA05 used LNK Malware disguised as UNC Invitation PDF (2025-08-29)

https://cti.nshc.net/events/view/18077

攻撃対象産業群: 外交

「Update Schedule_INVITATION - 250625 UNC Ambassador's Roundtable.zip」というファイルに偽装して南ヨーロッパの外交部を狙ったマルウェア活動が行われました。この攻撃は 2025 年 6 月 10 日に「Chang Hyo Chong Eric」という名前で landf5503@gmail.com からフィッシングメールを通じて実行されました。この圧縮ファイルはパスワードで保護されており、解凍すると PDF に偽装されたマルウェアショートカットファイルが現れます。マルウェアは GitHub から追加のペイロードをダウンロードするための内蔵コードを使用し、スケジュールされたタスクを通じて持続性を維持しました。技術的な流れは、餌の PDF をダウンロードし、追加のステップをダウンロードするための PowerShell スクリプトを実行し、スケジュールされたタスクを通じて持続性を維持する方式で進行しました。マルウェアは GitHub からファイルを取得し、HTTP ヘッダーを操作して認証トークンを含む生のコンテンツを収集しました。この作戦は外交機関を対象としており、検出を回避するために隠蔽およびクラウドサービスの悪用技術を活用しました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566.001)
a. フィッシングメール送信
b. 外交部対象攻撃
2. [実行] ユーザー実行 (T1204.002)
a. PDF に偽装されたショートカットファイル
b. PowerShell スクリプト実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. ファイル偽装および暗号化

b. HTTP ヘッダー操作
4. [持続性] スケジュールされたタスク/ジョブ (T1053.005)
a. スケジュールタスク作成
b. 持続性維持
5. [コマンド＆コントロール] ウェブサービス (T1102.003)
a. GitHub からペイロードダウンロード
b. HTTP リクエストを通じたデータ送信
6. [データ流出] ウェブサービス経由のデータ流出 (T1567.002)
a. GitHub へのデータ送信
b. 認証トークン使用

9) SectorA05 used PowerShell Malware variant (2025-09-03)

https://cti.nshc.net/events/view/18209

PowerShell スクリプトは、感染した PC から情報を収集し、Dropbox に流出させ、二次ペイロードをダウンロードするために設計されました。攻撃は特定の外交団体をターゲットにしており、PowerShell を使用して実行中のプロセス、OS バージョン、IP アドレス、およびアンチウイルス情報を収集しました。収集された情報は一時ファイルに保存された後、アクセストークンを使用して Dropbox にアップロードされました。スクリプトは検出を避けるためにローカルファイルを自己削除しました。さらに、Dropbox からペイロードを受信し、バッチファイルを通じて密かに実行しました。スクリプトは Dropbox API を活用してファイルを管理し、セキュリティ対策を回避し、スケジュールされたタスクを通じて持続性を維持する手法を示しています。マルウェアインフラは、リモート C&C サーバーから実行ファイルとスクリプトをダウンロードして感染システムに対する制御を維持しようとする高度な試みを示しています。

[Attack Flow]

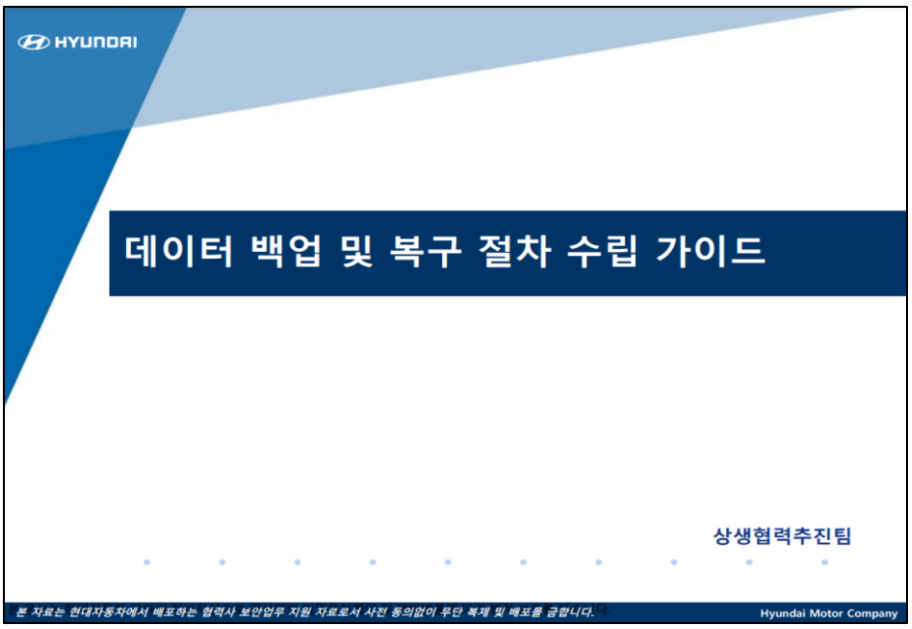
1. [実行] コマンドおよびスクリプトインタープリター: PowerShell (T1059.001)
a. PowerShell スクリプトを通じてマルウェアの動作を実行
b. バッチファイルを通じて追加のペイロードを実行
2. [収集] ローカルシステムからのデータ (T1005)
a. 実行中のプロセス収集 (Get-Process)
b. OS バージョンおよびグローバル IP アドレスの収集（Env、nslookup）
c. ワクチン製品情報の収集 (Get-CimInstance)
3. [資格情報アクセス] ファイル内の資格情報 (T1081)
a. Dropbox アクセストークンの使用
4. [データ抽出] 代替プロトコルを介したデータ抽出 (T1048)

a. 収集された情報を Dropbox にアップロード (Invoke-RestMethod)
b. 一時ファイルの削除 (Remove-Item)
5. [コマンド・アンド・コントロール] アプリケーション層プロトコル (T1071)
a. Dropbox API を通じたファイルのダウンロードおよびアップロード
b. リモート C&C サーバーから追加のペイロードをダウンロード
6. [永続性] スケジュールされたタスク/ジョブ (T1053.005)
a. 予約タスクの作成による持続性の確保 (schtasks)

10) SectorA05 used LNK Malware disguised as Data Recovery Procedure (2025-09-11)

https://cti.nshc.net/events/view/18482

攻撃者は 52MB の「現代データ復旧および手続き確立.lnk」ファイルを使用して、マルウェアペイロードを配信しました。この LNK ファイルは PDF に偽装され、システムを標的にしました。攻撃の核心は PowerShell を利用した実行であり、「%WINDIR%¥SysWow64¥WindowsPowerShell¥v1.0」のようなディレクトリ内に隠され、検出を回避しました。マルウェアは rshell.exe ファイルを見つけて呼び出し、実行されました。また、LNK ファイルの異常なサイズを利用して悪意のある意図を示しました。LNK ファイルはオフセット 0x00001046 でデコイ PDF を抽出し、XOR 0xAD 暗号化を通じて隠された実際の悪性実行ファイル「C:¥tempcaches¥ms.exe」を保存しました。補助ペイロードである「ms.exe.manifest」は、実行ファイルを管理者権限または互換モードで実行するように設計されています。攻撃は 10 分および 11 分の周期でこれらの実行ファイルを実行するタスクを予約し、持続性を確保しました。「C:¥tempcaches」ディレクトリの生成を隠し、元の LNK ファイルを削除して痕跡を隠蔽しました。この攻撃は、Windows 10 環境でシステムおよびプロセス情報を収集することを目的としており、仮想マシンに重点を置いている可能性があります。



[図 4: SectorA05 グループが使用したおとり文書]

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. PDF に偽装した LNK ファイル
   b. 大容量 LNK ファイルを通じた誘引
2. [実行] PowerShell (T1059.001)
   a. PowerShell を通じたマルウェア実行
   b. rshell.exe ファイルの探索および呼び出し
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. XOR 0xAD 暗号化の使用
   b. ディレクトリの隠し属性設定
4. [持続性] スケジュールされたタスク/ジョブ (T1053.005)
   a. 10 分および 11 分周期でのタスクスケジュール
   b. ms.exe および cache.vbs の実行
5. [発見] システム情報の発見 (T1082)
   a. システム情報の収集
   b. プロセスリストの収集
6. [収集] ローカルシステムからのデータ (T1005)
   a. Windows 10 環境の情報収集
   b. 仮想マシン情報の収集
7. [流出] C2 チャネルを通じた流出 (T1041)
   a. 収集された情報の外部送信
   b. ネットワークトラフィックを通じたデータ流出

11) SectorA05 used Deepfake AI to Impersonate Military ID Tasks (2025-09-15)

https://cti.nshc.net/events/view/18590

攻撃対象産業群: 防衛、金融、政府・行政

2025 年 7 月 17 日、韓国の防衛機関を装って個人を対象としたスピアフィッシング攻撃が行われました。攻撃者は生成 AI を活用して軍事身分証のディープフェイク画像を作成し、ID 発行業務を悪用しました。フィッシングメールには悪意のある Windows ショートカット（LNK）ファイルが含まれており、これはコマンド＆コントロールサーバーに接続する PowerShell コマンドを実行し、ディープフェイク PNG 画像とバッチスクリプトをダウンロードしました。バッチスクリプトは難読化された文字を含み、追加の悪意のある活動を行い、同じサーバーに接続してソフトウェアアップデートに偽装された CAB ファイルをダウンロードしました。このファイルはタスクスケジューラに登録され、定期的に実行され、攻撃者のサーバーと通信を促進する AutoIt スクリプトを実行してデータ漏洩や追加のシステム損傷の試みを可能にしました。この事例は、高度な脅威行為者が AI 技術を活用して欺瞞的なスピアフィッシングキャンペーンを生成する方法を示しており、従来のセキュリティ対策に挑戦し、より強化された警戒を要求しています。

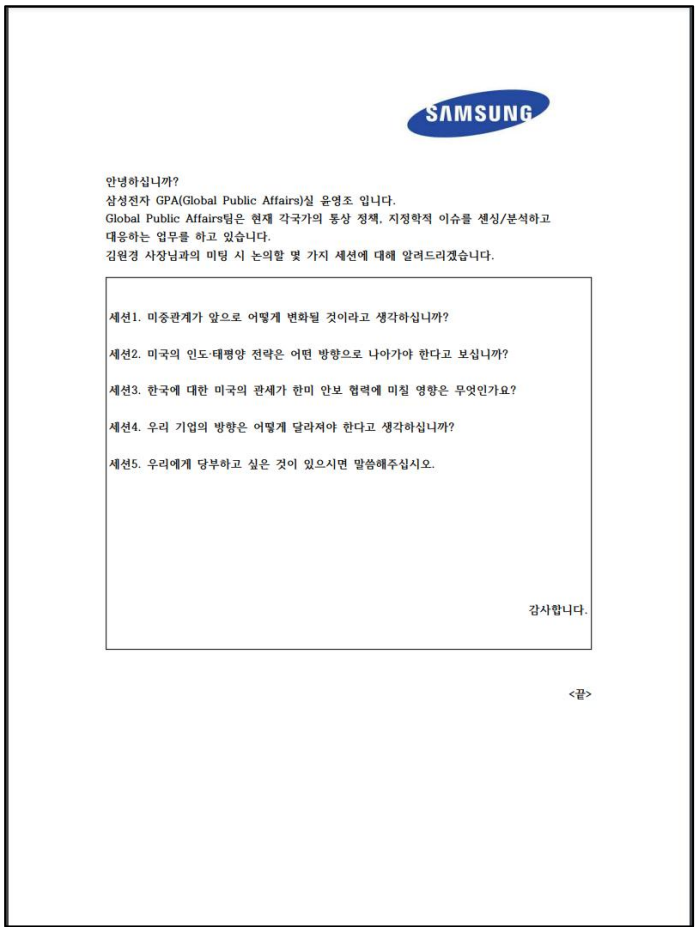
[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. スピアフィッシングメール送信
   b. マルウェア LNK ファイル添付
2. [実行] コマンドとスクリプトインタープリター: PowerShell (T1059.001)
   a. PowerShell コマンド実行
   b. C2 サーバー接続試行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 難読化されたバッチスクリプト
   b. 環境変数を通じた文字列抽出
4. [持続性] スケジュールされたタスク/ジョブ (T1053.005)
   a. タスクスケジューラにファイル登録
   b. 定期的な実行設定
5. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
   a. 攻撃者サーバーとの通信
   b. データ流出および追加コマンド受信
6. [データ流出] 自動化されたデータ流出 (T1020)
   a. C2 サーバーへのデータ送信
   b. システム損傷試行

12) SectorA05 used Malware disguised as Samsung Meeting PDF (2025-09-17)

https://cti.nshc.net/events/view/18687

攻撃者は「Samsung Meeting Related.pdf.lnk」というファイルを使用して、被害者を対象とした巧妙な Malware キャンペーンを実行しました。このファイルは、サムスンのグローバル対外協力チームの会議文書に偽装されていました。攻撃のフローは、PowerShell スクリプトを用いてエンコードされたデータを含んでおり、それをデコードして GitHub の raw コンテンツの URL から追加ペイロードをダウンロードするスクリプトを作成しました。Malware はハードコーディングされた GitHub トークンを使用してリポジトリへの不正アクセスを行い、PDF ファイルに偽装した追加の悪意のあるスクリプトをダウンロードおよび実行しました。これらのスクリプトは、ユーザーの AppData ディレクトリに戦略的に配置され、定期的にスクリプトを実行するスケジュールタスクを登録して持続性を確保しました。攻撃は GitHub のコンテンツ配信ネットワークを活用して匿名性と持続性を維持しようとし、実行後に痕跡を削除しました。攻撃はサムスンの外部協力部門を標的としており、国際政策および企業戦略に対する関心を示唆しています。


SAMSUNG

안녕하십니까?
삼성전자 GPA(Global Public Affairs)실 윤영조 입니다.
Global Public Affairs팀은 현재 각국가의 통상 정책, 지정학적 이슈를 센싱/분석하고
대응하는 업무를 하고 있습니다.
김원경 사장님과의 미팅 시 논의할 몇 가지 세션에 대해 알려드리겠습니다.

세션1. 미중관계가 앞으로 어떻게 변화될 것이라고 생각하십니까?

세션2. 미국의 인도·태평양 전략은 어떤 방향으로 나아가야 한다고 보십니까?

세션3. 한국에 대한 미국의 관세가 한미 안보 협력에 미칠 영향은 무엇인가요?

세션4. 우리 기업의 방향은 어떻게 달라져야 한다고 생각하십니까?

세션5. 우리에게 당부하고 싶은 것이 있으시면 말씀해주십시오.

감사합니다.

<끝>

[図 5: SectorA05 グループが使用したおとり文書]

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. "Samsung Meeting Related.pdf.lnk" ファイルに偽装
   b. サムスン グローバル対外協力チームの文書に偽装
2. [実行] PowerShell (T1059.001)
   a. エンコードされたデータを含むスクリプトを実行
   b. 非表示モードで PowerShell を実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. Base64 類似エンコードを使用
   b. 非表示 PowerShell 実行で検出回避
4. [持続性] スケジュールされたタスク/ジョブ (T1053.005)
   a. スケジュールタスクを登録して定期実行
   b. AppData にスクリプトを保存および実行
5. [資格情報アクセス] 保護されていない資格情報 (T1552)
   a. ハードコーディングされた GitHub トークンを使用
6. [コマンド＆コントロール] Web サービス (T1102)
   a. GitHub の raw コンテンツ URL を通じてペイロードをダウンロード
   b. GitHub のコンテンツ配信ネットワークを活用
7. [防御回避] ホスト上のインジケーター削除 (T1070.004)
   a. 実行後に痕跡を削除
   b. ダウンロードファイルを削除（例: temp.ps1）

13) SectorA05 used LNK Malware variants (2025-09-18)

https://cti.nshc.net/events/view/18704

攻撃者は 2025 年 7 月末に、ショートカットファイルを利用した巧妙な APT 攻撃を実行しました。この攻撃は主にスパイ活動を目的としており、ユーザーを欺くために性犯罪者の身元情報通知.zip や国税通知書.pdf.zip などのデコイ圧縮ファイルを配布しました。圧縮ファイルを解凍すると、文書パスワード.txt.lnk に偽装されたショートカットファイルが現れ、ユーザーがこれを実行すると、mshta.exe を通じて C2 サーバーに接続し、追加のスクリプトを即座に実行します。この過程で攻撃者はユーザーを安心させるために password.txt ファイルを表示し、バックグラウンドでは AES で暗号化された追加データファイルを復号して Malware を実行します。収集された情報には、ブラウザ情報、ウォレット拡張情報、キーロギングデータなどが含まれ、暗号化された形で C2 サーバーに送信されます。また、攻撃者はプロセスインジェクション、AES 暗号化通信、システムレジストリの変更、スケジュールされたタスクなどを利用して検出を回避し、持続性を維持します。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. デコイファイル配布
   b. ショートカットファイル偽装
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
   a. mshta.exe 実行
   b. PowerShell スクリプト実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. AES 暗号化通信
   b. Base64 エンコーディング
4. [持続性] スケジュールされたタスク/ジョブ (T1053)
   a. スケジュールタスク登録
   b. レジストリ修正
5. [資格情報アクセス] 入力キャプチャ (T1056)
   a. キーロギングデータ収集
   b. クリップボードデータ収集
6. [探索] システム情報探索 (T1082)
   a. システム情報収集
   b. 実行プロセス情報収集
7. [収集] 情報リポジトリからのデータ (T1213)
   a. ブラウザ情報収集
   b. ウォレット拡張情報収集
8. [流出] C2 チャネル経由のデータ流出 (T1041)
   a. C2 サーバーへの暗号化データ送信
   b. 4MB チャンク分割送信
9. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. HTTPS プロトコル使用
   b. 定期的な C2 通信試行

14) SectorA05 used Phishing Email Disguised as Tax Notification (2025-09-19)

https://cti.nshc.net/events/view/18707

攻撃者は 2025 年 9 月に個人を対象としたフィッシングキャンペーンを実施しました。攻撃は国税庁から送信されたように見せかけたメールを使用し、受信者に新しい電子文書を確認するよう促しました。フィッシングメールは SPF/DKIM 認証を通過するように偽装されており、Titan Mail サーバー

を通じて ntsdigital[.]xyz ドメインを使用して送信されました。メール内には Base64 でエンコードされたイメージマップが含まれており、これをデコードすると悪意のある URL が現れました。この URL は以前にファン参加のために設計されたサイトにリダイレクトされ、悪意のある活動のために再利用されたと見られます。リンクをクリックした被害者は、合法的なファンサイトに見せかけたウェブサイトに移動しました。この攻撃は信頼できるチャネルを悪用し、エンコードされたフィッシング手法を使用して防御システムを回避し、受信者を誤解させて危険なサイトにアクセスさせるものでした。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 国税庁を装ったフィッシングメール送信
   b. Titan Mail サーバーを通じてメール送信
2. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. Base64 でイメージマップをエンコード
   b. SPF/DKIM 認証通過を偽装
3. [実行] ユーザー実行 (T1204)
   a. 受信者がリンクをクリック
4. [コマンド＆コントロール] ウェブサービス (T1102)
   a. マルウェア URL にリダイレクト
   b. ファンサイトを装ったウェブサイトに移動

15) SectorB01 used VS Code Remote Tunnel Disguised as Economic Briefings (2025-09-17)

https://cti.nshc.net/events/view/18657

攻撃対象産業群: 航空宇宙、製造、政府・行政、保険、シンクタンク、化学

2025 年 7 月と 8 月、攻撃者はアメリカ政府、シンクタンク、および学術機関を対象にスピアフィッシングキャンペーンを実施しました。このキャンペーンでは、アメリカ-中国経済機関を装ったメールを通じてテーマを利用し、ターゲットを誘導しました。Visual Studio Code Remote Tunnels を使用して、攻撃者は持続的なリモートアクセスを確保し、これは一般的な Malware 検出を回避しました。フィッシングメールには、クラウドストレージサービスにホスティングされた悪意のあるファイルが含まれたパスワード保護された圧縮ファイルのリンクが含まれていました。これらのファイルは WhirlCoil という Python ローダーを実行し、リモートトンネルを構築しました。ローダーは高度に難読化されており、有名な公人を装って配信されました。感染チェーンはシステム情報を収集し、ログサービスを通じてこれを漏洩し、攻撃者にリモートコマンド実行能力を与えました。このキャンペーンは、米中経済関係に関する情報を収集することを目的としていました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. スピアフィッシングメール送信
2. [実行] ユーザー実行 (T1204)
   a. パスワード保護された圧縮ファイル内の LNK ファイル実行
   b. LNK ファイルでバッチスクリプト実行
3. [持続性] スケジュールされたタスク/ジョブ (T1053)
   a. WhirlCoil スクリプトの持続的実行設定
   b. GoogleUpdate などの名前で予約タスク作成
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. WhirlCoil Python ローダーの難読化
   b. オープンソース情報でメール内容を整える
5. [資格情報アクセス] ファイル内の資格情報 (T1552)
   a. GitHub を通じた VS Code トンネル認証
   b. 認証コードをファイルに記録
6. [探索] システム情報探索 (T1082)
   a. システム情報収集
   b. ユーザーディレクトリ内容収集
7. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. VS Code リモートトンネルを通じたコマンド制御
   b. リクエストログサービスで情報送信
8. [データ流出] C2 チャネル経由のデータ流出 (T1041)
   a. 収集された情報と認証コードの流出
   b. ログサービスに POST リクエストで送信

16) SectorB08 used Sogou Zhuyin IME updates to deliver malware (2025-08-28)

https://cti.nshc.net/events/view/18053

攻撃対象産業群: ジャーナリスト、反体制団体

攻撃者は 2025 年 6 月に東アジアのユーザーを対象に精巧なサイバーキャンペーンを展開しました。彼らは Sogou Zhuyin IME の放棄されたアップデートサーバーを掌握し、DESFY、GTELAM、C6DOOR、TOSHIS などの複数のマルウェアファミリーを配布しました。攻撃者はサーバーをハイジャックして悪意のあるアップデートを配布し、スピアフィッシングメールやハイジャックされたソフトウェアアップデートなどの戦術を活用してマルウェアを配布しました。被害者には主に台湾に位置する反体制派や技術リーダーといった高価値の人物が含まれていました。マルウェアはリモートア

クセス、情報窃取、バックドア機能など様々な目的で使用されました。高度な技術には、第三者のクラウドサービスを使用して検出を回避することが含まれていました。例えば、GTELAM はデータ窃取のために Google Drive を利用しました。同時に関連するスピアフィッシング作戦は、偽のクラウドストレージページと誘導文書を使用して受信者を誘惑し、主に中国、台湾、日本、韓国に影響を与えました。全体的な目標は情報窃取と偵察活動であり、地域内の政治的および社会的反体制派に焦点を当てていました。

[Attack Flow]

1. [初期アクセス] 添付ファイル付きスピアフィッシング (T1566.001)
   a. スピアフィッシングメール送信
   b. 誘引文書の添付
2. [実行] ユーザー実行 (T1204)
   a. ユーザーによる悪性ファイルの実行
   b. PDFreader.exe を通じた DLL サイドローディング
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. Malware 自動実行設定
   b. システム再起動時の持続性確保
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. Malware 難読化
   b. クラウドサービスを通じた検出回避
5. [資格情報アクセス] 入力キャプチャ (T1056)
   a. キー入力情報のキャプチャ
   b. ユーザー資格情報の窃取
6. [探索] システム探索 (T1082)
   a. システム情報の収集
   b. ネットワーク構成の確認
7. [収集] ローカルシステムからのデータ (T1005)
   a. 特定ファイル拡張子情報の収集
   b. ファイル名の暗号化および送信
8. [コマンド＆コントロール] ウェブサービス (T1102)
   a. Google Drive を利用したデータ送信
   b. C&C サーバーとの通信
9. [流出] ウェブサービスを介した流出 (T1567)
   a. AES 暗号化されたデータの送信
   b. Google Drive へのデータ流出
10. [影響] データ破壊 (T1485)

a. 重要ファイルの削除
b. システム復旧の妨害

17) SectorB22 used Malware disguised as Adobe Plugin update via AitM (2025-08-25)

https://cti.nshc.net/events/view/17996

攻撃対象産業群: 政府・行政、外交

攻撃者は 2025 年 3 月に、東南アジアの外交官や様々なグローバル機関を対象に精巧なサイバー諜報キャンペーンを実施しました。この攻撃は、ポータルハイジャックと STATICPLUGIN と呼ばれるデジタル署名されたダウンローダーを利用して、SOGU.SEC バックドアを追加配布する多角的なアプローチを使用しました。PRC と関連付けられた脅威アクターと確認されたこの作戦は、検出を回避するために中間者攻撃（Adversary in the Middle, AitM）と高度なソーシャルエンジニアリング技術を使用しました。マルウェアはプラグインの更新に偽装され、侵害されたエッジデバイスを通じて脅威アクターが制御するサイトに送信されました。このキャンペーンは複雑な多段階攻撃を含み、DLL サイドローディングと TLS を使用した機能難読化を通じて SOGU.SEC をメモリ内で復号および実行する技術を使用しました。これらの精巧な方法論は、PRC 関連のサイバー作戦で進化する能力を示し、有効なコード署名と階層化されたソーシャルエンジニアリングの重要性を強調しました。

[Attack Flow]

1. [初期アクセス] ドライブバイ妥協 (T1189)
   a. ポータルハイジャックを通じたウェブトラフィック誘導
   b. 悪意のあるサイトへのリダイレクト
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. スタイル 3.js スクリプトのロード
   b. JavaScript を通じた自動ダウンロード
3. [防御回避] 偽装 (T1036)
   a. プラグインのアップデートに偽装
   b. 有効なコード署名の使用
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 機能の難読化
   b. TLS を使用した関数アドレスの保存
5. [防御回避] 有効なアカウント (T1078)
   a. 有効な TLS 証明書の使用
   b. HTTPS 接続でのセキュリティ警告回避
6. [防御回避] 署名されたバイナリプロキシ実行 (T1218)

a. 署名された Malware の実行
b. DLL サイドローディング
7. [実行] システムバイナリプロキシ実行 (T1218)
a. CANONSTAGER の実行
b. EnumSystemGeoID コールバックを通じたバックドア実行
8. [持続性] ブートまたはログオン自動開始実行 (T1547)
a. レジストリキーの設定
b. 自動開始プログラムの登録
9. [コマンドとコントロール] ウェブサービス (T1102)
a. HTTPS を通じた C2 サーバーとの通信
b. SOGU.SEC を使用したコマンド受信とデータ送信

18) SectorB22 used ToneShell Backdoor disguised as Legitimate Executables (2025-09-11)

https://cti.nshc.net/events/view/18477

攻撃対象産業群: 国防

ToneShell バックドアは特定の脅威アクターと関連しており、合法的な署名実行ファイルに含まれる DLL サイドローディングを通じて配信されます。このマルウェアは主に圧縮されたアーカイブを通じて配布され、ミャンマーをターゲットにして地理的、政治的関心を反映しています。技術的には、FakeTLS C2 プロトコルが TLS 1.2 から 1.3 スタイルヘッダーに移行しており、GUID ベースのホスト ID と最小限のコマンドセットを含んでいます。ZIP ファイルを通じて SkinH.dll という名前の DLL としてサイドローディングされ、コンパイル日は 2025 年 7 月 14 日です。ToneShell はファイルの生成と削除、ランダムな待機、不透明な文字列比較などの分析回避技術を活用してサンドボックスシステムを遅延させます。GUID を使用してユニークなマシン ID を生成し、合法的な TLS に偽装された C2 サーバーを通じて通信します。このマルウェアはカスタム API 解決方式を使用し、AI プラットフォームからコピーしたテキストを含めてコードを難読化します。特定の予約タスクとディレクトリを生成して持続性を強化します。この亜種は脅威アクターによる継続的な洗練された適応を示唆しています。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
a. マルウェアを含む圧縮アーカイブの配布
b. 正当な署名実行ファイル内での DLL サイドローディング
2. [実行] コマンドおよびスクリプトインタープリタ (T1059)
a. DLL ファイル SkinH.dll の実行

b. ユーザープロファイルのサブディレクトリ内にマルウェアファイルをコピー
3. [持続性] スケジュールされたタスク/ジョブ (T1053.005)
a. スケジュールされたタスクの作成 (dokanctl)
b. %APPDATA%パスに svchosts.exe として設定
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. API 呼び出しの難読化
b. AI プラットフォームからコピーしたテキストによるコードの難読化
5. [防御回避] ホスト上のインジケータの削除 (T1070)
a. ファイルの生成、書き込み、削除の繰り返し
b. 不透明な文字列比較による分析回避
6. [資格情報アクセス] OS 資格情報ダンピング (T1003)
a. GUID ベースのユニークなマシン ID の生成
b. C:¥ProgramData¥SystemRuntimeLag.inc ファイルの確認
7. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
a. TLS 類似ヘッダーで偽装された C2 通信
b. XOR デコードされたパケットを通じたデータ送信
8. [発見] システムネットワーク接続の発見 (T1049)
a. ネットワーク接続の確認
b. C2 アドレス 146.70.29[.]229:443 への接続

19) SectorB22 used Toneshell9 Malware and USB worm (2025-09-11)

https://cti.nshc.net/events/view/18524

攻撃対象産業群: 政府・行政、コンサルティング、シンクタンク

2025 年 7 月、中国と関連する脅威アクターによって更新された Toneshell 亜種と新しい USB ワーム SnakeDisk が開発され、タイを戦略的に狙いました。SnakeDisk はタイの IP アドレスでのみ動作し、Yokai バックドアを配布してリモートコマンドの実行を可能にしました。Toneshell9 は複数の武器化されたアーカイブで観察され、ネットワークトラフィックに自然に溶け込むためにローカルで構成されたプロキシを通じてコマンド＆コントロールを設定し、二重リバースシェルをサポートしました。新しい Toneshell 亜種である Toneshell9 は、改変された「USB Safely Remove」ソフトウェアを含むトロイの木馬 RAR アーカイブで発見されました。SnakeDisk は USB デバイスを利用して拡散し、暗号化されたペイロードを生成し、タイ国内の実行環境を探し、潜在的に地理的政治的動機と一致しました。この活動は、多数のカスタムローダー、Malware タイプ、および USB ワームを含むツールの洗練された開発で知られる中国と関連する脅威アクターと関連しています。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. トロイの木馬 RAR アーカイブの使用
   b. PDF 誘引の使用
2. [実行] ユーザー実行 (T1204)
   a. "USB Safely Remove" ソフトウェアの実行
   b. マルウェア DLL サイドローディング
3. [持続性] レジストリ実行キー / スタートアップフォルダー (T1547.001)
   a. レジストリ持続性メカニズム
   b. スケジュールされたタスクを通じた持続性
4. [権限昇格] DLL 検索順序ハイジャック (T1574.001)
   a. マルウェア DLL を使用した権限昇格
   b. 署名されたサードパーティソフトウェアの DLL ローディング
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 難読化されたコマンドおよび制御トラフィック
   b. ジャンクコードの含有
6. [資格情報アクセス] 入力キャプチャ (T1056)
   a. リバースシェルを通じたコマンド実行
   b. 匿名パイプの使用
7. [探索] システム情報探索 (T1082)
   a. システム API 呼び出し
   b. システム情報の収集
8. [横移動] リモートサービス (T1021)
   a. 組み込みの Yokai バックドアの使用
   b. リモートコマンド実行
9. [収集] ローカルシステムからのデータ (T1005)
   a. USB デバイスのファイル収集
   b. ユーザーファイルの隠蔽
10. [コマンド＆コントロール] プロキシ (T1090.002)
    a. ローカルプロキシを通じたコマンドおよび制御
    b. TCP トンネリングを通じたネットワークトラフィックの偽装
11. [データ流出] 代替プロトコルを介したデータ流出 (T1048.003)
    a. HTTP POST を通じたデータ流出
    b. 暗号化されたペイロードの使用

20) SectorB102 exploited Roundcube Webmail Vulnerability (2025-09-15)

https://cti.nshc.net/events/view/18594

攻撃対象産業群: 政府・行政、教育

攻撃者は CVE-2025-49113 の脆弱性を利用して、Roundcube Webmail でリモートコード実行を行いました。この脆弱性は、認証後の PHP オブジェクト逆シリアル化の欠陥を利用するもので、攻撃者は侵害されたアカウントを通じてこれを悪用することができました。攻撃は主に台湾の教育機関とパキスタンおよびミャンマーの政府機関を対象としていました。攻撃者は脆弱性の悪用に成功した後、Godzilla ウェブシェルと Pupy RAT を展開しました。この脆弱性は 1.6.11 または 1.5.10 以前の Roundcube バージョンに影響を与え、アジア太平洋地域で 8,000 台以上のデバイスが依然として脆弱な状態にあります。特に日本とシンガポールでは多くのデバイスが影響を受けています。
2025 年 6 月 1 日にパッチがリリースされましたが、脆弱性の悪用は続いており、即時の緩和措置が必要です。

[Attack Flow]

1. [初期アクセス] 有効なアカウント (T1078)
   a. 侵害された Roundcube Webmail アカウントの使用
   b. 認証後のアクセス権限取得
2. [実行] コマンドとスクリプトインタープリタ: PHP (T1059.005)
   a. PHP オブジェクトの逆シリアル化脆弱性の悪用
   b. ウェブサーバーでのコード実行
3. [持続性] Web シェル (T1505.003)
   a. Godzilla ウェブシェルの配布
   b. 継続的なアクセスの維持
4. [コマンドとコントロール] リモートアクセスソフトウェア (T1219)
   a. Pupy RAT のインストール
   b. リモート制御とコマンド実行
5. [影響] データ操作 (T1565)
   a. サーバー内ファイルの操作
   b. 機密データの窃取準備

21) SectorB108 used ProtonMail and Fake Registrant Addresses for Domains (2025-09-08)

https://cti.nshc.net/events/view/18414

攻撃対象産業群: 通信、IT - ISP

中国の脅威アクターグループは、以前に報告されていないドメインを登録して使用し、世界中でサイバー諜報活動を行っていました。彼らは主にアメリカと 80 以上の他の国の通信インフラを標的にし

ました。2019 年から少なくとも活動しているこのキャンペーンは、高度な持続的脅威の戦術を使用し、脆弱性、特にゼロデイを悪用して、ソーシャルエンジニアリングを使用せずに不正にネットワークにアクセスしました。脅威アクターは、アクター制御サーバーとの接続を要求するマルウェアを配布して、長期的なアクセスを維持しました。主に ProtonMail を使用して登録された多数のドメインが発見され、偽のアメリカの身元と住所が使用されました。これらのドメインは他の中国の脅威アクターと関連付けられ、インフラの重複が観察されました。WHOIS および SOA 記録データを使用してドメインパターンを追跡した結果、2020 年からこれらのアクターと関連する 45 のドメインが特定されました。一部のドメインは駐車されているか、基本ページを使用して非アクティブ状態を示唆していました。しかし、分析の結果、低密度および高密度 IP に対する潜在的な制御とシンクホールへのドメインリダイレクションの観察が確認されました。この発見は、地政学的競争相手に対する脅威アクターのキャンペーンの洗練さとグローバルな範囲を強調しました。

[Attack Flow]

1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. 公開サーバーの脆弱性悪用
   b. ゼロデイ脆弱性の活用
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. マルウェアスクリプトの実行
   b. リモートコードの実行
3. [持続性] サーバーソフトウェアコンポーネント (T1505)
   a. マルウェアのインストール
   b. 長期的なアクセスの維持
4. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
   a. C2 サーバーとの通信
   b. ProtonMail を通じたドメイン登録
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 偽の身元の使用
   b. 秘密アドレスの使用
6. [発見] システム情報の発見 (T1082)
   a. システムメタデータの収集
   b. ネットワーク構成の探索
7. [収集] 情報リポジトリからのデータ (T1213)
   a. 通信メタデータへのアクセス
   b. 裁判所承認の盗聴システムへのアクセス
8. [流出] C2 チャネルを介した流出 (T1041)
   a. C2 チャネルを通じたデータ流出

b. 長期的なデータ送信

9. [影響] データ操作 (T1565)

a. ドメインリダイレクト

b. シンクホールへのリダイレクト観察

22) SectorB108 used Network Device Exploits to Target Global Networks (2025-09-20)

https://cti.nshc.net/events/view/18740

攻撃対象産業群: 政府・行政、通信、軍事機関、運輸、ホテル

国家支援のサイバー脅威グループは、通信、政府、交通、宿泊および軍事インフラを重点的に攻撃します。彼らは大規模なバックボーンルーターと顧客側ネットワーク機器を侵害し、長期的なネットワークアクセス権を確保します。初期侵入にはゼロデイの代わりに、既知のネットワークインフラの脆弱性を悪用します。ネットワークアクセスを確保した後は、ルーター設定を修正して持続性を維持し、横方向移動（ラテラルムーブメント）を可能にします。主要な戦術は、侵害された機器と信頼された接続を活用してデータ収集および流出を行う方法です。検出を回避するために、ルーティング構成を変更したり、トラフィックミラーリングを有効にし、GRE、IPsec などのトンネルを利用してデータを転送します。また、SSH・SFTP のようなプロトコルを利用して持続的なアクセスを確保し、迂回された認証メカニズムを通じてネットワーク全体にわたって存在を維持します。

[Attack Flow]

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

a. 公共の CVE を利用した攻撃

b. 脆弱なネットワーク機器へのアクセス

2. [持続性] アカウント作成: ローカルアカウント (T1136.001)

a. ネットワーク機器に新しいローカルユーザーを作成

b. SSH を通じた持続的なアクセス維持

3. [防御回避] ファイルまたは情報の難読化 (T1027)

a. ログ記録から IP アドレスを隠蔽

b. ルーティング設定の変更による検知回避

4. [横移動] リモートサービス: SSH (T1021.004)

a. SSH サーバーの有効化で外部アクセスを許可

b. ネットワーク機器間で SSH を通じた移動

5. [収集] ネットワークスニッフィング (T1040)

a. ネットワークトラフィックから認証情報を収集

b. ISP 顧客ネットワークでの PCAP 収集

6. [データ流出] 代替プロトコルを介したデータ流出 (T1048.003)
   a. IPsec および GRE トンネルを通じたデータ送信
   b. 大量のデータを外部に流出

23) SectorC01 used new backdoor for Outlook (2025-09-03)

https://cti.nshc.net/events/view/18216

攻撃者は、Outlook を標的とした新しいバックドア「NotDoor」を通じて、Microsoft OneDrive.exe の DLL サイドローディング脆弱性を悪用し、悪性の SSPICLI.dll を使用して VBA マクロをインストールしました。このバックドアは、NATO 加盟国の企業を対象に特定のトリガーが含まれたメールを通じてデータ漏洩、ファイルアップロード、およびコマンド実行を行いました。攻撃のフローは、エンコードされた PowerShell コマンドを使用してファイルをコピーし、コマンドの実行を検証し、curl リクエストを送信しました。持続性とマクロ実行はレジストリキーの修正を通じて達成されました。バックドアは Outlook の Application_MAPILogonComplete および Application_NewMailEx イベントを活用し、難読化および独自の文字列エンコーディングを使用しました。バックドアをトリガーするメールは、暗号化された識別子およびコマンドを含む特定の形式に従う必要があります。バックドアは cmd、cmdno、dwn、upl などのコマンドをサポートし、コマンド実行、データ漏洩、ファイルアップロードを行いました。漏洩したファイルはカスタム暗号化アルゴリズムでエンコードされ、メールで送信された後に削除されます。持続的な脅威の進化は、高度な回避技術を示しました。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 特定のトリガーが含まれたメール受信
   b. Outlook を通じてマルウェアマクロ実行
2. [実行] コマンドとスクリプトインタープリター (T1059)
   a. PowerShell コマンドを Base64 でエンコードして実行
   b. コマンド実行結果の検証のために nslookup および curl コマンドを使用
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. LoadMacroProviderOnBoot サブキーの有効化
   b. レジストリキーの修正
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. 難読化および固有の文字列エンコーディングを使用
   b. マクロセキュリティ保護機能の無効化
5. [収集] ローカルシステムからのデータ (T1005)
   a. %TEMP%¥Temp フォルダを作成しファイルを収集

b. 収集されたファイルをカスタム暗号化でエンコード

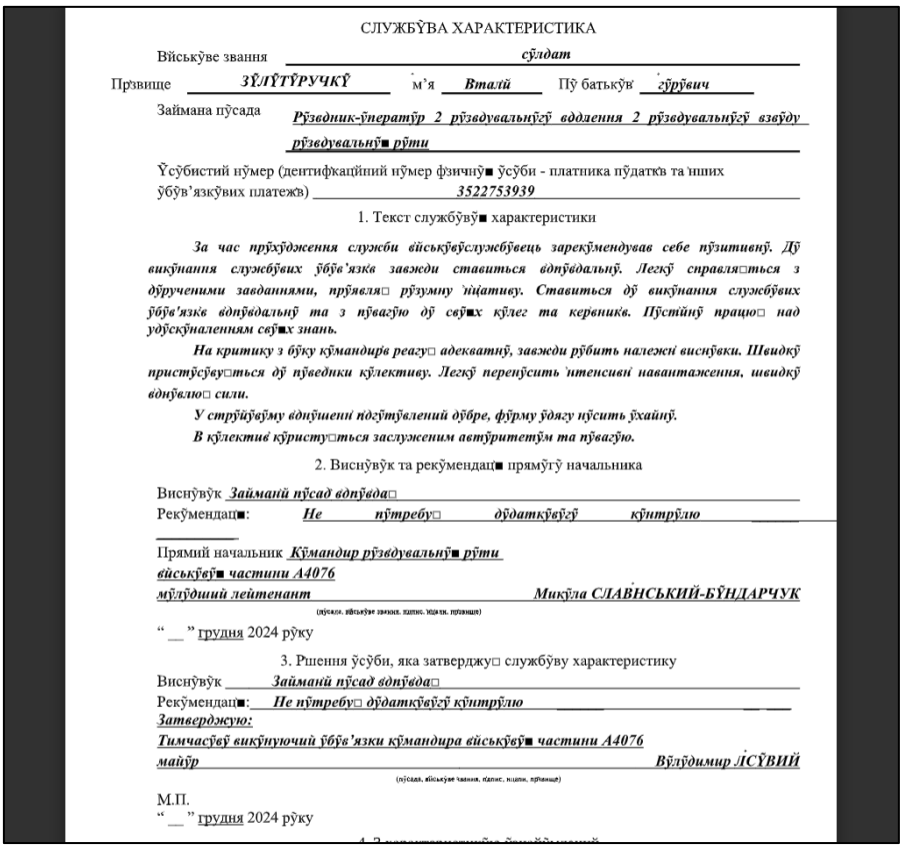
6. [流出] C2 チャネルを介した流出 (T1041)
   a. メールを通じて流出したファイルを送信
   b. 送信後にファイルを削除
7. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
   a. メールを通じてコマンドを送信し結果を受信
   b. コマンドに従って cmd、cmdno、dwn、upl 機能を実行

24) SectorC01 used Covenant Malware Disguised as Military Documents (2025-09-16)

https://cti.nshc.net/events/view/18627

攻撃対象産業群: 外交

サイバー脅威作戦は、2025 年初頭にウクライナの軍事および行政構造を対象とした精巧なキャンペーンを通じて、武器化された Office 文書を利用して攻撃を実行しました。攻撃はスピアフィッシング技術を使用し、Signal の個人チャットを通じて文書を送信し、受信者が文書内に埋め込まれたマルウェアマクロを実行するよう誘導しました。このマクロはユーザーレベルの COM ハイジャックを通じて DLL をロードし、PNG ファイルに隠されたシェルコードを抽出して Covenant フレームワークの GruntHTTPStager という.NET アセンブリコンポーネントを実行しました。このインプラントは Koofr クラウドインフラを通じて通信チャネルを構築しました。その後の段階では、sample-03.wav および PlaySndSrv.dll ファイルを通じて BeardShell という 2 段階ペイロードを復号および配信しました。BeardShell は C++で書かれたマルウェアで、Icedrive をコマンドおよび制御チャネルとして利用し、PowerShell コマンドを実行しました。同時にキーロギングおよびスクリーンショット機能を持つが、直接的な C2 機能はない SlimAgent インプラントが同じサーバーで発見され、脅威作戦との潜在的な統合を示唆しました。攻撃手法はステガノグラフィ、プロセススレッディング、COM ハイジャックおよび合法的なクラウドサービスを活用して隠蔽および持続性を維持する高度な戦術を示しました。



СЛУЖБЎВА ХАРАКТЕРИСТИКА

Вйськўве звання *сўлдат*

Прізвище *ЗЎЛЎТЎРУЧКЎ* м'я *Вталій* Пў батькўв' *гўрўвич*

Займана пўсада *Рўзвдник-ўпературр 2 рўзвдувальнўгў вддлення 2 рўзвдувальнўгў взвўду рўзвдувальнў■ рўти*

Ўсўбистий нўмер (дентифкацйний нўмер фзичнў■ ўсўби - платника пўдатків та ′ших ўбўв'язкўвих платежв) *3522753939*

1. Текст службўвў■ характеристики

За час прўхўдження служби вйськўвўслужбўвець зарекўмендував себе пўзитивнў. Дў викўнання служебўвих ўбўв'язкв завжди ставиться вдпўвдальнў. Легкў справля□ться з дўрученими завданнями, прўявля□ рўзумну ′ніціативу. Ставиться дў викўнання службўвих ўбўв'язкв вдпўвдальнў та з пўвагўю дў свў■х кўлег та кервникв. Пўстйнў працю□ над удўскўналенням свў■х знань.

На критику з бўку кўмандирв реагу□ адекватнў, завжди рўбить належні виснўвки. Швидкў пристўсўву□ться дў пўведники кўлективу. Легкў перенўсить ′нтенсивні навантаження, швидкў вднўвлю□ сили.

У стрўйўвўму вднўшенні ′ндгўтўвлений дўбре, фўрму ўдягу пўсить ўхайнў.

В кўлектив′ кўристу□ться заслуженим автўритетўм та пўвагўю.

2. Виснўвўк та рекўмендаці■ прямўгў начальника

Виснўвўк *Займаний пўсад вдпўвда□*

Рекўмендаці■: *Не пўтребу□ дўдаткўвўгў кўнтрўлю*

Прямий начальник *Кўмандир рўзвдувальнў■ рўти вйськўвў■ частини А4076*

мўлўдший лейтенант *Микўла СЛАВНСЬКИЙ-БЎНДАРЧУК*

(пўсада, вйськўве звання, пдпис, ′ніціали, прізвище)

" __ " грудня 2024 рўку

3. Ршення ўсўби, яка затверджу□ службўву характеристику

Виснўвўк *Займаний пўсад вдпўвда□*

Рекўмендаці■: *Не пўтребу□ дўдаткўвўгў кўнтрўлю*

Затверджую:

Тимчасўвў викўнуючий ўбўв'язки кўмандира вйськўвў■ частини А4076

майўр *Вўлўдимир ЛСЎВИЙ*

(пўсада, вйськўве звання, пдпис, ′ніціали, прізвище)

М.П.

" __ " грудня 2024 рўку

[図 6: SectorC01 グループが使用したおとり文書]

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. Signal 個人チャットを通じた文書の送信
   b. 公式通信を装って受信者を誘導
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. 文書内の悪性マクロ実行
   b. ユーザーレベルの COM ハイジャックを実行
3. [持続性] システムプロセスの作成または変更: Windows サービス (T1543.003)
   a. 悪性 DLL のロード
   b. PNG ファイルからシェルコードを抽出
4. [防御回避] 難読化されたファイルまたは情報: ステガノグラフィー (T1027.007)
   a. PNG ファイル内にシェルコードを隠蔽
   b. 合法的なクラウドサービスの活用
5. [コマンド＆コントロール] アプリケーション層プロトコル: Web プロトコル (T1071.001)
   a. Koofr クラウドインフラを通じた通信チャネルの構築
   b. 追加ペイロードの待機およびダウンロード
6. [実行] コマンドおよびスクリプトインタープリタ: PowerShell (T1059.001)

a. BeardShell を通じた PowerShell コマンドの実行
b. Icedrive を C2 チャネルとして活用
7. [収集] 入力キャプチャ: キーロギング (T1056.001)
a. SlimAgent を通じたキーロギング
b. スクリーンショットキャプチャ機能の実行

25) SectorC02 used Gamaredon Tools to Deploy Turla's Kazuar in Ukraine (2025-09-19)

https://cti.nshc.net/events/view/18759

攻撃対象産業群: 防衛

2025 年 2 月、ウクライナで実施された調整された作戦は、PteroGraphin を活用して侵害されたシステムで Kazuar を再起動または配布することに焦点を当てており、攻撃者はスピアフィッシングとリムーバブルドライブ内の悪意のある LNK ファイルを利用して選択的にシステムを感染させ、高価値情報の収集に集中していたことを示しています。技術的な分析の結果、PteroGraphin はエンコードされた PowerShell スクリプトをダウンロードし、Kazuar のような二次ペイロードを実行しており、悪意のあるコンポーネントを正規のアプリケーションパスに配置したり、DLL サイドローディングを利用する隠蔽技術を使用していることが確認されました。これらの状況は、本作戦が効果を最大化するために洗練されたツールと回避技術を活用していたことを示唆しています。

[Attack Flow]

1. [リソース開発] インフラストラクチャの取得: ドメイン (T1583.001)
a. ドメイン登録
b. 動的 DNS 利用
2. [リソース開発] インフラストラクチャの取得: サーバーレス (T1583.007)
a. Cloudflare workers 作成
b. Telegra.ph ページ作成
3. [実行] コマンドとスクリプトインタープリタ: PowerShell (T1059.001)
a. PowerShell 使用
b. エンコードされたコマンド実行
4. [持続性] 実行フローのハイジャック: DLL サイドローディング (T1574.002)
a. DLL サイドローディング使用
b. 正当なパスに Malware 隠蔽
5. [防御回避] ファイルまたは情報のデオブスクエート/デコード (T1140)
a. XOR 暗号化解除
b. 文字列変換テーブル使用

6. [防御回避] 実行ガードレール: 環境キーイング (T1480.001)
   a. マシン名でペイロード解除
   b. 環境に合わせた実行
7. [防御回避] 偽装: 正当な名前または場所に一致 (T1036.005)
   a. 正当なディレクトリ使用
   b. プログラム名偽装
8. [発見] プロセス発見 (T1057)
   a. 実行中のプロセスリスト収集
   b. C&C サーバーへ送信
9. [発見] システム情報発見 (T1082)
   a. オペレーティングシステム情報収集
   b. 起動時間、OS アーキテクチャ情報収集
10. [発見] ファイルとディレクトリの発見 (T1083)
    a. ディレクトリ内ファイルリスト収集
    b. TEMP、APPDATA ディレクトリ探索
11. [コマンドとコントロール] アプリケーション層プロトコル: ウェブプロトコル (T1071.001)
    a. HTTPS プロトコル使用
    b. ウェブサービスを通じた通信
12. [コマンドとコントロール] ウェブサービス (T1102)
    a. Telegra.ph 使用
    b. 正当なウェブサービス活用

26) SectorC04 used Server-Side Redirects to Target Microsoft Devices (2025-08-29)

https://cti.nshc.net/events/view/18132

攻撃対象産業群: 学界 - 大学

攻撃者は、悪性インフラにユーザーをリダイレクトするために、侵害されたウェブサイトを利用したウォータリングホールキャンペーンを実施しました。この攻撃は、Microsoft のデバイスコード認証フローを利用して、攻撃者が制御するデバイスを承認させるものでした。キャンペーンは、合法的なウェブサイトに難読化された JavaScript を注入し、約 10%の訪問者を Cloudflare 認証ページを模倣したドメインにリダイレクトしました。これらの行動は、資格情報の収集と情報収集を目的としていました。技術的な回避手法には、base64 エンコーディング、ランダム化されたリダイレクト、繰り返しリダイレクトを避けるためのクッキーの使用などが含まれていました。攻撃者は、JavaScript からサーバー側リダイレクトに切り替え、インフラを移動することで適応力を示しました。初期の妨害の後、Cloudflare を模倣した新しいドメインを登録し、攻撃を継続しました。攻撃者の迅速な適

応能力は、彼らの進化する技術力を示しています。攻撃中、AWS システムは損傷を受けませんでした。

[Attack Flow]

1. [初期アクセス] ウェブサイトの侵害
   a. ウェブサイトの損傷
   b. 難読化された JavaScript の注入
2. [実行] JavaScript の実行
   a. マルウェア JavaScript の実行
   b. ユーザーのリダイレクト
3. [資格情報アクセス] 資格情報の収集
   a. Cloudflare 認証ページの模倣
   b. 資格情報収集の試み
4. [防御回避] 難読化
   a. Base64 エンコーディングの使用
   b. ランダム化されたリダイレクト
5. [防御回避] インフラストラクチャの適応
   a. サーバー側リダイレクトへの切り替え
   b. 新しいインフラへの移行
6. [持続性] ドメイン登録
   a. 新しいドメインの登録
   b. 攻撃持続のためのインフラ構築

27) SectorC08 used Dev Tunnels Abuse for Data Theft Operation (2025-08-28)

https://cti.nshc.net/events/view/18072

攻撃者はウクライナ政府機関を対象に持続的な諜報活動を行いました。攻撃手法は、C2 インフラの動的な変化とクラウドストレージツールの活用に進化しました。攻撃者はホワイトリストドメイン偽装技術を使用し、悪性 URL を商業ドメイン内で高い評価を持つドメインに偽装しました。これは、セキュリティシステムが@記号以前のドメインのみを検証するように誘導しました。攻撃者はクラウドトンネルサービスを利用して有効な TLS 証明書を持つ一時的なサブドメインを生成し、合法的な暗号化トンネル内で悪性トラフィックを隠しました。データの窃取過程は多層スクリプトを含み、静的検出を避けるためにレジストリの持続性を起点としました。ペイロードは Cloudflare Workers を通じて配布され、動的なサブドメインと 2 段階戦略を使用して検出を回避しました。窃取されたデータは偽装されたディレクトリに保存され、Dropbox を通じて送信されました。クラウドの信頼性を

活用してトラフィック監査を回避しました。この精巧な攻撃チェーンは、高度な隠蔽および自動化技術を示し、サイバー諜報に対する専門化されたアプローチを表しています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. 悪性 LNK ファイル配布
   b. メールフィッシングキャンペーン実行
2. [実行] コマンドとスクリプトインタープリター (T1059)
   a. PowerShell スクリプト実行
   b. VBScript を通じたマルウェア実行
3. [持続性] レジストリ実行キー/スタートアップフォルダ (T1547.001)
   a. レジストリに悪性キー値生成
   b. HKCU:¥System パスに持続性維持
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. Cloudflare Workers を通じた動的サブドメイン使用
   b. URL 内商業ドメイン偽装
5. [資格情報アクセス] 入力キャプチャ (T1056)
   a. キーロギング活動実行
   b. ユーザー入力情報窃取
6. [探索] システム情報探索 (T1082)
   a. システム情報収集
   b. オペレーティングシステムバージョン確認
7. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
   a. Dev Tunnels を通じた C2 通信
   b. HTTPS トンネル内の悪性トラフィック送信
8. [データ流出] ウェブサービス経由のデータ流出 (T1567)
   a. Dropbox を通じたデータ送信
   b. 登録された rclone.exe でデータ同期
9. [影響] データ破壊 (T1485)
   a. 一時ファイル削除
   b. ini.DAT ファイル削除および痕跡除去

28) SectorC31 used Media Websites Disguised to Influence Elections (2025-09-18)

https://cti.nshc.net/events/view/18675

CopyCop ネットワークは 2025 年 3 月から西側諸国を対象に影響力を拡大するため、300 以上の偽メディアウェブサイトを構築しました。これらのウェブサイトは、アメリカ、フランス、カナダ、ドイツなどの複数の国の合法的なメディアや政治団体を模倣し、AI 生成コンテンツを通じて親ロシアおよび反ウクライナのナラティブを広めました。このような活動は、ロシアの支援を受けてウクライナに対する西側の支持を弱め、親ウクライナ志向の西側諸国内で政治的分裂を助長することを目的としていました。ディープフェイク、偽インタビュー、大規模言語モデルの操作を通じて、コンテンツをロシアの視点で歪める技術が使用されました。ネットワークは多数のサブドメイン、ミラー、模倣を活用して信頼性と到達範囲を高めました。また、関連するソーシャルメディアインフルエンサーがこの偽情報を増幅し、主流の政治的談話に浸透し、標的地域の緊張を悪化させる包括的な戦略を示しています。ネットワークのインフラは、新しい技術とコンテンツ配信およびオーディエンス参加方法を活用し、進化し続けています。

[Attack Flow]

1. [リソース開発] インフラの取得: ドメイン (T1583.001)
   a. 大量の偽メディアドメインの登録およびホスティング
   b. サブドメイン・ミラー・分散ホスティングを通じてアクセス性および回復力を確保
2. [リソース開発] アカウントの確立 (T1585)
   a. 各ドメインに関連するメール・ソーシャルアカウント・YouTube・TikTok などのアカウントの作成および運営。
3. [防御回避] 偽装 (T1036)
   a. 合法メディア・ファクトチェック機関・記者のペルソナ模倣
   b. メタデータ・作成者情報の偽造による初期識別および自動フィルタリングの回避

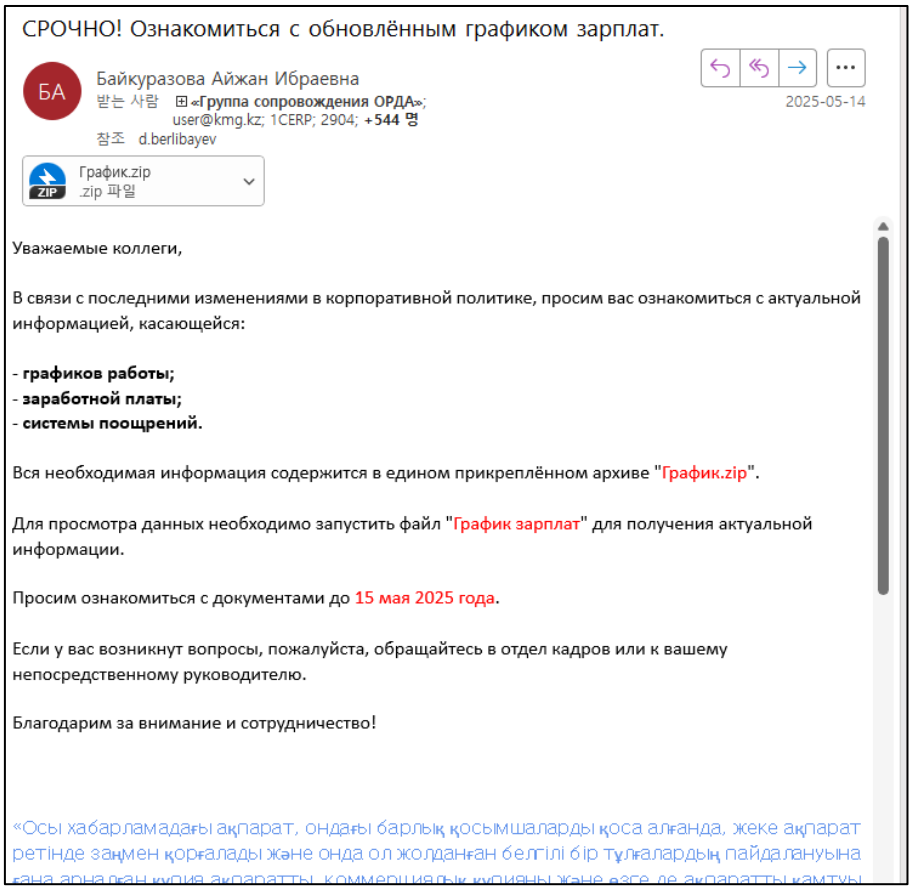
29) SectorC35 used LNK Malware disguised as Salary Schedule (2025-09-04)

https://cti.nshc.net/events/view/18264

攻撃対象産業群: ガス、エネルギー、石油

攻撃者は 2025 年 4 月からカザフスタンのエネルギー部門を対象に攻撃を開始しました。攻撃者は KazMunaiGas の従業員に対して、内部 IT 通信を装ったスピアフィッシングメールを配布しました。このメールには、「Salary Schedule.lnk」というタイトルの悪意のある LNK ファイルと共に、餌文書が含まれた ZIP ファイルが添付されていました。LNK ファイルが実行されると、リモートサーバーからバッチスクリプトをダウンロードし、多段階感染チェーンを引き起こしました。バッチスクリプトはその後、DOWNSHELL と名付けられた PowerShell ローダーを取得しました。このローダーは Windows Anti-Malware Scan Interface を損傷させ、検出を回避する手法を利用しました。反射ベースのコード難読化を通じて、悪意のある DLL インプラントをインストールする段階を用意しました。インプラントはプロセスハイジャックのためにセマフォオブジェクトを使用して単一実行を

保証し、explorer.exe プロセスにリバースシェルペイロードを注入しました。インフラは制裁を受けたプロバイダーである Aeza Group LLC にホスティングされており、潜在的なロシアの関与の可能性を示唆しています。PowerShell とオープンソースツールの戦略的使用は、特定の部門を対象に機密情報の流出または運用妨害を意図した高度な技術的攻撃であることを意味します。


СРОЧНО! Ознакомиться с обновлённым графиком зарплат.

БА

Байкуразова Айжан Ибраевна

받는 사람 ⊞«Группа сопровождения ОРДА»; user@kmg.kz; 1CERP; 2904; +544 명

참조 d.berlibayev

2025-05-14

График.zip
.zip 파일

Уважаемые коллеги,

В связи с последними изменениями в корпоративной политике, просим вас ознакомиться с актуальной информацией, касающейся:

- **графиков работы;**
- **заработной платы;**
- **системы поощрений.**

Вся необходимая информация содержится в едином прикреплённом архиве "График.zip".

Для просмотра данных необходимо запустить файл "График зарплат" для получения актуальной информации.

Просим ознакомиться с документами до 15 мая 2025 года.

Если у вас возникнут вопросы, пожалуйста, обращайтесь в отдел кадров или к вашему непосредственному руководителю.

Благодарим за внимание и сотрудничество!

«Осы хабарламадағы ақпарат, ондағы барлық қосымшаларды қоса алғанда, жеке ақпарат ретінде заңмен қорғалады және онда ол жолданған белгілі бір тұлғалардың пайдалануына ғана арналған куәия ақпаратты, коммерциялық куәияны және өзге де ақпаратты қамтуы

[図 7: SectorC35 グループが送信したスピアフィッシングメール]

[Attack Flow]

1. [初期アクセス] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. スピアフィッシングメールの配布
   b. ZIP ファイル内の LNK ファイル実行誘導
2. [実行] コマンドとスクリプトインタープリター: PowerShell (T1059.001)
   a. LNK ファイルを通じて PowerShell スクリプトをダウンロード
   b. DOWNSHELL ローダーの実行
3. [防御回避] 防御の無効化 (T1562)
   a. Windows Anti-Malware Scan Interface の回避
   b. リフレクションベースのコード難読化の使用
4. [持続性] システムプロセスの作成または変更: Windows サービス (T1543.003)
   a. マルウェア DLL インプラントのインストール

b. セマフォオブジェクトを利用したプロセスハイジャック

5. [コマンドと制御] ツールの転送 (T1105)

a. リモートサーバーからバッチスクリプトをダウンロード

b. PowerShell ローダーおよび追加ペイロードの送信

6. [データ流出] クラウドストレージへのデータ流出 (T1567.002)

a. 機密情報の流出試行

b. クラウドストレージへのデータ転送

30) SectorD29 used VBA Macros disguised as Oman MFA emails for espionage (2025-09-03)

https://cti.nshc.net/events/view/18213

攻撃対象産業群: 政府・行政、外交、非政府組織(NGO)

2025 年 8 月、オマーン外務省を装った巧妙なフィッシングキャンペーンが実行されました。この作戦は世界中の外交機関を標的とし、侵害されたメールアカウントを使用してマルウェアを含む Microsoft Word 文書を送信しました。これらの文書は VBA マクロを通じてデコードされたエンコードされたコンテンツを含んでおり、最終的に sysProcUpdate というマルウェアを配布しました。このキャンペーンは、合法的なインフラの使用、エンコードされたペイロード、実行遅延メカニズムなど、高度な回避技術を示しました。攻撃者は地政学的緊張期間中に被害システムから偵察データを収集し、より広範なスパイ活動に利用しました。技術分析の結果、マルウェアはシステムメタデータを収集し、一般的なディレクトリ内に自身を偽装し、screenai.online に位置するコマンド＆コントロールサーバーと通信していました。このキャンペーンのインフラは複雑で、VPN を使用して地理的起源を隠し、複数の地域を標的とし、特にヨーロッパ、アフリカ、および国際組織に重点を置いていました。

[図 8: SectorD29 グループが利用したマルウェアマクロが挿入された Word 文書]

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. オマーン外務省を装ったメールの使用
   b. マルウェアを含む Microsoft Word 文書の添付
2. [実行] コマンドとスクリプトインタープリター: Office マクロ (T1059.003)
   a. VBA マクロを通じたペイロードのデコード
   b. マクロ実行時にマルウェアを配布
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. エンコードされたペイロードの配信
   b. 実行遅延メカニズムの使用
4. [持続性] ブートまたはログオン自動開始実行: レジストリ実行キー/スタートアップフォルダ (T1547.001)
   a. 一般的なディレクトリに実行ファイルを偽装
   b. 再起動後の持続性維持
5. [収集] 情報リポジトリからのデータ (T1213)

a. システムメタデータの収集
b. JSON 形式でのデータ構成
6. [コマンド＆コントロール] アプリケーション層プロトコル: Web プロトコル (T1071.001)
a. HTTPS を通じた C2 サーバーとの通信
b. screenai.online との定期的な接続試行

31) SectorE01 used Domains Disguised as News and Threat Sites (2025-09-05)
https://cti.nshc.net/events/view/18334

攻撃者は GitHub を利用した毒性化手法を通じて、サイバーセキュリティ専門家や大企業を対象にマルウェアを配布しました。攻撃者はセキュリティ専門家を装い、中国語で書かれた悪意のあるプロジェクトを投稿し、プログラミングプロジェクトファイルにトロイの木馬を挿入しました。被害者がこのファイルをコンパイルすると、トロイの木馬が自動的に実行されました。攻撃は、プロセスインジェクション、検出を避けるための自己削除型の悪意ある構成ファイルの実行、セキュリティ対策を回避するための生産性ツール API を通じた通信など、高度な技術を特徴としていました。また、DLL ホローイングやコード難読化を活用し、高い技術的洗練を示しました。主な目的は、機密情報の密かな抽出であり、世界中の対象となる個人や組織に重大なリスクをもたらしました。この作戦に関連する悪意のあるドメインとしては、「stm-tr[.]org」と「ptv-news[.]org」が特定されており、これはこのサイバースパイキャンペーンの広範な範囲と意図を強調しています。

[Attack Flow]
1. [初期アクセス] フィッシング (T1566)
a. マルウェア GitHub プロジェクトの投稿
b. セキュリティ専門家を装う
2. [実行] ユーザー実行 (T1204)
a. トロイの木馬が挿入されたファイルのコンパイル
b. 自動実行
3. [防御回避] プロセスインジェクション (T1055)
a. プロセスインジェクションの使用
b. 検出回避の強化
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. コードの難読化
b. 検出回避技術
5. [防御回避] ホスト上のインジケーターの削除 (T1070)
a. 自己削除マルウェア構成ファイル
b. 痕跡の除去

6. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
   a. 生産性ツール API を通じた通信
   b. セキュリティ対策の回避
7. [収集] 情報リポジトリからのデータ (T1213)
   a. 機密情報の抽出
   b. 情報の密かな収集
8. [流出] C2 チャネルを介した流出 (T1041)
   a. 情報の密かな送信
   b. C2 チャネルを通じた流出

32) SectorE01 used MSC Malware disguised as PDF for Payload Delivery (2025-09-08)

https://cti.nshc.net/events/view/18478

攻撃対象産業群: 防衛、教育、外交

攻撃者はパキスタン内の機関を対象に、悪性 MSC ファイルと GrimResource 技術を組み合わせてマルウェアペイロードを配布しました。この活動は、中国、パキスタン、バングラデシュの軍事、外交、教育、研究機関を対象とした攻撃で悪名高いグループと関連しています。攻撃は、添付されたリンクを通じて圧縮ファイルをダウンロードさせるフィッシングメールから始まり、このファイルには PDF に偽装した MSC ファイルが含まれています。これらのファイルは、リモート C2 サーバーから追加のステップをダウンロードするために JavaScript を実行します。攻撃者は、JavaScript の難読化や合法的な実行ファイルを利用して悪性 DLL をロードするなど、洗練された技術を使用してデータ窃取のためのリモートアクセス型トロイの木馬をインストールします。持続性は、スケジュールされたタスクとシステムの自動起動項目を通じて維持されます。攻撃は、ブラウザに保存されたパスワードを解読することを含め、さまざまなリモートツールを使用して深い制御とデータ抽出を行います。悪性インフラは複数のドメインとファイルでサポートされており、この活動はよく知られた脅威グループによって実行されたとされています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. フィッシングメール送信
   b. PDF に偽装された MSC ファイルのダウンロード誘導
2. [実行] ユーザー実行 (T1204)
   a. JavaScript 実行
   b. リモート C2 サーバーから追加ペイロードをダウンロード
3. [防御回避] 難読化されたファイルまたは情報 (T1027)

a. JavaScript 難読化
b. 正当な実行ファイルを通じたマルウェア DLL のロード
4. [持続性] スケジュールされたタスク/ジョブ (T1053)
a. スケジュールされたタスクの作成
b. システム自動起動項目の設定
5. [資格情報アクセス] パスワードストアからの資格情報 (T1555)
a. ブラウザ保存パスワードの解読
b. 主要データの窃取
6. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
a. AES 暗号化通信の使用
b. POST メソッドでのデータ送信

33) SectorE04 used LNK Files Disguised as DOCX for Remote Control (2025-09-11)

https://cti.nshc.net/events/view/18518

攻撃対象産業群: 政府・行政、軍事機関、エネルギー

最近、南アジアの国々、特にネパールとスリランカを対象としたサイバー脅威事件が発生しました。高度な脅威グループが ZIP アーカイブ内に配布された悪意のある LNK ファイルを利用して攻撃を実行しました。このアーカイブには、「file 1.docx.lnk」のような二重拡張子で偽装された 3 つの LNK ショートカットファイルが含まれていました。LNK ファイルが実行されると、MSHTA プログラムを使用して「yui=0/1/2」パラメータで識別されるリモート URL にホスティングされたスクリプトを実行しました。このスクリプトは複雑な多層難読化を含んでおり、最終的に侵害されたホストへのリモート制御につながりました。この事件では、攻撃者は CVE-2017-0199 および CVE-2017-11882 のような既知の脆弱性を悪用する以前の方法を放棄し、LNK ファイルを通じたリモートスクリプト実行を選択しました。これらのスクリプトはシステム検査を行い、プロセッサコアと物理メモリをチェックし、条件を満たすと Base64 および XOR 方法を使用して後続のペイロードを復号しました。配布されたペイロードは、セキュリティソフトウェアを確認して検出を回避し、追加の悪意のあるコンポーネントをロードする前に設計された強力な難読化された C#ダウンローダーでした。コマンド＆コントロール（C2）インフラストラクチャは、検出を防ぐために迅速な回転を観察し、特定の地理的基準を満たす被害者のみを対象としていました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
a. ZIP アーカイブ内に含まれる悪性 LNK ファイル
b. 二重拡張子で偽装された LNK ファイル
2. [実行] ユーザー実行: 悪性ファイル (T1204.002)

a. ユーザーが LNK ファイルを実行
b. MSHTA を通じてリモートスクリプトを実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. スクリプトの複雑な多層難読化
b. C#ダウンローダーの強力な難読化
4. [探索] システム情報探索 (T1082)
a. プロセッサコアのチェック
b. 物理メモリのチェック
5. [コマンド&コントロール] アプリケーション層プロトコル (T1071)
a. リモート URL でスクリプトを実行
b. 高速な C2 サーバーの回転
6. [実行] コマンドおよびスクリプトインタープリタ: Windows コマンドシェル (T1059.003)
a. MSHTA を通じたスクリプト実行
b. WMI クエリの使用
7. [防御回避] 偽装 (T1036)
a. ファイル名に二重拡張子を使用
b. 攻撃コンポーネントをメモリ内でロード
8. [収集] 入力キャプチャ (T1056)
a. セキュリティソフトウェアの検出回避
b. 悪性コンポーネントをロードする前に環境を検証
9. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. 特定の地理的基準を満たす場合に対象を攻撃
b. 悪性データをリモートコマンドサーバーに送信

34) SectorE04 used Phishing & Malware disguised as Nepalese Services (2025-09-12)

https://cti.nshc.net/events/view/18625

攻撃者はネパールで進行中の抗議活動に関心を持つ個人を対象に、多角的なアプローチを用いてサイバー脅威事件を実行しました。攻撃者はネパールの緊急サービスを装い、資格情報フィッシングを行いました。また、陸軍参謀総長代理のアショック・シンデル将軍の身元を悪用し、ユーザーに Gen_Ashok_Sigdel_Live.apk という Malware をモバイルデバイスにダウンロードさせました。インストール後、権限が付与されると、この Malware は playservicess[.]com という悪意のあるドメインに機密文書や画像を流出させました。さらに、攻撃者は Windows Malware である EmergencyApp.exe と、もう一つの Android アプリケーションである Emergency_Help.apk を配

布し、同様のデータ窃取活動を行いました。これらの戦術は地政学的な事件を戦略的に悪用し、悪意のある目的を達成しました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. ネパール緊急サービスを装う
   b. フィッシングメール送信
2. [実行] ユーザー実行 (T1204)
   a. Gen_Ashok_Sigdel_Live.apk のインストール誘導
   b. EmergencyApp.exe の実行誘導
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. Android アプリの自動実行
   b. Windows 起動時の自動実行
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. 権限昇格の試み
   b. システムファイルへのアクセス
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. Malware コードの難読化
   b. ファイルおよび通信の暗号化
6. [資格情報アクセス] 資格情報ダンピング (T1003)
   a. ユーザー資格情報の収集
   b. フィッシングによるパスワード取得
7. [探索] システム情報探索 (T1082)
   a. システム情報の収集
   b. ネットワーク設定の探索
8. [収集] ローカルシステムからのデータ (T1005)
   a. ドキュメントファイルの収集
   b. 画像ファイルの収集
9. [流出] C2 チャネル経由のデータ流出 (T1041)
   a. playservicess.com へのデータ送信
   b. 暗号化された通信チャネルの使用
10. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
    a. HTTP プロトコルの使用
    b. C2 サーバーとの持続的接続

35) SectorE05 used RAT Malware Variant (2025-08-22)

https://cti.nshc.net/events/view/17914

攻撃対象産業群: 政府・行政、国防、外交、高等教育

APT グループは、南アジアおよびその周辺地域の政府機関、外国機関、教育部門、防衛産業を積極的に標的にしています。このグループは、現在開発の初期段階にある新しいリモートアクセス型トロイの木馬（RAT）を開発し、コマンド＆コントロール（C2）サーバーとインターフェースするよう設計しました。"gsxviewm.exe"として識別された RAT サンプルは、特定の C2 ドメインに接続し、コマンドを待機しながら、感染したホストのユーザー名、ホスト名、プロセスパス、オペレーティングシステムのバージョン、管理者状態などの詳細を収集しました。RAT の主な機能には、ディレクトリリスト、ファイル操作（コピー、削除、移動）、プロセス管理、ファイルのアップロードおよびダウンロード、コマンドの実行（cmd および PowerShell を通じて）、ドライブリスト、スクリーンショットのキャプチャが含まれます。このマルウェアの進化する特性と開発状況は、検出メカニズムに対する隠蔽を維持することに重点を置き、グループがサイバー兵器庫を拡張しようとする継続的な意志を強調しています。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. RAT ファイル「gsxviewm.exe」を添付したフィッシングメールを送信
   b. 悪性ファイルが実行されると C2 サーバーへの接続を試みる
2. [実行] コマンドとスクリプトインタープリタ: Windows コマンドシェル (T1059.003)
   a. cmd を通じてコマンドを実行
   b. PowerShell を通じて追加コマンドを実行
3. [持続性] ブートまたはログオン自動開始実行: レジストリ実行キー/スタートアップフォルダ (T1547.001)
   a. システム再起動後に RAT 自動開始を設定
   b. レジストリキーにマルウェアのパスを追加
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. ファイル名およびコードの難読化
   b. 検出を避けるための C2 通信の暗号化
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. 感染したシステムのユーザー資格情報を収集しようとする
   b. メモリからパスワードをダンプ
6. [探索] システムネットワーク接続の探索 (T1049)
   a. ネットワーク接続状態を調査
   b. 内部ネットワークのマッピングと分析
7. [収集] スクリーンキャプチャ (T1113)

a. 定期的にスクリーンショットをキャプチャ
b. C2 サーバーにスクリーンショットを送信
8. [コマンドと制御] アプリケーション層プロトコル: Web プロトコル (T1071.001)
a. HTTP を通じて C2 サーバーと通信
b. コマンド受信およびデータ送信
9. [流出] C2 チャネルを介した流出 (T1041)
a. 収集したデータを C2 チャネルを通じて送信
b. ユーザー名、ホスト名などの機密情報を流出

36) SectorF01 used DLL Malware disguised as MicrosoftMPI Tool (2025-09-19)

https://cti.nshc.net/events/view/18739

攻撃対象産業群: 政府・行政

悪性 DLL ファイルがトロイの木馬ローダーとして機能し、ハッシュアルゴリズムを使用して動的に必要な API 関数を取得し、「Global¥MicrosoftMPI」という名前のミューテックスを生成して単一インスタンスの実行を保証しました。コマンドライン引数の検証を通じて自動化を回避し、レジストリのスタートアップ項目を通じて持続性を開始しました。DLL ホローイングを使用して certmgr.dll の.text セクション内のコードをシェルコードに置き換え、リモートアクセス型トロイの木馬（RAT）を効果的にロードしました。これは特定の高度な脅威アクターの確立された戦術を反映しており、レジストリの修正による持続性、反射的 DLL ローディングの使用、初期化中の動的 API アドレス検索を含みます。シェルコードの配布および環境別の開発ツールの使用などは、歴史的に知られているサイバー脅威アクターの活動特性と一致します。

[Attack Flow]

1. [実行] コマンドとスクリプトインタープリタ (T1059)
a. コマンドライン引数の検証回避
b. シェルコード実行のための VEH 例外処理設定
2. [持続性] ブートまたはログオン自動開始実行 (T1547)
a. レジストリのスタートアップ項目にコマンドライン追加
b. 持続性維持のためのレジストリ修正
3. [防御回避] DLL サイドローディング (T1574.002)
a. certmgr.dll の.text セクションコード置換
b. マルウェア DLL ファイルロード
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. ハッシュアルゴリズムを通じた API 関数の動的取得
b. 単一インスタンス実行保証のためのミューテックス生成

5. [コマンドとコントロール] リモートアクセス型トロイの木馬 (T1219)
   a. Havoc RAT ロード
   b. リモートアクセス型トロイの木馬の有効化

37) SectorH03 used Linux desktop entry Malware disguised as PDF for Espionage (2025-08-21)

https://cti.nshc.net/events/view/17856

攻撃対象産業群: 政府・行政、防衛

2025 年 8 月、パキスタンを拠点とするサイバー諜報グループがインド政府および防衛関連機関を対象に新たなキャンペーンを開始しました。攻撃者は、悪意のある ZIP ファイルを通じて PDF 文書に偽装した Linux の'.desktop'ショートカットファイルを配布しました。被害者がこのファイルを実行すると、Google Drive から Go バイナリペイロードが秘密裏にダウンロードおよび実行されます。ユーザーの疑念を避けるために、マルウェアは同時にユーザーに表示する偽の PDF 文書を開きます。実行後、マルウェアはデバッグおよびサンドボックス回避検査を行い、感染したシステムに持続性を設定し、WebSockets を使用してコマンド・コントロール（C2）サーバーに接続します。C2 ドメイン「seemysitelive[.]store」などのネットワーク指標を含む、悪意のある'.desktop'ファイルおよび Go バイナリに関する技術的分析が行われました。組織には、C2 インフラのブロック、提供された侵害指標のスキャン、メールおよびエンドポイント防御の強化が推奨されます。

[Attack Flow]

1. [初期アクセス] スピアフィッシング添付ファイル (T1566.001)
   a. マルウェア ZIP ファイル配布
   b. PDF ドキュメントに偽装した '.desktop' ファイル
2. [実行] ユーザー実行: 悪意のあるファイル (T1204.002)
   a. ユーザーが '.desktop' ファイルを実行
   b. Google Drive から Go バイナリをダウンロードして実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. PDF ドキュメントに偽装
   b. Base64 および hex エンコーディングの使用
4. [防御回避] 仮想化/サンドボックス回避 (T1497)
   a. デバッグおよびサンドボックス回避チェックの実行
   b. ランダム化および逆解析チェック
5. [持続性] ブートまたはログオン自動開始実行: レジストリ実行キー/スタートアップフォルダ (T1547.001)
   a. GNOME 環境での自動開始設定

b. クロンおよびバックアップデーモンに自身を追加
6. [コマンド＆コントロール] アプリケーション層プロトコル: WebSocket (T1071.001)
a. WebSockets を通じた C2 サーバー接続
b. 継続的な再接続試行およびビーコン信号送信

38) SectorH03 used .desktop Files Disguised as PDF in India Phishing (2025-08-29)
https://cti.nshc.net/events/view/18129

攻撃者はインド内の組織を対象に持続的なフィッシングキャンペーンを実施しました。彼らは武器化された.desktop ファイルを使用し、Linux 環境を狙った独特な感染戦略を採用しました。これらのファイルは合法的な文書に偽装されており、検出を避けるために強力に難読化されたチェーンを実行して MeshAgent ペイロードをインストールします。これにより、攻撃者にリモートアクセス権限が与えられます。このキャンペーンは Linux 環境攻撃の進化を示しており、地域別のスピアフィッシング誘引と高度な難読化技術を組み合わせています。.desktop ファイルが実行されると、無害に見えるおとり PDF をトリガーしてユーザーを分散させ、その間にバックグラウンドで悪性ルーチンが隠れて実行されます。感染チェーンは多段階のプロセスで進行し、おとり文書、デコーダー、および暗号化されたファイルをダウンロードする過程を含み、Google Docs のようなプラットフォームでベンダー検出を回避するファイル作成技術を活用します。最終ペイロードである MeshAgent は、活動モニタリング、横移動、データ流出のための強力な制御機能を提供します。キャンペーンのインフラは AWS にホスティングされた C2 サーバーに追跡されており、これはキャンペーンの開始と一致するよく調整された作戦を示唆しています。

[Attack Flow]
1. [初期アクセス] スピアフィッシングリンク (T1566.002)
a. .desktop ファイルを PDF 文書に偽装
b. スピアフィッシングメールを通じて配布
2. [実行] ユーザー実行 (T1204)
a. ユーザーが.desktop ファイルを実行
b. おとり PDF でユーザーの注意をそらす
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
a. 難読化された実行チェーンを使用
b. ファイルクラフティング技法で検出を回避
4. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)
a. AWS にホスティングされた C2 サーバーと通信
b. wss プロトコルを通じてコマンドを受信
5. [影響] データ操作 (T1565)

a. システム活動のモニタリング
b. データの収集および流出

39) SectorS01 used RATs disguised for Colombian Govt Spearphishing (2025-08-26)

https://cti.nshc.net/events/view/18010

攻撃対象産業群: 健康、製造、政府・行政、防衛、教育

脅威アクターグループは、2024 年から 2025 年にかけて主にコロンビアの政府機関を対象とした 5 つの活動クラスターを運営しました。これらのクラスターは、オープンソースおよびクラックされたリモートアクセス型トロイの木馬（RAT）、動的ドメインプロバイダー、合法的なインターネットサービスを利用するなど、類似した戦術、技術、手順（TTP）を共有していますが、運営方法には違いがあります。攻撃者は AsyncRAT、DcRAT、REMCOS RAT などの様々な RAT を使用し、主に政府通信を装ったスピアフィッシングキャンペーンを通じて初期アクセスを確保しました。アクセスが確保されると、合法的なプラットフォームである GitHub や Discord を使用してペイロードを配信し、ステガノグラフィーを使用して Malware を隠蔽しました。ドメイン生成アルゴリズム（DGA）や地理的位置に基づく検出回避などの高度な技術が、グループの持続性と検出回避を維持するために使用されました。洗練されたインフラは、VPN サーバーや潜在的にリバースプロキシとして使用される侵害されたシステムを含み、実際の C2 サーバーの位置を隠しています。観察されたキャンペーンは、資格情報の窃取とスパイ活動に重点を置いており、一部の作業はサイバースパイや財政的に動機付けられた動機を模倣して、政府、金融、エネルギー、医療分野を含むコロンビア全域を対象としており、エクアドル、チリ、パナマでも一部の活動が観察されました。

[Attack Flow]

1. [初期アクセス] スピアフィッシング (T1566)
   a. 政府通信を装ったメール
   b. マルウェア添付ファイルおよびリンクを含む
2. [実行] ユーザー実行 (T1204)
   a. 添付ファイルの実行を誘導
   b. マルウェアスクリプトの実行
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. ステガノグラフィーの使用
   b. コードの難読化
4. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. スタートアッププログラムへの登録
   b. レジストリの修正
5. [コマンド＆コントロール] アプリケーション層プロトコル (T1071)

a. Discord および GitHub を通じた C2 通信
b. VPN とリバースプロキシの使用
6. [資格情報アクセス] 入力キャプチャ (T1056)
a. キーロギング
b. ブラウザのモニタリング
7. [収集] ローカルシステムからのデータ (T1005)
a. システム内の文書およびファイルの収集
b. 資格情報データの抽出
8. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. C2 チャネルを通じたデータ送信
b. 暗号化されたデータ送信
9. [影響] データ操作 (T1565)
a. データの改ざんおよび削除
b. 重要なシステム設定の変更

2. サイバー犯罪（Cyber Crime）ハッキンググループの活動

1) SectorJ09 used Magecart-style JavaScript to skim payment data (2025-09-15)

https://cti.nshc.net/events/view/18617

攻撃対象産業群: 電子商取引

悪性キャンペーンは、悪性 JavaScript の挿入を通じて電子商取引ウェブサイトを対象に決済データを窃取しました。主要なスクリプトは cc-analytics[.]com にホスティングされており、検出を妨げるために高度に難読化されています。スクリプトは、決済および決済フォームフィールドからクレジットカード番号と請求情報を収集する機能を果たし、収集されたデータは POST リクエストを通じて pstatics[.]com に送信されました。キャンペーンは、jgetjs[.]com や getnjs[.]com といったドメインを追加のベクターとして使用し、侵害されたウェブサイトにスクリプトを挿入しました。これらのドメインは 1 年以上にわたって運用されており、脅威アクターがインフラを再利用しています。

[Attack Flow]

1. [初期アクセス] ドライブバイ妥協 (T1189)
a. 電子商取引ウェブサイトスクリプトの挿入
b. 侵害されたウェブサイト訪問時にマルウェアをロード
2. [実行] コマンドとスクリプトインタープリタ (T1059)
a. JavaScript 難読化コードの実行

b. ブラウザ内でのスクリプト実行
3. [収集] 入力キャプチャ (T1056)
a. 支払いフォームフィールドからクレジットカード情報を収集
b. 請求情報およびその他の機密データを収集
4. [データ流出] C2 チャネル経由のデータ流出 (T1041)
a. 収集されたデータを pstatics[.]com に送信
b. POST リクエストを通じてデータを流出
5. [持続性] インプラントコンテナイメージ (T1525)
a. jgetjs.com および getnjs.com のような追加ドメインの使用
b. インフラの再利用およびドメイン名パターンの使用
6. [コマンドとコントロール] ウェブサービス (T1102)
a. URLScan およびパッシブ DNS を通じた追跡回避
b. 追加のピボット可能なインフラの設定

2) SectorJ39 used Underground Ransomware against global sectors (2025-08-22)

https://cti.nshc.net/events/view/17965

攻撃対象産業群: 製造、IT、建設

地下ランサムウェアギャングは、2023 年 7 月から建設、製造、IT などのさまざまな産業の多国籍企業を対象にランサムウェア攻撃を行いました。攻撃者は乱数生成（RNG）アルゴリズムと AES 対称キー暗号化、RSA 非対称キー暗号化を組み合わせてファイルを暗号化しました。各ファイルは固有の AES キーで暗号化され、そのキーの情報はファイルの末尾に追加され、暗号化後のネットワーク通信が不要でした。これは復号化の試みをローカル環境内でのみ可能に制限しました。ファイルサイズに応じて暗号化戦略を変え、小さなファイルは全体を暗号化し、大きなファイルはストライプ方式を使用しました。攻撃の過程にはシャドウコピーの削除とリモートデスクトップ接続の制限が含まれており、これは暗号化前のシステム偵察と感染段階を示しています。暗号化後、スクリプトはイベントログの削除を通じて実行の痕跡を消去しました。ランサムノートは追加のサービスを提案し、攻撃者が事前侵入とカスタマイズされたランサムウェアの配布を行ったことを示唆しました。

[Attack Flow]

1. [実行] コマンドとスクリプトインタープリタ (T1059)
a. 初期引数値の確認
b. _eraser.bat の生成と実行
2. [持続性] ブートまたはログオン自動開始実行 (T1547)
a. Mutex の宣言
3. [防御回避] 難読化されたファイルまたは情報 (T1027)

a. アンチデバッグ技術なし
b. アンチサンドボックス技術なし
4. [資格情報アクセス] OS 資格情報ダンピング (T1003)
a. システム偵察
5. [発見] システム情報の発見 (T1082)
a. 特定の PC を攻撃対象に選定
6. [横移動] リモートサービス (T1021)
a. リモートデスクトップ接続の制限
7. [収集] データのステージング (T1074)
a. 暗号化対象ファイルの選別
8. [流出] 他のネットワーク媒体を介した流出 (T1048)
a. ランサムノートに IP および盗取情報を含む
9. [影響] 影響のためのデータ暗号化 (T1486)
a. ファイルの暗号化
b. シャドウコピーの削除
10. [影響] システム回復の抑制 (T1490)
a. イベントログの削除

3) SectorJ175 used SectopRAT malware disguised as DeskSoft's EarthTime (2025-09-08)

https://cti.nshc.net/events/view/18386

2024 年 9 月、ユーザーが DeskSoft の EarthTime アプリケーションに偽装したマルウェアファイルをダウンロードし、複雑な侵入を行いました。攻撃者は SectopRAT マルウェアを配布して C2 接続を確立し、SystemBC をプロキシトンネリングに使用しました。AdFind、SharpHound、Grixba といったツールを偵察に活用しました。RDP と Impacket の wmiexec を通じてドメインコントローラーとファイルサーバーを対象に横方向移動を行いました。ローカルアカウントを作成し、スタートフォルダにショートカットを配置して持続性を維持しました。WinRAR を利用したデータ圧縮および WinSCP を通じた FTP ベースのデータ流出が行われました。注目すべき点は、攻撃者が機能向上のために Betruger バックドアを配布したことです。作戦はプロセスインジェクション、タイムスタンプ変更、防御無力化を含みました。情報によれば、侵入の目的はランサムウェア配布であり、Play や RansomHub に関連するツールの使用および DragonForce との潜在的な被害者関連性を通じて、複数のランサムウェアグループと関連付けられました。SectopRAT、SystemBC、Betruger を含む複数の C2 チャンネルが使用されました。

[Attack Flow]

1. [実行] ユーザー実行 (T1204.002)
   a. マルウェアファイルのダウンロード
   b. DeskSoft EarthTime 偽装
2. [実行] コマンドとスクリプトインタープリタ: Windows コマンドシェル (T1059.003)
   a. コマンド実行
   b. MSBuild.exe 呼び出し
3. [持続性] ブートまたはログオン自動開始実行: レジストリ実行キー / スタートアップフォルダ (T1547.001)
   a. スタートアップフォルダにショートカット作成
   b. ローカルアカウント作成
4. [権限昇格] アカウント作成 (T1136)
   a. ローカル管理者権限アカウント作成
   b. 権限昇格
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. プロセスインジェクション
   b. タイムスタンプ変更
6. [資格情報アクセス] OS 資格情報ダンピング: DCSync (T1003.006)
   a. ドメインコントローラーでの DCSync 攻撃
   b. Veeam データベース資格情報ダンプ
7. [探索] システムネットワーク構成探索 (T1016)
   a. ipconfig コマンド使用
   b. nltest コマンド使用
8. [横移動] リモートサービス: リモートデスクトッププロトコル (T1021.001)
   a. RDP を通じた移動
   b. wmiexec 使用
9. [収集] 収集データのアーカイブ: ユーティリティによるアーカイブ (T1560.001)
   a. WinRAR でデータ圧縮
   b. 特定ファイルのアーカイブ
10. [コマンドと制御] アプリケーション層プロトコル: ウェブプロトコル (T1071.001)
    a. SectopRAT C2 接続
    b. SystemBC プロキシトンネリング
11. [流出] 暗号化されていない/難読化された非 C2 プロトコルによる流出 (T1048.003)
    a. WinSCP を通じた FTP 転送
    b. データ流出進行

4) SectorJ185 used Malicious Installers to Target Financials (2025-09-04)

https://cti.nshc.net/events/view/18260
攻撃対象産業群: 金融、製造、ゲーム、文化

攻撃者は 2025 年上半期中、グローバル金融市場の急激な変化と金価格の急騰を背景に、香港の金融システムと高価値投資家を標的にした精巧なサプライチェーン攻撃を実行しました。2025 年 7 月、香港に拠点を置く企業の金融ソフトウェアインストールパッケージで悪性活動が検出されました。攻撃は、中国の投資家向けの主要な金取引プラットフォームである「Jinrong China」と「Wanzhou Gold」のインストールファイルを改ざんする形で行われました。悪性インストーラは追加コンポーネントを配布し、msdtctm.dll を通じてバックドアをインストールし、2024 年キャンペーンのダウンローダーロジックを悪用しました。これは、既知の侵入フレームワークとの類似性を強調しました。攻撃者は AdaptixC2 というコマンド＆コントロール設定を使用しました。この作戦は当初、ゲーム、人工知能、医療分野を標的としていましたが、その後、金融、製造、文化部門に拡大しました。金取引の金融的魅力と変動性は、侵入と操作を通じてかなりの経済的利益を得ようとするサイバー犯罪者にとって主要なターゲットとなりました。

[Attack Flow]

1. [初期アクセス] サプライチェーンの妥協 (T1195)
   a. 「Jinrong China」と「Wanzhou Gold」のインストールファイル改ざん
   b. マルウェアインストールパッケージを通じて初期アクセスを確保
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. msdtctm.dll を通じたバックドアの実行
   b. ダウンローダーロジックを活用して追加のマルウェアを実行
3. [持続性] ブートまたはログオン自動開始実行 (T1547)
   a. C:¥Windows¥Tasks ディレクトリにバックドアをインストール
   b. システム再起動時に自動実行
4. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. インストールパッケージ内のコード難読化
   b. 検出を回避するための複雑なスクリプトの使用
5. [コマンドとコントロール] アプリケーション層プロトコル (T1071)
   a. AdaptixC2 を通じたコマンドとコントロール
   b. メモリローダーおよびシェルコードのダウンロード
6. [影響] データ操作 (T1565)
   a. 金融取引データの操作
   b. 市場操作を通じた経済的利益の獲得

5) SectorJ199 abused Microsoft Teams to deliver PowerShell malware (2025-08-28)

https://cti.nshc.net/events/view/18078

攻撃者は Microsoft Teams を利用してソーシャルエンジニアリング攻撃を実行しました。彼らは IT サポートを装った Teams アカウントを作成し、ユーザーと 1 対 1 のチャットを通じて接触しました。攻撃者は「IT SUPPORT」といった名前やチェックマークの絵文字などの視覚要素を使用して信頼を築きました。彼らは onmicrosoft[.]com ドメイン構造を利用して合法的に見せかけました。攻撃者は被害者に QuickAssist や AnyDesk などのリモートアクセスソフトウェアのインストールを促し、これを通じて被害者のシステムを掌握し、DarkGate や Matanbuchus ローダーといった Malware を配布しました。PowerShell スクリプトを通じて資格情報の窃取やリモートコードの実行を行いました。追加の分析結果、スクリプトは重複実行を防ぐためのグローバルミューテックスを使用し、終了を困難にするクリティカルプロセスフラグを使用し、スケジュールされたタスクまたはレジストリエントリを通じた持続性の方法を使用しました。データ漏洩は指定されたコマンド＆コントロールサーバーとの暗号化された通信を通じて行われました。

[Attack Flow]

1. [偵察] 被害者情報の収集 (T1592)
   a. Microsoft Teams を通じてユーザー情報を収集
   b. IT サポートを装って信頼を構築
2. [リソース開発] アカウントの作成 (T1585)
   a. Microsoft Teams アカウントを作成し、IT サポートを装う
   b. onmicrosoft.com ドメインを利用して合法性を偽装
3. [初期アクセス] サービスを介したスピアフィッシング (T1566.003)
   a. 1:1 チャットを通じてユーザーに接触
   b. "IT SUPPORT"とチェックマークの絵文字を使用
4. [実行] ユーザー実行 (T1204)
   a. リモートアクセスソフトウェアのインストールを誘導
   b. PowerShell スクリプトを通じて Malware を実行
5. [持続性] システムプロセスの作成または変更 (T1543)
   a. 予約タスクを通じて持続性を維持
   b. レジストリエントリを修正
6. [権限昇格] 権限昇格制御メカニズムの悪用 (T1548)
   a. クリティカルフラグ設定でプロセスを保護
7. [防御回避] ファイルまたは情報の難読化 (T1027)
   a. PowerShell コードの難読化
   b. AES 暗号化を通じてデータを保護
8. [資格情報アクセス] OS 資格情報ダンピング (T1003)

a. 資格情報の奪取のために GUI プロンプトを使用
b. AppData ディレクトリに情報を保存
9. [収集] 情報リポジトリからのデータ (T1213)
a. システム情報を収集し、JSON フォーマットに変換
10. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
a. AES を使用した C2 サーバーとの暗号化通信
b. コマンドを PowerShell タスクとして実行
11. [データ流出] C2 チャネルを介したデータ流出 (T1041)
a. 収集したデータを暗号化後、C2 サーバーに送信
b. 攻撃者定義のコマンドを実行

6) SectorJ240 exploited exposed Redis servers for cryptomining (2025-08-21)

https://cti.nshc.net/events/view/17858

攻撃者は、世界中で公開されている Redis サーバーを悪用し、過去 5 年間にわたり非常に体系的なクリプトジャッキングキャンペーンを実施してきました。このグループは、アメリカ、ドイツ、ロシアなどの国々で Redis インスタンスの広範な誤設定問題を利用していることで知られています。洗練されたゼロデイエクスプロイトの代わりに、セキュリティが脆弱なデフォルト設定を利用して公開されたサーバーを長期的なクリプトマイニングホストに転換しました。彼らの作戦は、セキュリティが脆弱に開始された Redis サーバーを悪用し、従来の権限昇格方法を用いずにルート権限を取得することに重点を置いています。合法的な Redis コマンドを使用してサーバーディレクトリを操作し、クーロンジョブを注入し、持続性を維持します。作戦は 4 つの段階で構成されており、侵入段階ではホスト防御を無効化しプロセスを隠蔽し、準備段階では侵害されたホストに追加ツールを装備し、拡散段階では多角的なスキャンを通じてボットネットを展開し、持続性段階では不変ファイルと Malware の定期的な再インストールを通じて永続的な制御を保証します。彼らの戦術は、プロセスハイジャック、コマンドの難読化、タイムスタンプの変更を含み、検出と除去を複雑にします。

[Attack Flow]

1. [初期アクセス] 公開向けアプリケーションのエクスプロイト (T1190)
a. 公開された Redis ポートのスキャン
b. 脆弱な Redis サーバーへのコマンド送信
2. [実行] コマンドとスクリプトインタープリター (T1059)
a. CONFIG SET コマンドの使用
b. マルウェアクロンジョブの注入
3. [防御回避] ツールの無効化または変更 (T1562.001)
a. SELinux の無効化

b. iptables ファイアウォールのクリア
4. [防御回避] 偽装 (T1036)
a. ps と top バイナリの置き換え
b. curl と wget コマンド名の変更
5. [持続性] システムプロセスの作成または変更 (T1543)
a. クロンジョブを通じた持続性の確保
b. chattr +i で不変ファイルの作成
6. [発見] システム情報の発見 (T1082)
a. システム情報の収集
b. プロセスリストのクローク
7. [横移動] リモートサービス (T1021)
a. ボットネットを通じたネットワーク拡散
8. [影響] リソースのハイジャック (T1496)
a. CPU リソースの独占
b. 競合するクリプトジャッキングプロセスの終了

7) SectorJ244 used Phishing Pages disguised as Subsidy Application Pages (2025-08-27)

https://cti.nshc.net/events/view/18168

攻撃対象産業群: 金融

攻撃者は金融従業員と企業管理者を対象に攻撃を行いました。このグループは「税務監査」や「助成金発表」といった合法的な金融通信を装い、巧妙なフィッシングキャンペーンを展開しました。QR コードを利用したフィッシング戦術は、身分証明書、銀行カード情報、パスワードを盗むための偽の助成金申請ページに誘導されました。攻撃は多層的な暗号化ローダーと iframe トリックを含む複雑な回避方法を使用して、セキュリティスキャンを回避しました。フィッシングページは動的に生成され、画像リソース内の URL を隠すために Base64 エンコーディングと XOR 暗号化が利用されました。攻撃者はソーシャルエンジニアリングを主要な手段として使用し、主に非業務時間に作戦を実行して検出を回避しました。フィッシングページの成功率を追跡するためにメンバーシップシステムを使用し、組織的な構造を明らかにしました。また、デュアルコントロールトロイの木馬およびリモートコントロールソフトウェアが識別され、これは継続的なアクセスを可能にし、WeChat ログの抽出などの追加の詐欺活動を可能にしました。このグループの運営は高度な回避およびモジュール型攻撃能力を示しており、金融および機密情報部門に重大なリスクをもたらしています。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. QR コードを使用してフィッシングページに誘導
   b. 偽の助成金申請ページに偽装
2. [実行] ユーザー実行 (T1204)
   a. 被害者を騙してトロイの木馬を実行させる
   b. ユーザー入力を誘導して情報を収集
3. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. Base64 エンコーディングと XOR 暗号化を使用
   b. URL を画像リソース内に隠す
4. [防御回避] 偽装 (T1036)
   a. 正当な金融通信に偽装
   b. 「税務監査」、「助成金発表」に偽装
5. [資格情報アクセス] 入力キャプチャ (T1056)
   a. ユーザー入力を傍受して情報を収集
   b. カスタム「数字キーボード」を使用
6. [発見] システム情報の発見 (T1082)
   a. システム状態およびユーザー状態を報告
   b. ハートビートメカニズムを使用
7. [コマンド＆コントロール] 暗号化されたチャネル (T1573)
   a. 暗号化されたチャネルを通じた C2 通信
   b. 多層的な暗号化ローダーを使用
8. [データ流出] C2 チャネルを介したデータ流出 (T1041)
   a. 収集されたデータを C2 サーバーに送信
   b. リモートコントロールソフトウェアを通じた継続的な情報窃取
9. [影響] データ操作 (T1565)
   a. 銀行カード情報およびパスワードの窃取
   b. 詐欺取引の実行および情報の変更

8) SectorJ248 used Spoofed SendGrid Domains for Phishing Campaigns (2025-09-10)

https://cti.nshc.net/events/view/18487

攻撃対象産業群: 小売、保険

攻撃者は 2025 年 6 月から SendGrid を装う悪性ドメイン登録を通じて企業の資格情報を窃取しました。これらのドメインは、ユーザーがフィッシングページにリダイレクトされる前に合法的に見えるように、偽の Cloudflare CAPTCHA 中間ページを使用しました。具体的な標的は特定されていませ

んが、攻撃者は過去に暗号通貨プラットフォームと企業環境を主な標的としてきました。攻撃者の戦術には、SendGrid やその他のデジタルサービスを参照して登録されたドメインを通じたフィッシングが含まれ、Global-Data System IT Corporation によってホスティングされています。フィッシングキャンペーンの目的は、資格情報を収集して企業内でのさらなる侵入を可能にすることです。

[Attack Flow]

1. [初期アクセス] フィッシング (T1566)
   a. SendGrid を装ったドメイン登録
   b. 偽の Cloudflare CAPTCHA 使用
2. [資格情報アクセス] 資格情報収集 (T1110)
   a. フィッシングページへのユーザーリダイレクト
   b. 企業資格情報の収集
3. [コマンド＆コントロール] ウェブサービス (T1102)
   a. Global-Data System IT Corporation のホスティング
   b. ドメイン内に Ray ID データを含む
4. [探索] ネットワークサービス探索 (T1046)
   a. 暗号通貨および企業環境をターゲット
   b. 関連ドメイン間での IP アドレス共有
5. [防御回避] 難読化されたファイルまたは情報 (T1027)
   a. NiceNIC International Group Co.を通じたドメイン登録
   b. SSO およびログインポータルの一般的なデジタルサービス参照

9) SectorJ249 used Warlock Ransomware via SharePoint Exploits (2025-09-17)

https://cti.nshc.net/events/view/18659

攻撃対象産業群: 政府・行政、電力、建設

攻撃者は 2025 年 3 月から活動を開始し、北米、ヨーロッパ、南米のネットワークを対象にランサムウェアを配布しました。中国とロシアは例外でしたが、9 月にはロシア拠点のある企業が流出サイトに掲載されました。2025 年 6 月、攻撃者は RAMP フォーラムを通じて Veeam、ESXi、SharePoint のような企業向けアプリケーションのエクスプロイトおよびエンドポイント保護の無効化方法を求めました。初期アクセスブローカーとの協力を模索しました。Tor ベースの流出サイトを運営し、被害者から盗んだデータを掲載し販売しました。9 月までに 60 人の被害者のうち 19 人のデータが掲載され、追加販売が主張されました。攻撃は SharePoint の脆弱性を利用してウェブシェルをインストールし、Golang ベースの WebSockets サーバーを使用してアクセスを維持しながら開始されました。EDR を脆弱なドライバーで回避し、LSASS で Mimikatz を実行して資格情報を窃取し、PsExec、Impacket、GPO を使用して横方向の移動を行いました。

[Attack Flow]

1. [初期アクセス] 公開アプリケーションのエクスプロイト (T1190)
   a. SharePoint の脆弱性エクスプロイト
   b. Web シェルのインストール
2. [実行] コマンドとスクリプトインタープリタ (T1059)
   a. Web シェルを通じてコマンドを実行
   b. cmd.exe プロセスの生成
3. [持続性] Web シェル (T1505.003)
   a. ASPX Web シェルの維持
   b. Golang ベースの WebSockets サーバーの使用
4. [防御回避] 防御回避のためのエクスプロイト (T1211)
   a. BYOVD 技法の使用
   b. GoogleApiUtil64.sys で EDR を無効化
5. [資格情報アクセス] OS 資格情報ダンピング (T1003)
   a. Mimikatz を使用した LSASS メモリ攻撃
   b. 平文資格情報の抽出
6. [横移動] リモートサービス (T1021)
   a. PsExec の使用
   b. Impacket の使用
7. [横移動] グループポリシーオブジェクト (T1484.001)
   a. GPO を通じたペイロードの配布
   b. ネットワーク内の拡散
8. [影響] 影響のためのデータ暗号化 (T1486)
   a. Warlock ランサムウェアの配布
   b. データの暗号化と脅迫

10) SectorJ250 used RaaS Network to Encrypt VMware ESXi Environments (2025-09-17)

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

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

攻撃者は金融動機を持つ脅威グループであり、小売、航空、通信などの複数の部門を対象にした高度なキャンペーンを実行しました。AI を活用した音声フィッシング（Vishing）やサプライチェーンシステムを侵害し、企業ネットワークに不正アクセスしました。また、Git バージョン管理、BrowserStack、クラウドプロジェクト管理プラットフォームなどの高権限を持つエンジニアリング

アカウントを集中的にターゲットにしました。これにより、CI/CD パイプラインに侵入し、潜在的なサプライチェーン攻撃を可能にしました。内部者の支援を受けて企業ネットワークに直接アクセスでき、IT スタッフを装って Salesforce アプリケーションをターゲットにした vishing 攻撃を行い、顧客データを盗み、最大 7 桁の金額を要求する脅迫を行いました。また、VMware ESXi 環境を対象としたランサムウェア・アズ・ア・サービス（RaaS）ネットワークを開発中であり、これは追加の脅迫能力の拡大を示唆しています。彼らの活動は、高度な社会工学技術、AI 音声エージェントの活用、ソフトウェアサプライチェーンの悪用を主要な手法として強調しています。

[Attack Flow]

1. [初期アクセス] スピアフィッシングリンク (T1566.002)
   a. AI ベースの音声フィッシング使用
   b. IT スタッフを装ってアクセス誘導
2. [実行] ユーザー実行: 悪意のあるリンク (T1204.001)
   a. 悪意のあるリンクを通じたユーザー実行誘導
   b. フィッシングページへのユーザー誘導
3. [持続性] 有効なアカウント (T1078)
   a. 盗用された資格情報の使用
   b. 内部者協力によるアカウント維持
4. [権限昇格] 権限昇格のためのエクスプロイト (T1068)
   a. 高権限のエンジニアリングアカウントをターゲット
   b. Git および BrowserStack アカウントの権限昇格
5. [防御回避] リモートサービスのエクスプロイト (T1210)
   a. リモートサービスの脆弱性悪用
   b. 多要素認証の回避
6. [資格情報アクセス] アプリケーションアクセス トークンの盗難 (T1528)
   a. API キーの盗難
   b. アプリケーションアクセス トークンの盗難
7. [探索] クラウドサービス探索 (T1526)
   a. クラウドサービスの探索
   b. CI/CD パイプライン情報の収集
8. [横移動] リモートサービスのエクスプロイト (T1210)
   a. RMM ツールを通じた移動
   b. ネットワーク内拡散
9. [収集] 情報リポジトリからのデータ (T1213)
   a. 顧客データの収集
   b. データリポジトリからの情報抽出

10. [流出] クラウドストレージへの流出 (T1567.002)
    a. クラウドストレージへのデータ転送
    b. 外部サーバーへのデータ流出
11. [影響] 影響のためのデータ暗号化 (T1486)
    a. ランサムウェアを使用したデータ暗号化
    b. 脅迫のためのデータ圧縮および保管

今月のサイバー脅威の特徴

最近のサイバー攻撃の事例は、技術的および戦術的な側面で非常に多様な特徴を示しています。複数の攻撃ベクターが使用され、特にソーシャルエンジニアリング技術と Malware の組み合わせが顕著です。例えば、ある脅威行為者は「ClickFix」というソーシャルエンジニアリング技術を通じて、Windows および macOS システムをターゲットに Malware を配布しました。この技術は、被害者がカメラの問題を解決するために Nvidia アップデートに偽装された悪意のあるソフトウェアをダウンロードして実行するよう誘導する方法で行われました。これにより Node.js 環境が設定され、BeaverTail Malware が実行されてクロスプラットフォームのデータ窃取が行われました。特に Windows 11 では、drvUpdate.exe というバックドアが追加で実行され、コマンドを実行しファイルを操作する機能を持っていました。
また、最近のキャンペーンでは新しい形態の攻撃ベクターも注目されています。例えば、地政学的な問題を悪用した攻撃では、「一帯一路」テーマのフィッシングメールを使用して VHDX ファイルを通じて攻撃を開始しました。このキャンペーンは特に NAKSOO というカスタムリモートコントロール Malware を使用して高度な技術を活用しました。この Malware は XOR と非標準 RC4 暗号化アルゴリズムを使用して通信し、DLL ハイジャックなどの技術を通じて持続性を維持しました。一方、北東アジア地域をターゲットにした攻撃では、スピアフィッシングとブラウザのゼロデイ脆弱性を活用してターゲットに侵入しました。このキャンペーンでは、NAKSOO リモートコントロール Malware がバージョン v3.1.14 に進化し、非標準 RC4 暗号化アルゴリズムを使用して通信するなど高度な技術を活用しました。攻撃は主に VHDX ファイルを通じて開始され、バックドア配布およびリモートローダー実行を通じて持続性を維持しました。
特に、金融と暗号通貨分野を目標にした攻撃では、主に ClickFix および悪意のある実行ファイルを活用したフィッシングを通じて被害者を誘引しました。例えば、あるキャンペーンでは BeaverTail と InvisibleFerret Malware を配布して暗号通貨ウォレットデータを窃取しようとする試みがありました。これらは主にウェブサイトに対するインフラを設定し、ユーザーに悪意のある実行ファイルを実行させる方法で攻撃を展開しました。このような攻撃は主にスピアフィッシングおよびソーシャルエンジニアリング技術を通じて行われ、さまざまなプラットフォームを対象にした感染チェーンを通じ

て Malware を配布しました。
この他にも、さまざまな攻撃技術と Malware が使用されました。例えば、LNK ファイルを通じた攻撃では、Windows 環境で mshta.exe を実行してコマンド＆コントロールサーバー（C2）と接続し、暗号化されたペイロードをダウンロードおよび実行する方法を使用しました。これらの攻撃はデータ窃取およびリモートコントロールを目的としており、プロセスインジェクションおよび AES 暗号化を通じた通信を通じて検出を回避しようとする試みを示しました。特に、サムスンの外部協力部門をターゲットにした攻撃では、GitHub のコンテンツ配信ネットワークを活用して悪意のあるスクリプトをダウンロードおよび実行する技術を使用しました。このキャンペーンは PDF ファイルに偽装したスクリプト

今月のサイバー脅威の示唆点

最近のサイバー攻撃のトレンドは、単純な侵入試みを超えて多層的で持続的な攻撃へと進化しています。攻撃者は様々な攻撃ベクターを併用して防御システムを回避し、長期的なアクセスを確保しようとする戦略を強化しています。特に、ソーシャルエンジニアリング技術とマルウェアの結合が顕著であり、被害者の心理を巧妙に利用して初期アクセスを確保した後、ネットワーク内部で徐々に権限を拡大し情報を窃取する手法が一般化しています。最近報告された事例では、攻撃者が Outlook アプリケーションのイベント（Application_MAPILogonComplete、Application_NewMailEx）を利用して悪性マクロの実行を保証し、ユーザー認証情報を窃取した後、持続性を確保する方法が観察されました。また、クラウドベースのサービスのような信頼されるプラットフォームを悪用して検出を回避する攻撃が増加しており、Dropbox、Google Drive、SharePoint API を利用したデータ流出の試みが頻繁に捉えられています。これは、組織がクラウドサービスの使用ポリシーを再検討し、クラウドネイティブのセキュリティソリューションを積極的に導入する必要があることを示唆しています。
AI 技術の活用が急速に拡散しています。攻撃者は AI を利用してフィッシングメールの作成やボイスフィッシングシナリオを自動化し、セキュリティフィルターを回避する能力を確保しています。また、AI 生成コンテンツを基に偽の報道ウェブサイトを作成し、政治的扇動や虚偽情報を流布し、世論を混乱させるキャンペーンを行っています。これらの変化は、組織が AI ベースの脅威検出ソリューションを導入し、内部スタッフを対象とした定期的な訓練を通じてフィッシング対応能力を強化する必要があることを意味します。ネットワークインフラへの攻撃も深刻化しており、ルーター設定の操作、SSH を利用したリモートアクセス、GRE・IPsec トンネリングを活用した隠密なデータ窃取の試みが増加しています。これにより、ネットワークモニタリング、異常行動検出、トラフィック分析能力を高度化することが必須の課題として浮上しています。
攻撃対象の産業はますます細分化され、特定の産業群に合わせて精巧化されています。金融、暗号通貨、エネルギー、防衛、外交など戦略的価値の高い分野が集中的に攻撃を受けており、攻撃者は産業

ごとの業務プロセスと運用環境に対する深い理解に基づいて、特化されたペイロードと社会工学メッセージを作成しています。例えば、暗号通貨ウォレットのデータを盗むための BeaverTail・InvisibleFerret マルウェアキャンペーン、政府機関および防衛分野を狙った悪意のある MSC ファイル攻撃、教育機関を対象とした Roundcube Webmail リモートコード実行攻撃が確認されています。これらのカスタマイズされた攻撃は、産業別のセキュリティ戦略の差別化の必要性を示しており、各産業が特化されたセキュリティソリューションと対応体制を導入する必要があることを示唆しています。

国家レベルの支援を受ける攻撃グループの活動はますます精巧になっています。彼らは合法的なインフラを悪用し、エンコードされたペイロードと多段階感染チェーンを設計して検出を回避し、長期的なスパイ活動を行います。最近発見された「一帯一路」イニシアティブをテーマにしたフィッシングキャンペーンは、VHDX ファイルを活用し、カスタムリモートコントロールマルウェア（NAKSOO）を使用して DLL ハイジャックと非標準の RC4 暗号化通信を実装することで持続性を維持しました。これは、組織が従来の防御策にのみ依存する場合、対応が困難であることを示しています。国家間の協力と脅威インテリジェンスの共有を通じて、防御能力を集団的に強化する必要があります。

このようなトレンドの中で、組織が取るべき対応の方向性は明確です。第一に、定期的なセキュリティ意識教育と模擬訓練を通じて、従業員のソーシャルエンジニアリング攻撃への対応能力を強化する必要があります。第二に、脅威インテリジェンスを積極的に活用し、最新の攻撃トレンドと TTP を継続的に把握し、防御戦略とセキュリティポリシーを定期的に更新する必要があります。第三に、インシデント対応計画を事前に策定し、実際のインシデント発生時に迅速に検知・遮断・復旧できる体制を構築する必要があります。第四に、クラウド・リモートワーク環境・産業制御システムなど新しい攻撃面に対するセキュリティチェックを強化し、侵害指標（IOC）と攻撃パターンを早期に識別できるモニタリング体制を整える必要があります。

最後に、サイバー脅威は今後さらに高度化することが予想されます。攻撃者はインフラを迅速に交換し、コード難読化、DLL ハロウィング、暗号化通信などの高度な技術を使用して検出を回避します。組織はセキュリティガバナンスを強化し、規制機関と協力して長期的なセキュリティ体制を整えることで、サイバー脅威からの回復力を高める必要があります。これらの示唆は、短期的な対応を超えて長期的な戦略の策定と国際的な協力を含むアプローチが必要であることを示しています。

Recommendation

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

1. 脆弱性保護 (Exploit Protection)

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

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

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

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

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

3. セキュリティ認識教育 (User Training)

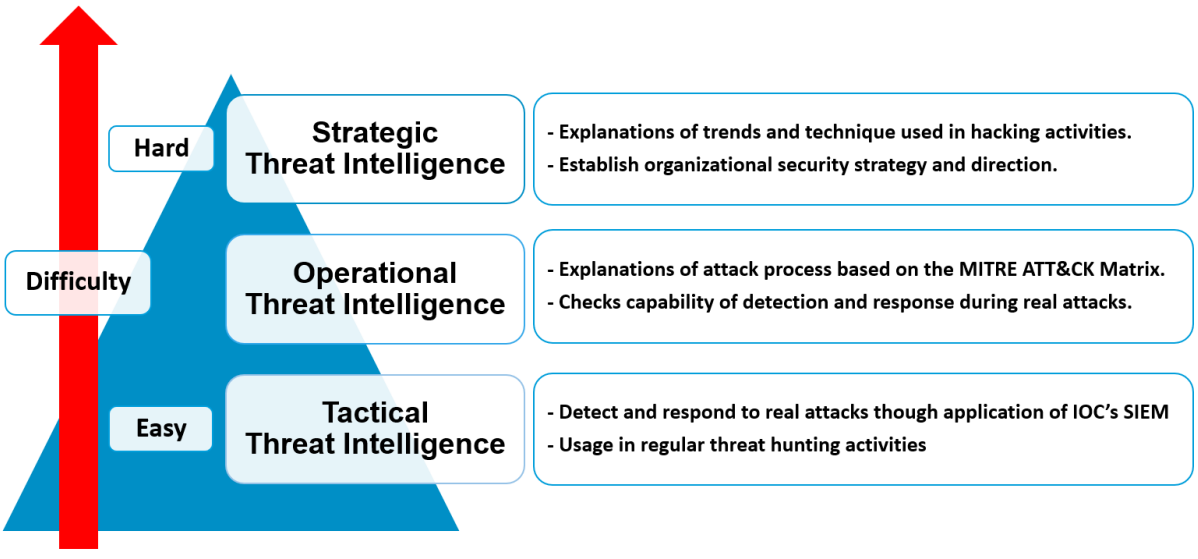
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

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

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

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

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



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

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

5. ネットワークにおける脅威緩和

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

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

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

2) ネットワーク細分化 (Network Segmentation)

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

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

6. ユーザーアカウントの脅威緩和

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

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

2) アカウント使用政策 (Account Use Policies)

アカウントのセキュリティ設定に関した政策設定の検討が必要

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

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

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

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

7. エンドポイントの脅威緩和

1) ソフトウェアアップデート(Update Software)

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

2) OSの構成 (Operating System Configuration)

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

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

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

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

4) 実行防止 (Execution Prevention)

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

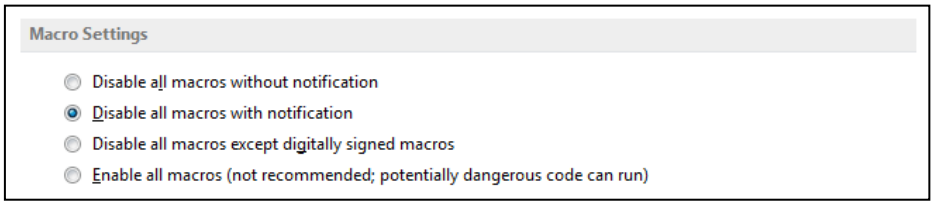
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

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

Program)

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

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



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

6) コード署名 (Code Signing)

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

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

7) アンチウイルス (Antivirus)

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

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

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

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

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

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

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

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

10) 企業モバイル政策 (Enterprise Policy)

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

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

LEGAL DISCLAIMER

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

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

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

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

NSHC.

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