NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI20250404

2024年度 SectorDグループの活動まとめ

Cyber Threat Intelligence

April 2025

NSHC PTE. LTD.

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

목차

- 無断転載禁止(Do not share) ー この著作物の内容は特定の顧客へご提供しております。当コンテンツの内容、画像などの無断転載・無断使用を固く禁じます。
- 秘密保持契約(Non-disclosure agreement) ー この著作物は NDA(秘密保持契約）の同意の上、ご提供しております。これに違反した場合は、法的措置になる恐れがございます。
- 注意 ー このライセンスの許容範囲を含んだその他の著作権関係の事項はサービス担当者を通した上、必ず確認を行った上でご利用ください。

イラン政府支援のハッキンググループSectorD

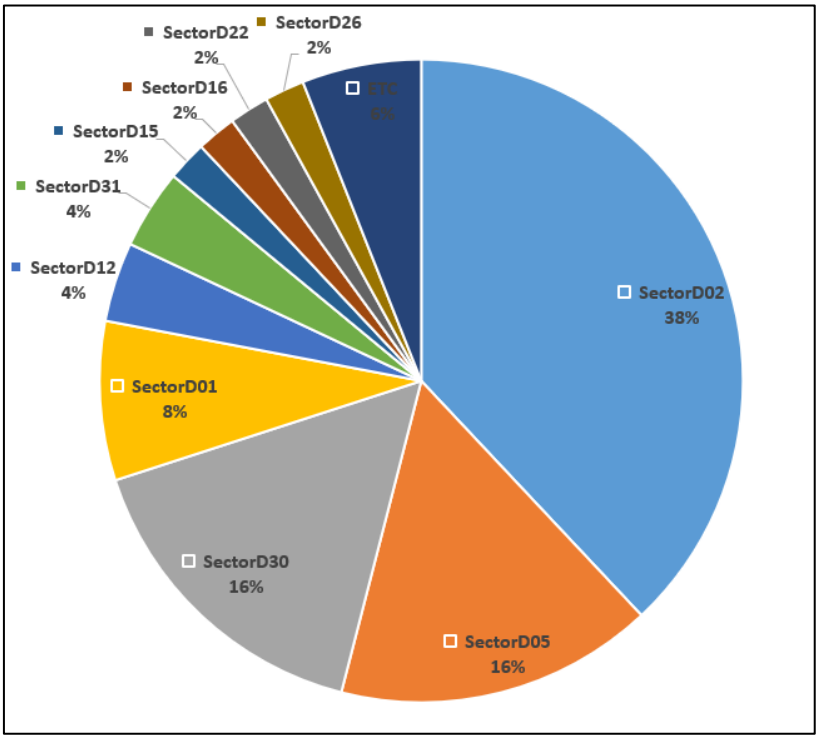
1. SectorDグループの活動

イラン政府支援のハッキンググループであるSectorDグループは、主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行ってきました。最近のSectorDハッキンググループの活動目的は、イラン政府に反対する人物や国家の政治、外交活動など、政府活動に関連する高度な情報を収集することを目的としていると分析されています。

2024年の1年間に発生したSectorDグループの活動量を分析した結果、合計13のサブグループが発見され、SectorD02グループの活動が最も顕著であることが確認されました。

SectorD02グループは、他のセキュリティ企業によってMuddyWaterとして知られているグループであり、このグループはソーシャルエンジニアリング手法を利用してマルウェアを拡散する戦略を主に使用するグループです。

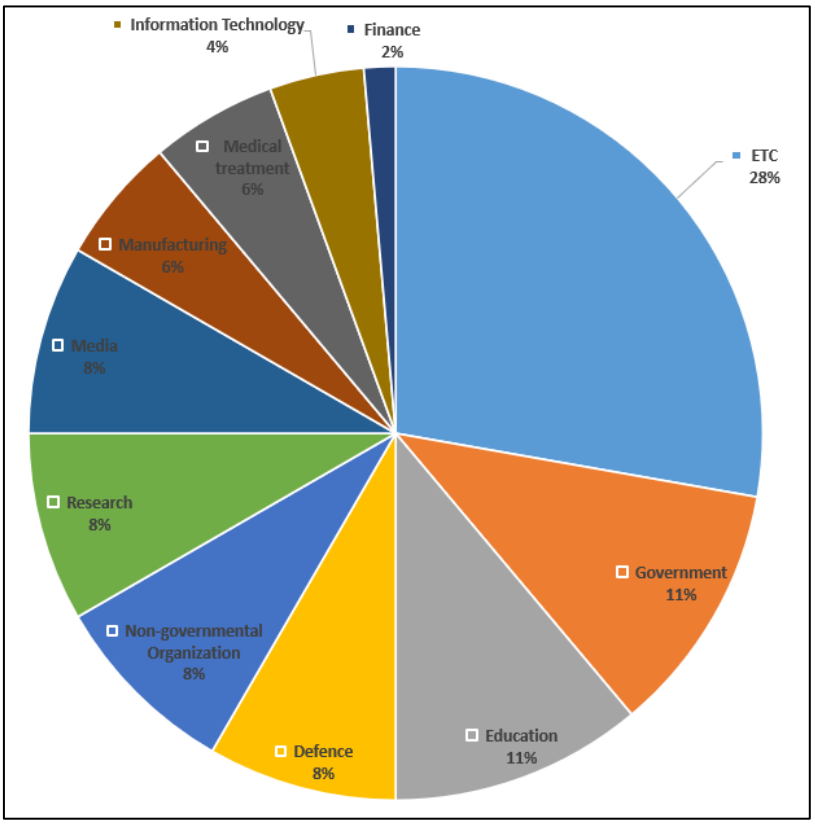
このグループは、彼らを支援する政府の情報機関であるMOIS（情報保安省）と関連があるとされており、この関係を基に主要なサイバー活動に参加した可能性があると見られています。



[図 1: 2024 年に確認された SectorD グループのサブグループ活動量]

2. 攻撃対象産業群

SectorDグループの攻撃対象産業群を分析した結果、政府（Government）産業群と教育産業群を対象に最も多くの攻撃を行ったことが確認される。
このような産業群が優先的に選ばれた背景には、SectorDグループの活動目的が高価値データを確保し、それを長期的に蓄積・活用できる情報収集基盤を構築することにあると見られるためである。
特に政府部門は、外交、安全保障、エネルギーおよびインフラなど国家戦略に関連する多様な情報を扱っており、教育部門もまた研究開発（R&D）、学術協力、高等教育機関の技術資産など高価値データを含んでいるため、情報収集活動の優先対象となる傾向があります。これらの対象選別は単なる情報アクセスを超えて、長期的な動向把握や政策環境分析など複合的な戦略的目的に関連していると評価されています。

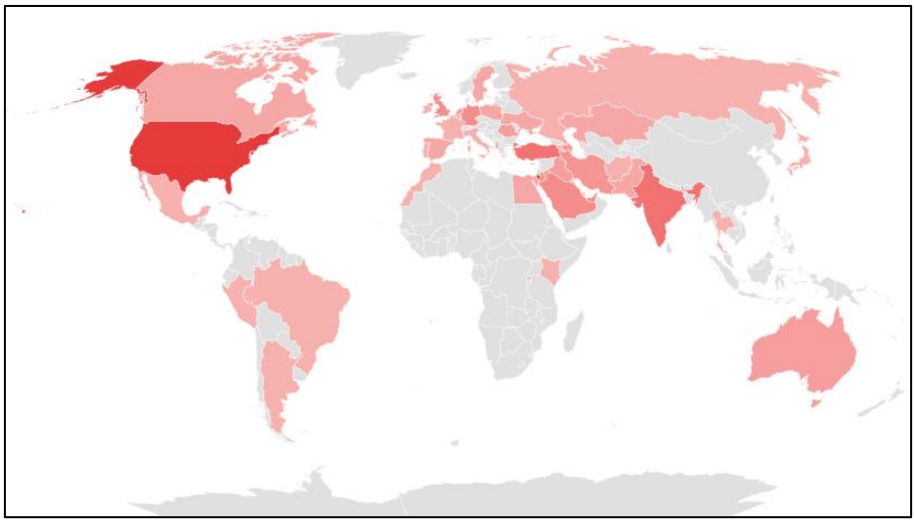


[図 2: 2024 年 SectorD グループの攻撃対象となった産業群の統計]

3. 攻撃対象国

次は、2024年のSectorDグループの攻撃対象国を地図に視覚化した結果であり、赤色が濃いほど攻撃頻度が高かったことを意味します。
分析の結果、該当グループはイスラエルを主要な攻撃対象としていることが確認され、アメリカがそれに続いていることが分かりました。
イスラエルは、SectorDグループを支援する国と長期間にわたり複雑な外交および安全保障関係を維持してきた主要な国の一つであり、軍事および情報インフラに関連するサイバー活動の戦略的優先順位が高く評価されている国と見られている。

次に、アメリカはこれらを支援する政府に対して経済制裁とサイバー活動制限措置を主導的に行ってきた国であり、SectorD グループの観点からは外交的・経済的脅威要因として認識される可能性がある。このような背景の中で、アメリカ国内の政府および安全保障関連機関を対象とした情報収集および影響力行使を目的とするサイバー脅威活動が継続していると判断される。

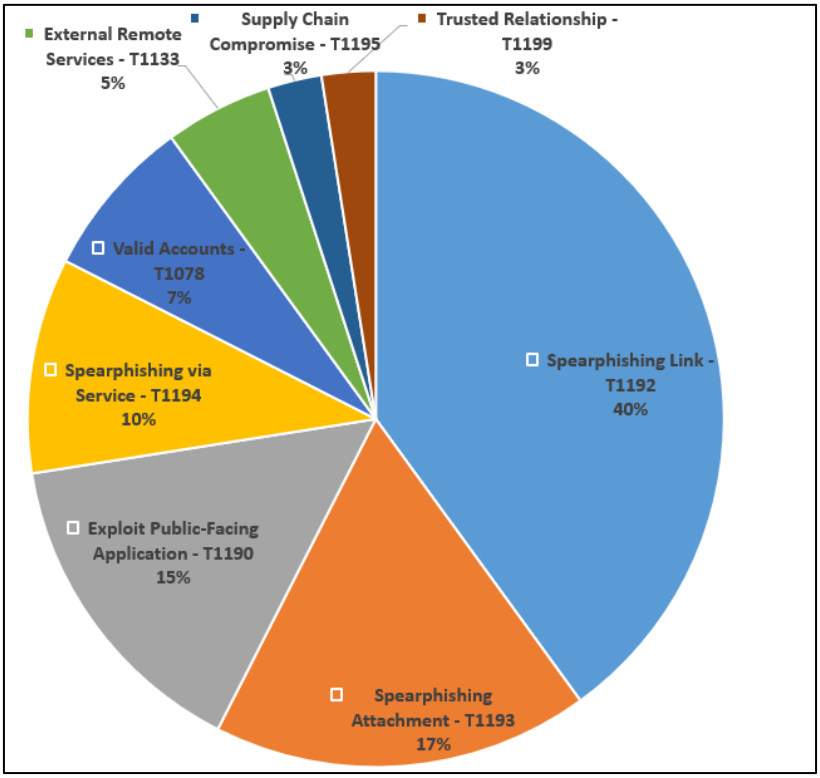


[図 3: SectorD グループの攻撃対象国]

4. 最初の侵入（Initial Access）

2024年、SectorDグループの攻撃事例を分析した結果、最初の侵入戦術としてフィッシング（スピアフィッシング）が最も多く悪用されていることが確認されました。フィッシングは特定の対象を精密に狙う社会工学に基づく攻撃手法であり、伝達されるメディアの種類に応じて「添付ファイルを通じた戦術（スピアフィッシングアタッチメント）」、「悪意のあるリンクを利用した戦術（スピアフィッシングリンク）」、「正常なサービスを悪用する戦術（スピアフィッシングviaサービス）」の3つに分類されます。
これは、リンクベースの戦術が他の侵入方法よりも攻撃インフラの再利用と攻撃フローの柔軟な制御が可能であるため、戦術的に有利であると解釈されます。悪性リンクは、メール送信時には単純なURLの形で存在し、該当グループがサーバー側で悪性コンテンツを後から挿入したり、攻撃対象の接続条件（時間帯、IP、ブラウザなど）に応じて応答を動的に変更することができるため、状況に応じて攻撃を自由に制御できる利点があります。

また、SectorDグループはリンクに接続されたページを短期間運営後に廃棄したり、同じ攻撃コード構造を持つ複数のサーバー間で自動化されたインフラを活用することで、攻撃インフラの回転率と運用効率を最大化しているようです。このような戦術は、精巧なバックエンド（Backend）インフラと結合されており、検出されるまで繰り返し攻撃が可能であるという点で、彼らの意図と資源運用の両面において適合する侵入手段として機能します。



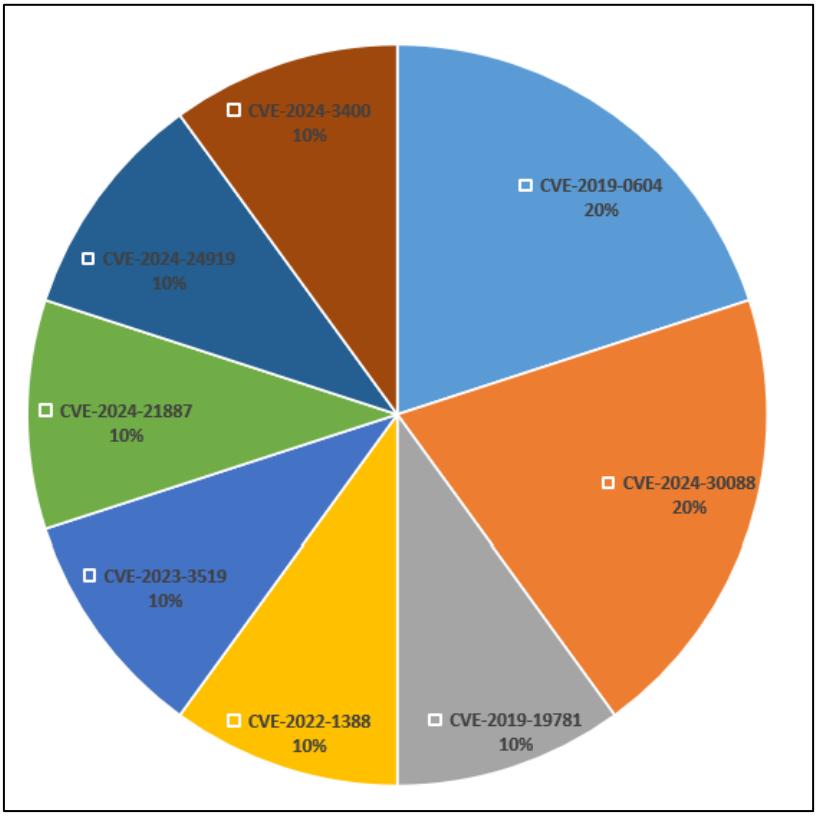
[図 4: SectorD グループ活用初期侵入統計]

5. 脆弱性 (Vulnerability)

SectorDグループは「CVE-2019-0604」と「CVE-2024-30088」の脆弱性を比較的多く使用していることが確認されている。

「CVE-2019-0604」脆弱性は、マイクロソフト シェアポイント（Microsoft SharePoint）で発生するリモートコード実行の脆弱性です。この脆弱性は、アカウントや認証情報がなくても内部ネットワークに侵入できるため、この脆弱性が悪用されたと分析されています。

「CVE-2024-30088」脆弱性は、Windowsカーネルの権限昇格脆弱性であり、権限を奪取した後、システム全体を掌握するために利用され、特にマルウェアのインストールおよび内部拡散の段階で利用度が高い脆弱性と見られます。



[Figure 5: SectorD グループが悪用した脆弱性]

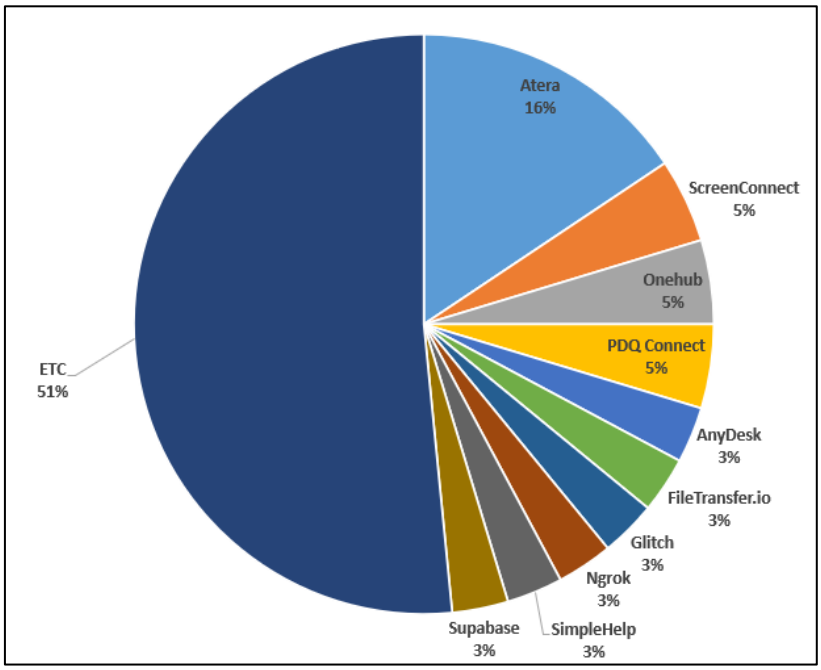
脆弱性コード	脆弱性分類	脆弱性対象
CVE-2019-0604	Remote Code Execution Vulnerability	F5 BIG-IP
CVE-2024-30088	Privilege Escalation Vulnerability	Citrix NetScaler ADC and NetScaler Gateway
CVE-2019-19781	Remote Code Execution Vulnerability	Ivanti Connect Secure and Policy Secure
CVE-2022-1388	Authentication Bypass Vulnerability	Check Point Security Gateways
CVE-2023-3519	Remote Code Execution Vulnerability	Palo Alto Networks PAN-OS (GlobalProtect)
CVE-2024-21887	Command Injection Vulnerability	F5 BIG-IP
CVE-2024-24919	Information Disclosure Vulnerability	Citrix NetScaler ADC and NetScaler Gateway
CVE-2024-3400	Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure

[表 1: SectorD グループが悪用した脆弱性リスト]

6. オープンソース（Open-Source）およびフリーウェア（Freeware）

SectorDグループが最も多く悪用したオープンソースおよびフリーウェアを分析した結果、最も頻繁に使用されたツールはリモート管理ツールの一つであるアテラ（Atera）であることが確認された。

このツールは合法的なリモート制御ソフトウェアであり、セキュリティソリューションによってブロックされたり検出されたりする可能性が比較的低いです。これらはこのツールを悪用してリモートで攻撃対象のシステムを制御し、悪意のある行為を行おうとしたと分析されています。



[図 6: SectorD グループが悪用したオープンソースおよびフリーウェア]

2024年 SectorD グループ活動

次に示すのは、2024年の1年間に発見されたSectorDグループのハッキング活動に関する月別活動の詳細です。

1月のハッキング活動

イラン政府の支援を受けている SectorD グループの中で、今年 1 月に 1 つのハッキンググループの活動が発見されました。それは SectorD05 グループです。
SectorD05 グループの活動はセーシェルで発見されました。該当グループはニュース記者を装い、攻撃対象にイスラエルとハマスの戦争に関する記事への意見を求めるフィッシングメールを使用しました。
SectorD のハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行ってきました。最近の SectorD ハッキンググループの活動目的は、イラン政府に反対する人物や国々の政治、外交活動など、政府活動に関連する高度な情報を収集することを目的としていると分析されています。

3月のハッキング活動

イラン政府の支援を受けている SectorD グループの中で、今年 3 月に 1 つのハッキンググループの活動が発見されました。それは SectorD15 グループです。
SectorD15 グループの活動は、ドイツ、アラブ首長国連邦、インド、イスラエル、イラン、ルーマニア、トルコ、アルバニアで発見されました。該当グループは、中東諸国の航空宇宙および防衛産業を対象に、偽の求人提案テーマとイスラエル-ハマス戦争テーマを使用し、フィッシングウェブサイトを通じた資格情報の収集や情報収集、リモート制御機能を実行する Malware を使用しました。
SectorD のハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行ってきました。最近の SectorD ハッキンググループの活動目的は、イラン政府に反対する人物や国々の政治、外交活動など、政府活動に関連する高度な情報を収集することを目的としていると分析されています。

4月のハッキング活動

イラン政府の支援を受けている SectorD グループの中で、今年 4 月に 2 つのハッキンググループの活動が発見されました。それらは SectorD02 と SectorD12 グループです。
SectorD02 グループの活動は、イスラエル、ルーマニア、トルコ、カナダで発見されました。該当グループは、ウェブセミナー招待文書に偽装したリンクが含まれたフィッシングメールを使用し、最終的にリモート制御ツールであるアテラ（Atera）を通じて攻撃対象システムへのリモート制御を試みました。
SectorD12 グループの活動はアメリカで発見されました。該当グループは航空宇宙および防衛産業の求職者を対象にフィッシング攻撃を行い、人事管理ソフトウェアに偽装した Malware を攻撃対象が直接実行するように誘導しました。
SectorD ハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行っており、最近の SectorD ハッキンググループのハッキング活動の目的は、イラン政府に反対する人物または国々の政治、外交活動など政府活動に関連する高度な情報を収集することを目的として分析されています。

5月のハッキング活動

イラン政府の支援を受けている SectorD グループの中で、今年 5 月に 2 つのハッキンググループの活動が発見されました。それらは SectorD02 と SectorD30 グループです。

SectorD02 グループの活動は、アメリカ、シンガポール、イスラエル、エジプト、イタリア、インド、トルコで発見されました。該当グループはフィッシングメールを通じて Egnyte ファイル共有ウェブサイトから圧縮ファイルをダウンロードするよう誘導し、中東地域のゴラン高原議会に関連する内容に偽装して、リモートモニタリングおよび管理ソリューション（Remote Monitoring and Management, RMM）の一つである Atera をインストールするよう誘導しました。
SectorD30 グループの活動は、アメリカ、イギリス、ウクライナ、イスラエル、オーストラリアで発見されました。該当グループは、追加のマルウェアをダウンロードできる VBS（Visual Basic Script）ファイルを攻撃対象のシステムに配布しました。攻撃対象が VBS ファイルを実行すると、ジェンダー平等に関連する内容の Adobe PDF おとりファイルと共に、Windows PE 形式の追加のマルウェアが攻撃対象のシステムにダウンロードされることが確認されています。
SectorD ハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行っており、最近の SectorD ハッキンググループのハッキング活動の目的は、イラン政府に反対する人物または国々の政治、外交活動など政府活動に関連する高度な情報を収集することを目的として分析されています。

6月のハッキング活動

イラン政府の支援を受けている SectorD グループの中で、今年 6 月に 1 つのハッキンググループの活動が発見されました。これらは SectorD02 グループです。
SectorD02 グループの活動は、サウジアラビア、ケニア、イスラエル、アゼルバイジャン、ヨルダン、トルコで発見されました。該当グループは、文書内にフィッシングリンクが存在するウェブセミナー招待内容の餌 PDF 文書を使用し、最終的に情報収集およびリモート制御機能を実行するマルウェアを使用しました。
SectorD ハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行っており、最近の SectorD ハッキンググループのハッキング活動の目的は、イラン政府に反対する人物または国々の政治、外交活動など政府活動に関連する高度な情報を収集することを目的としていると分析されています。

7月のハッキング活動

イラン政府の支援を受けている SectorD グループの中で、今年 7 月に活動が発見されたハッキンググループは 1 つであり、それは SectorD02 グループです。
SectorD02 グループの活動は、ヨルダン、イスラエル、トルコ、サウジアラビア、インド、ポルトガル、ポーランド、ドイツ、シンガポール、オランダで発見されました。該当グループは、ウェブセ

ミナー資料に偽装した MSI（Windows Installer）マルウェアを使用し、最終的にリモート制御ツールであるアテラ（Atera）を通じて攻撃対象システムのリモート制御を試みました。
SectorD ハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行っており、最近の SectorD ハッキンググループのハッキング活動の目的は、イラン政府に反対する人物または国々の政治、外交活動など政府活動に関連する高度な情報を収集することを目的として分析されています。

8月のハッキング活動

イラン政府の支援を受けている SectorD グループの中で、今年 8 月に合計 3 つのハッキンググループの活動が発見されました。これらは SectorD02、SectorD05、SectorD30 グループです。
SectorD02 グループの活動は、スウェーデン、アメリカ、ウクライナ、ポーランド、インド、イスラエルで発見されました。該当グループは、ウェブセミナー資料に偽装した MSI（Windows Installer）マルウェアを使用し、最終的に商用リモート制御ツールであるアテラ（Atera）を通じて攻撃対象システムへのリモート制御を試みました。
SectorD05 グループの活動はレバノンで発見されました。該当グループは、Microsoft SQL サーバー関連プログラムに偽装した Go 言語（Golang）で作成されたマルウェアを使用し、攻撃用サーバーから命令を受け取り、ファイルシステムの操作やネットワークを通じた内部拡散機能を実行します。
SectorD30 グループの活動は、アメリカ、イラン、オーストラリア、イスラエル、イギリスで発見されました。該当グループは、マイクロソフト Word 形式のマルウェアを使用し、内部に含まれるマクロによって VBA スクリプトがバッチスクリプト形式のマルウェアをダウンロードおよび実行し、最終的に攻撃対象システムの情報収集および資格情報の窃取機能を持つ PE マルウェアを使用しました。
SectorD ハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行っており、最近の SectorD ハッキンググループのハッキング活動の目的は、イラン政府に反対する人物または国々の政治、外交活動など政府活動に関連する高度な情報を収集することを目的として分析されています。

9月のハッキング活動

イラン政府の支援を受けている SectorD グループの中で、今年 9 月に合計 5 つのハッキンググループの活動が発見されました。これらは SectorD01、SectorD02、SectorD12、SectorD16、SectorD28 グループです。

SectorD01 グループの活動はイラク、パキスタン、バーレーンで発見されました。該当グループが使用したマルウェアは、政府機関のメールアカウントをコマンド・アンド・コントロール（C2）サーバーとして利用し、DNS リクエストを通じてデータを送信できる DNS トンネリング技術を使用してデータを外部に流出させました。
SectorD02 グループの活動はイスラエルで発見されました。該当グループは情報セキュリティ関連のフォームを記入するよう求める内容を含んだスピアフィッシングメールを使用し、最終的にリモートコントロールツールである Atera を通じて攻撃対象システムへのリモート制御を試みました。
SectorD12 グループの活動は、アメリカとアラブ首長国連邦で発見されました。このグループは、衛星通信会社のポリシーガイドとインフラセキュリティガイドの内容を Adobe PDF 文書に偽装した Malware を使用し、最終的にシステムおよびネットワーク環境に関する情報を収集し、状況に応じて持続性の確保、コマンドの実行、追加の Malware のダウンロードなどを行うことができる Malware を使用しました。
SectorD16 グループの活動は、イスラエル、アメリカ、アゼルバイジャン、アラブ首長国連邦で発見されました。該当グループはネットワークデバイスの脆弱性を悪用して初期アクセスを確保した後、それを基にネットワークアクセス権を取得し、後続のランサムウェア攻撃の足場を築きました。彼らは取得したネットワークアクセス権とドメイン管理者権限をランサムウェア提携組織に提供し、ランサムウェアの配布を支援し、その見返りとしてランサム支払い金額の一部を手数料として受け取り、収益を上げました。
SectorD28 グループの活動は、イスラエル、イギリス、ヨルダン、イラン、サウジアラビア、トルコ、キプロス、スウェーデン、イラク、インド、オランダ、アメリカ、クウェート、カタールで発見されました。該当グループはウェブシェルを通じて初期アクセス権限を確保し、その後、リモート制御マルウェアを使用してネットワーク内でコマンド制御を行い、これにより他の脅威グループにアクセス権限を渡したり、後続攻撃を行うための基盤を整えました。
SectorD ハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行っており、最近の SectorD ハッキンググループのハッキング活動の目的は、イラン政府に反対する人物または国家の政治、外交活動など政府活動に関連する高度な情報を収集することを目的としていると分析されています。

10月のハッキング活動

イラン政府の支援を受けている SectorD グループの中で、今月 10 月に合計 4 つのハッキンググループの活動が発見されました。これらは SectorD01、SectorD02、SectorD05、SectorD30 グループです。
SectorD01 グループの活動は、アラブ首長国連邦とイランで発見されました。該当グループは、Microsoft Exchange サーバーのような公共アプリケーションの脆弱性を悪用し、攻撃対象のサーバ

ーに Web シェルをインストールしてリモートコマンド実行環境を構築しました。そして、攻撃対象システムで.NET ベースのマルウェアを実行し、攻撃対象システムからデータを収集し、暗号化された形で外部に送信しました。
SectorD02 グループの活動は、アゼルバイジャン、イスラエル、アイルランド、アメリカ、パキスタン、ドイツで発見されました。該当グループは、カンファレンス資料に偽装した Windows インストーラー（MSI）マルウェアを使用し、最終的にリモート制御ツールである PDQ Connect を通じて攻撃対象システムのリモート制御を試みました。
SectorD05 グループの活動はアメリカとイスラエルで発見されました。該当グループは政府機関、軍事組織、研究機関などを主要な攻撃対象としており、フィッシングメールを通じてマルウェアを含む PDF 文書を送信しました。
SectorD30 グループは、メール、メッセージングプラットフォーム、またはソーシャルメディアを通じて攻撃対象に接触し、信頼できる機関や個人を装って資格情報を入力するように誘導しました。
SectorD ハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行っており、最近の SectorD ハッキンググループのハッキング活動の目的は、イラン政府に反対する人物または国々の政治、外交活動など政府活動に関連する高度な情報を収集することを目的としていると分析されています。

11月のハッキング活動

イラン政府の支援を受けている SectorD グループの中で、今回 11 月に合計 3 つのハッキンググループの活動が発見されました。それらは SectorD02、SectorD05、SectorD31 グループです。
SectorD02 グループの活動は、ルワンダ、モロッコ、イスラエル、カナダ、ブラジル、アフガニスタン、イギリス、アメリカ、カザフスタン、インド、ペルー、アルメニア、エジプト、スペイン、日本、イラク、アルゼンチン、ヨルダン、ドイツ、ルクセンブルクで発見されました。該当グループは未払い請求書に関する内容の PDF 文書が添付されたフィッシングメールを使用し、最終的にリモート制御ツールであるレベル(Level)を通じて攻撃対象システムへのリモート制御を試みました。
SectorD05 グループの活動は、イスラエル、インド、アルバニア、トルコ、アラブ首長国連邦で発見されました。該当グループは、LinkedIn のようなプラットフォームで偽の採用担当者プロフィールを作成し、採用ウェブサイトに偽装したフィッシングリンクを攻撃対象に送信し、攻撃対象がフィッシングリンクを通じてマルウェアをダウンロードおよび実行するように誘導しました。最終的にリモート制御機能を持つバックドア方式のマルウェアを使用し、DLL サイドローディング技法を活用して検出を回避し、システム情報を収集します。
SectorD31 グループの活動は、アメリカ、ロシア、イスラエル、ドイツ、メキシコ、スペインで発見されました。該当グループは、イスラエル国家サイバー局（Israel National Cyber Directorate,

INCD）を装ったフィッシングメールを通じてモジュール型マルウェアを配布し、リモートコマンドの実行、データの窃取、スクリーンショットのキャプチャなどの機能を実行します。
SectorD ハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行っており、最近の SectorD ハッキンググループのハッキング活動の目的は、イラン政府に反対する人物または国々の政治、外交活動など政府活動に関連する高度な情報を収集することを目的としていると分析されています。

12月のハッキング活動

イラン政府の支援を受けている SectorD グループの中で、今年 12 月に 1 つのハッキンググループの活動が発見されました。それは SectorD37 グループです。
SectorD37 グループの活動はアメリカとイスラエルで発見されました。該当グループはサプライチェーン攻撃とフィッシングメールを活用して初期侵入（Initial Access）に成功した後、IoT（Internet of Things）および OT（Operational Technology）環境に特化したマルウェアを使用しました。彼らが使用したマルウェアは MQTT（Message Queuing Telemetry Transport）プロトコルを使用して攻撃者のサーバーと通信し、主な機能には燃料サービスの妨害、データの窃取、機器の誤作動の誘発が含まれています。
SectorD ハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行っており、最近の SectorD ハッキンググループのハッキング活動の目的は、イラン政府に反対する人物または国々の政治、外交活動など政府活動に関連する高度な情報を収集することを目的としていると分析されています。

特徴点（Adversary Tradecraft）

2024 年の 1 年間で、SectorD には合計 13 以上のサブグループが識別され、その中で SectorD02 は年間 11 ヶ月以上活動が確認されるほど、継続的かつ集中的な作戦を展開しました。
全体的には、月に 1～5 つのサブグループが並行して活動しており、活動地域はイスラエル、アメリカ、ドイツ、アラブ首長国連邦、インド、トルコ、サウジアラビアなど、地政学的な利害関係が鋭い国々を中心に構成されていました。
攻撃対象は軍事および防衛産業、政府および外交組織、技術およびインフラ企業、エネルギー産業、メディア、教育機関など非常に広範囲に分布しており、これらの組織は高度な情報を保有するか、外部政策の意思決定に影響を与えることができる敏感な組織として分類されます。
攻撃手法はスピアフィッシング（Spear Phishing）に基づくアプローチが主流を占めており、LinkedIn チャンネルを活用した採用詐称、政府文書やセキュリティ通知の偽装、ウェビナー招待状

形式の文書ベースの攻撃、フィッシングウェブサイトへの誘導方式など、さまざまなソーシャルエンジニアリング手法が繰り返し利用されました。
攻撃に使用されたマルウェアは主にリモートモニタリングツール（RMM）に基づいており、Atera、Level、PDQ Connect などの商用ソリューションが悪用されました。一部のグループは自作のバックドアにモジュール化を適用し、リモートコマンド実行、資格情報の窃取、持続性の確保、追加のマルウェアダウンロードなどの機能を細分化しました。また、DNS トンネリング、Web シェル、SSH ベースのアクセスなど、検出を回避するコマンド＆コントロール（C2）方式が多数観察され、この過程で感染したシステムのコマンドを他の脅威グループに伝達する形の協力関係も捉えられました。
特定のサブグループは、侵害されたインフラを提携ランサムウェアグループに提供し、ランサム収益を共有する構造で運営されており、12 月にはサプライチェーン攻撃と IoT/OT に特化した Malware を組み合わせて物理的な機器の妨害を試みた状況も報告されました。
プラットフォームの観点からも、Windows を超えて IoT、OT、Linux、産業用プロトコル（MQTT、Message Queuing Telemetry Transport）などを狙うなど、攻撃ポートフォリオの技術的分散度が高まった年と分析される。

洞察（Analyst Insights）

2024 年の SectorD の活動は、明確に組織化された作戦単位に基づく戦略的ハッキングキャンペーンの性格を帯びています。特に、多数のサブグループが定期的に活動しており、攻撃の範囲や手段、プラットフォーム、被害の種類が多様化する構造は、単なる情報収集ではなく、持続可能な影響力の確保戦略の一環として解釈できます。
攻撃主体は政府機関や政策決定組織を狙い、政治・外交的な戦略情報を収集する一方で、後続攻撃（ランサムウェア、データ窃取、世論操作など）のための基盤構築も並行して行った。
技術的には単一のベクトルに依存せず、ソーシャルエンジニアリング技術と商用ツールを組み合わせたり、暗号化されたコマンド通信構造を通じて検出回避を最大化しています。特に、Atera、PDQ Connect、Level などの商用 RMM ツールの継続的な悪用は、セキュリティソリューションに依存した防御システムの弱点を攻撃する戦術と評価されています。
また、サブグループ間でのインフラ再利用、類似したコード構造、共有されたコマンドパターンは、内部ツールセットが共同で活用されている可能性を示唆しており、これによりグループ間の識別がさらに困難になっています。注目すべき点は、ランサムウェアのアフィリエイト形式の協力作戦とサプライチェーン攻撃が本格的に登場したことです。これは単に攻撃を実行する段階を超え、脅威行為者が外部グループとの連携を通じて「サービスとしての侵害」を提供する方式に拡張されていることを示しています。

対応の側面では、ウイルス対策ソフトの回避検出技術への対応だけでなく、ユーザー側の脅威認識の高度化、採用プラットフォームおよびコラボレーションツールのセキュリティ強化、外部共有インフラの正常な行動の異常兆候検出、IoT/OT システム専用のセキュリティルール設定など、産業に特化した検出戦略が必須とされる。

特に産業制御システム（ICS, Industrial Control System）と融合セキュリティの観点からの検出ルールの整備および脅威ハンティングに基づく先制検出戦略の策定が、今後の重要な課題となると見られる。

Recommendation

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

1. 脆弱性保護（Exploit Protection)

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

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

2. 脆弱性のスキャニング（Vulnerability Scanning)

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

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

3. セキュリティ認識教育（User Training)

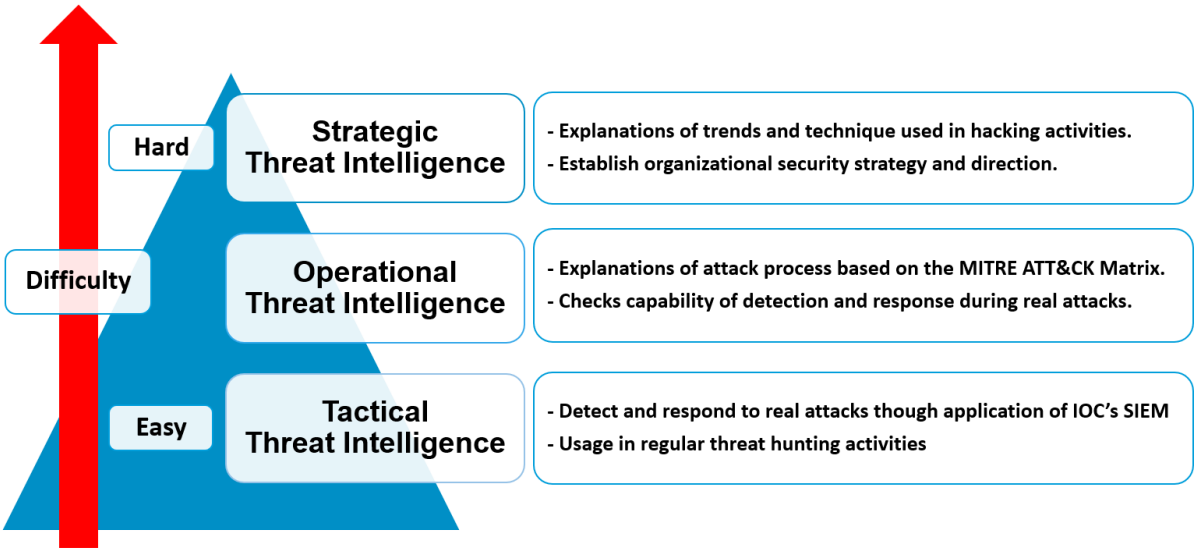
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

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

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

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

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



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

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

5. ネットワークにおける脅威緩和

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

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

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

2) ネットワーク細分化（Network Segmentation)

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

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

6. ユーザーアカウントの脅威緩和

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

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

2) アカウント使用政策 (Account Use Policies)

アカウントのセキュリティ設定に関した政策設定の検討が必要

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

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

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

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

7. エンドポイントの脅威緩和

1) ソフトウェアアップデート(Update Software)

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

2) OSの構成（Operating System Configuration)

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

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

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

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

4) 実行防止（Execution Prevention)

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

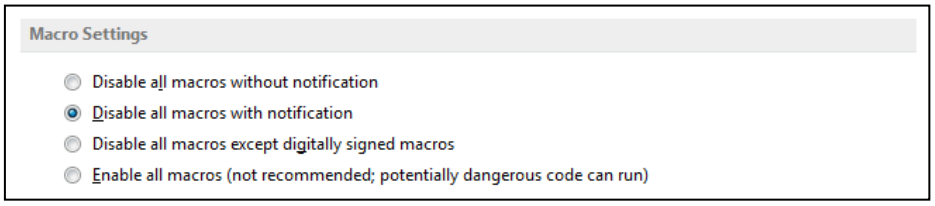
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

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

Program)

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

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



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

6) コード署名 (Code Signing)

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

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

7) アンチウイルス (Antivirus)

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

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

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

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

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

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

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

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

10) 企業モバイル政策 (Enterprise Policy)

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

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

Appendix

SectorDグループ関連の脅威イベントリスト

TimeStamp	ThreatRecon Platform Event Name	ThreatRecon Platform
2024-01-17	SectorD05 used a Phishing Email requesting comments on an Israel-Hamas war article	https://cti.nshc.net/events/view/6975
2024-02-13	SectorD30 used LNK Malware disguised as a US strategy in the Middle East documents	https://cti.nshc.net/events/view/7141
2024-02-27	SectorD15 used Malware disguised as Survey documents	https://cti.nshc.net/events/view/7235
2024-03-07	SectorD26 used Supply Chain Attack for hacktivist activities	https://cti.nshc.net/events/view/7313
2024-03-14	SectorD02 used RMM(Remote Monitoring & Management) tool disguised as tourism software	https://cti.nshc.net/events/view/7353
2024-03-21	SectorD02 used MSI Malware disguised as Pay Slip	https://cti.nshc.net/events/view/7402
2024-03-21	SectorD12 used Malware to target job applicants in the aerospace and defense industries	https://cti.nshc.net/events/view/7432
2024-03-29	SectorD02 used MSI Malware disguised as webinar program	https://cti.nshc.net/events/view/7480
2024-04-04	SectorD02 used Domain disguised as Google	https://cti.nshc.net/events/view/7558
2024-04-22	SectorD02 used MSI Malware disguised as tourism software	https://cti.nshc.net/events/view/7655
2024-05-02	SectorD30 used social engineering techniques to distribute Malware	https://cti.nshc.net/events/view/8055
2024-05-03	SectorD30 used a new Domains	https://cti.nshc.net/events/view/8059
2024-05-06	SectorD30 used social engineering techniques to distribute Malware	https://cti.nshc.net/events/view/8060
2024-05-20	SectorD29 used Wiper Malware targeted attack against ISRAEL	https://cti.nshc.net/events/view/8178
2024-05-24	SectorD02 used Word Malware disguised as Hajj Report	https://cti.nshc.net/events/view/8251
2024-06-09	SectorD02 used malicious PDF disguised as webinar program	https://cti.nshc.net/events/view/8349
2024-06-13	SectorD02 used phishing links disguised as online course themes	https://cti.nshc.net/events/view/8402
2024-06-23	SectorD02 used MSI Malware disguised as webinar software	https://cti.nshc.net/events/view/8478
2024-07-02	SectorD02 used MSI Malware variants	https://cti.nshc.net/events/view/8532
2024-07-04	SectorD02 used a new Domains	https://cti.nshc.net/events/view/8521
2024-07-11	SectorD02 used a malicious PDF of the National Cyber Security Forum content	https://cti.nshc.net/events/view/8584

2024-07-16	SectorD02 used Malware disguised as updated software	https://cti.nshc.net/events/view/8612
2024-08-05	SectorD02 used RAT Tool disguised as safety guidelines	https://cti.nshc.net/events/view/8837
2024-08-14	SectorD05 used Golang Malware variants	https://cti.nshc.net/events/view/8890
2024-08-14	SectorD30 used tailored credential phishing	https://cti.nshc.net/events/view/8894
2024-08-15	SectorD30 used a new Domains	https://cti.nshc.net/events/view/8895
2024-08-15	SectorD30 used a new Domains	https://cti.nshc.net/events/view/8905
2024-08-20	SectorD05 used Malware disguised as Fake Podcast invitation	https://cti.nshc.net/events/view/8935
2024-08-20	SectorD30 used tailored credential phishing	https://cti.nshc.net/events/view/8940
2024-08-28	SectorD16 sells admin credentials that enable ransomware attacks	https://cti.nshc.net/events/view/9002
2024-08-29	SectorD02 used Malware disguised as information security-related forms	https://cti.nshc.net/events/view/9183
2024-08-30	SectorD12 used LinkedIn-based social engineering techniques to deliver Malware	https://cti.nshc.net/events/view/9025
2024-09-10	SectorD02 used a new Domains	https://cti.nshc.net/events/view/9477
2024-09-11	SectorD01 used Malware disguised as PDF file	https://cti.nshc.net/events/view/9293
2024-09-12	SectorD01 used a new Domains	https://cti.nshc.net/events/view/9476
2024-09-20	SectorD28 used Malware to Support Initial Access Operations	https://cti.nshc.net/events/view/9413
2024-09-25	SectorD30 used a new Domains	https://cti.nshc.net/events/view/9660
2024-09-30	SectorD05 used a new Domains	https://cti.nshc.net/events/view/9639
2024-10-02	SectorD05 used a new Domains	https://cti.nshc.net/events/view/9693
2024-10-11	SectorD01 conducted Webshell attacks targeting exchange servers in the Middle East	https://cti.nshc.net/events/view/9785
2024-10-15	SectorD02 used RAT Tool disguised as conference materials	https://cti.nshc.net/events/view/9899
2024-10-29	SectorD02 used RAT Tool disguised as conference materials	https://cti.nshc.net/events/view/10256
2024-10-30	SectorD31 used fake hosting resellers and IP camera content for cyber information operations	https://cti.nshc.net/events/view/10212
2024-11-12	SectorD05 used Fake Job Offers to Target Aerospace Industry	https://cti.nshc.net/events/view/10507
2024-11-12	SectorD22 used a new Domains	https://cti.nshc.net/events/view/10504
2024-11-14	SectorD31 Used Malware Disguised as a Google Chrome Installer	https://cti.nshc.net/events/view/10612
2024-11-20	SectorD02 Used RMM Tool in Phishing Campaign to Dump Credentials	https://cti.nshc.net/events/view/10674
2024-12-10	SectorD37 used a Custom-Built IoT/OT Malware	https://cti.nshc.net/events/view/11276
2024-12-13	SectorD01 used Malware disguised as GoogleUpdate	https://cti.nshc.net/events/view/11642
2024-12-16	SectorD05 used a new Domains	https://cti.nshc.net/events/view/11336

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.