NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI2025090302

2025年上半期の金融産業の業界をターゲットにしたハッキンググループの活動分析レポート

Cyber Threat Intelligence Report

Sep 2025

NSHC PTE. LTD.

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

Table of Contents

- 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。

序論

金融業界は、機密データと金融取引システムの高い経済的価値のため、継続的にハッキンググループの主要な攻撃対象となっています。

金融業界で発生するサイバー脅威は、グローバル経済および企業運営に直接的な影響を与える可能性があるため、継続的なモニタリングと深層的な分析が不可欠です。

このような背景の中、NSHC脅威分析研究所（Threat Research Lab）は、金融業界を対象とするハッキンググループの動向をより体系的に把握し、対応戦略を策定するために、ThreatReconプラットフォームの脅威データを活用して2025年の金融業界関連のハッキンググループの活動情報を分析しました。ThreatReconプラットフォームは、NACEコード（欧州連合産業標準分類システム）の産業分類法に基づいて攻撃対象の産業を分類しており、その中で金融業界に関連する主要なカテゴリーは、金融（Finance）、銀行（Bank）、保険（Insurance）、投資（Investment）の4つで構成されています。

本報告書は、該当する4つの金融産業群に関連する脅威イベントデータを基に、ハッキンググループの活動情報を分析し、主要な攻撃対象国、侵入戦術、悪用された脆弱性、オープンソースおよびフリーウェアツールの使用事例を調査しました。これにより、金融産業群が直面するサイバー脅威を明確に把握し、効果的な対応戦略を策定するために必要な情報を提供することを目的としています。

ハッキンググループのタイプ

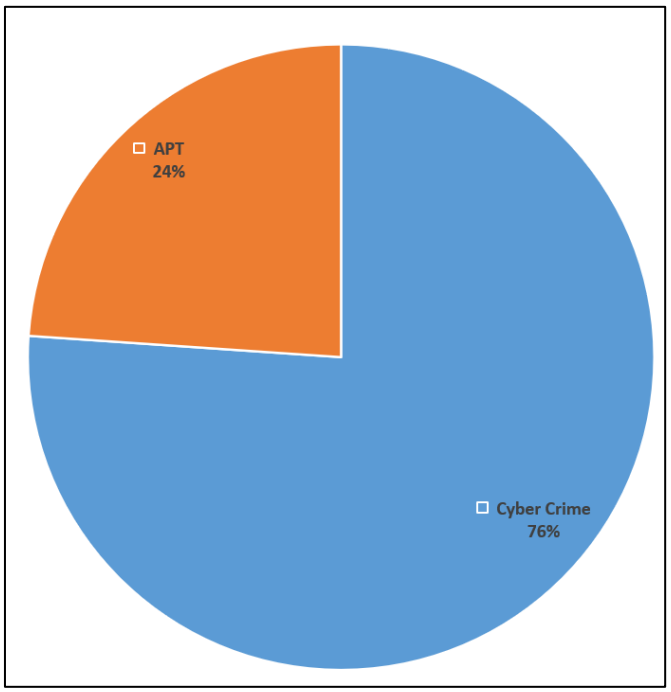
ハッキンググループのタイプは大きく分けてAPT（Advanced Persistent Threat）グループとサイバー犯罪グループに分類されます。APTグループは国家または特定の組織の支援を受け、長期的な情報窃取および偵察活動を行う特徴があり、攻撃の動機は主にスパイ活動や政治的利益、または地政学的目的の達成にあります。

一方、サイバー犯罪グループは主に金銭的利益を目的として活動し、直接的な収益を生み出すことができるランサムウェアやフィッシングなどの攻撃手法を好む。

2025年上半期に収集された脅威データを分析した結果、金融業界を対象とした攻撃の24%はAPTグループによって行われ、残りの76%はサイバー犯罪グループによって発生したことが確認されました。

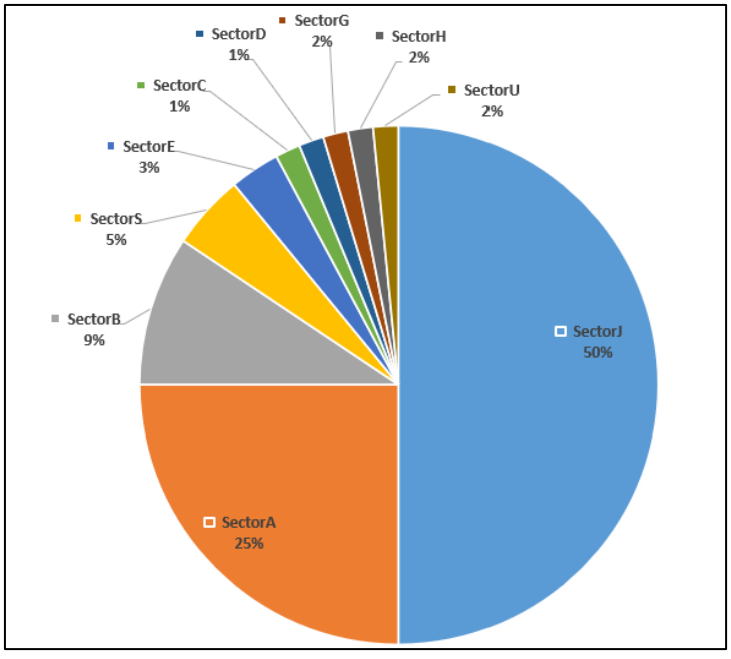
金融産業は直接的な金銭取引が行われる産業であり、この産業を対象に攻撃を行う場合、即時の金銭的利益を得ることができる口座情報やクレジットカードデータなどの高付加価値資産を奪取することができます。この特性により、金融産業はサイバー犯罪グループの主要なターゲットとなり、それに伴い、これらのグループによる攻撃の割合が相対的に高いと判断されます。

一方、APTグループの攻撃率はサイバー犯罪グループに比べて相対的に低く見えるが、これを根拠に金融業界を対象としたAPTグループの脅威が少ないと断定するのは難しいと思われる。APTグループは長期的な侵入と高度化された攻撃を通じて特定の高価値ターゲットを精密に狙う可能性があり、攻撃によって金融システム全般に及ぼす影響力が大きいため、注意が必要である。したがって、金融業界を対象としたAPTグループの攻撃パターンと動向に関する分析が必要と判断される。



[図 1: 金融業界を対象とした主要なハッキンググループ]

ハッキンググループ別の攻撃比率を分析した結果、[図 2]のように金銭的動機でハッキング活動を行うSectorJグループ、北朝鮮政府の支援を受けるハッキンググループであるSectorAがそれに続いた。
金銭的動機に基づいて活動するSectorJグループは、ランサムウェアの拡散やアカウント情報の窃取など、直接的な利益を狙った攻撃を主に行っており、国家の支援を基盤とするSectorAグループは、金融ネットワークを通じた資金確保と戦略的情報収集を目的として活動していると分析されている。
このような結果は、金融業界が犯罪目的と国家的目的の両方で主要なターゲットと見なされていることを示しています。



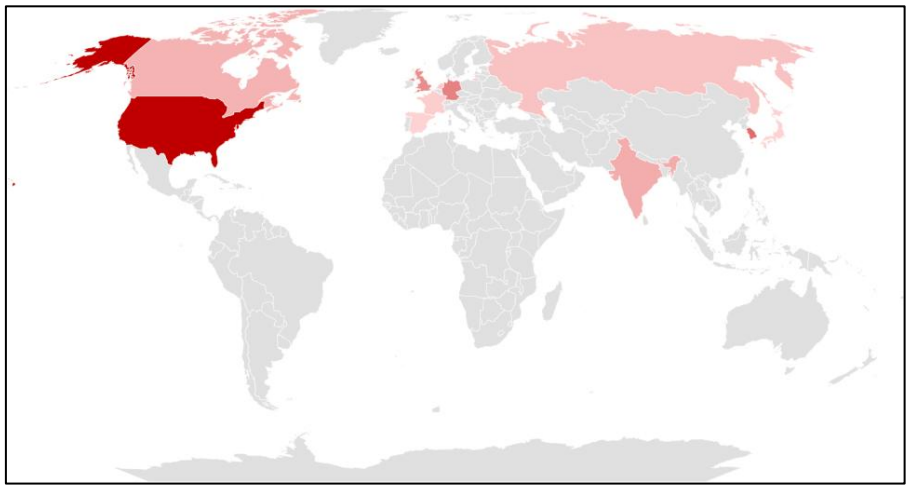
[図 2: 金融業界を対象にハッキング活動を行ったハッキンググループの割合]

攻撃対象国

2025 年上半期の間、APT グループとサイバー犯罪グループが攻撃対象とした国を地図で視覚化した結果、特定の地域で攻撃頻度が特に高い様子が見られました。地図で赤色が濃いほど、その国がより多くの攻撃を受けたことを意味します。分析によれば、APT グループとサイバー犯罪グループは北アメリカに位置するアメリカを主要な標的とし、多数のハッキング活動を行ったことが示されています。

2024 年の国際通貨基金（IMF）の世界経済見通しデータベースによれば、アメリカの 2024 年の名目 GDP は約 29 兆ドルで、世界で最も高いと分析されています。また、アメリカドルは国際取引で最も広く使用されている通貨です。つまり、アメリカは経済規模と通貨価値が最も高い国と評価されているため、ハッキンググループがアメリカを主要なターゲットにした可能性が高いです。

そして、[図 3]で確認できるもう一つの特異な点は、灰色の地域が存在するという点です。灰色の地域は 2025 年上半期にハッキンググループの攻撃対象にならなかった国々を意味し、アフリカ、一部の中央アジア、南太平洋に位置する国々であることが確認されます。これらの国々は相対的に通貨価値が低いため、攻撃が行われたとしてもハッキンググループにとって得られる金銭的利益が大きくないため、攻撃対象にならなかったと分析されます。



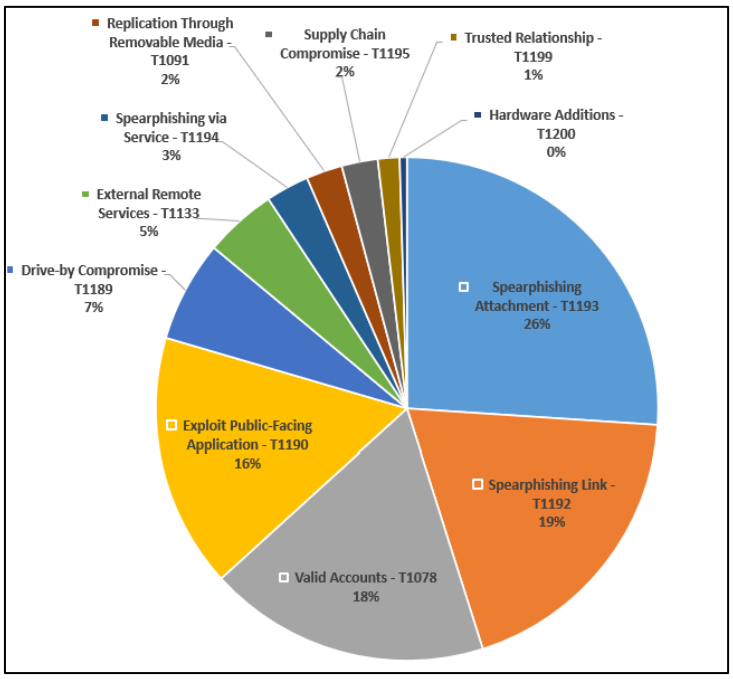
[図 3: 攻撃対象国]

ハッキンググループの攻撃手法

ハッキンググループは、目標システムを侵害し、悪意のある活動を行うために、さまざまな攻撃手法を活用します。彼らは技術的な脆弱性だけでなく、ソーシャルエンジニアリング技術やオープンソースツールを組み合わせて、セキュリティシステムを回避し、継続的なアクセス権を維持する戦略を使用します。
本章では、ハッキンググループが金融業界を対象に使用した主要な攻撃手法を分析した内容を説明する。

1. 初期侵入（Initial Access）

NSHC脅威分析研究所は、ハッキンググループが攻撃対象システムに最初に侵入するために使用した経路を、MITRE ATT&CKマトリックスの初期アクセス（Initial Access）戦術（Tactics）に基づいて分析しています。
2025年上半期、APTグループとサイバー犯罪グループが金融業界を対象に行った攻撃事例を分析した結果、APTグループとサイバー犯罪グループの両方が最初の侵入戦術としてフィッシングを最も多く悪用していることが確認されました。
フィッシングは、メール、メッセージ、偽のウェブサイトなどを利用して、攻撃対象が自ら悪意のあるリンクをクリックしたり、Malwareを実行したりするように誘導する社会工学的（ソーシャルエンジニアリング）手法であるため、攻撃成功率が高い戦術の一つです。特に、特定の組織や個人をターゲットにして精密に設計された攻撃手法であるスピアフィッシング（Spear Phishing）などの高度な攻撃技術を利用すると、特定の対象を狙ったカスタマイズされた攻撃を実行できると考えられます。
フィッシングが広く利用されるもう一つの理由は、攻撃コストに対する効果（投資利益率、ROI）が高いからです。脆弱性を悪用した攻撃を行うには、セキュリティ研究やエクスプロイトの開発が必要ですが、フィッシングは比較的少ないコストと技術で効果的な攻撃が可能です。また、ダークウェブではフィッシング攻撃に必要なフィッシングキットやメールアドレスリストなどが活発に取引されており、これを活用すればハッキンググループは特別な技術的知識がなくても大規模なフィッシングキャンペーンを展開できると考えられます。
何よりも、フィッシングは技術的な脆弱性ではなく人間の心理を悪用する方法であるため、企業がセキュリティポリシーを徹底的に策定しても、業務関連のメールを装ったフィッシング攻撃に従業員が騙されるリスクは依然として存在します。特に金融業界では、取引要求や文書交換がメールを通じて頻繁に行われる環境であるため、セキュリティ技術が進化しても依然として効果的な侵入手段として利用される可能性が高く、試みが多い分、フィッシング攻撃が成功する可能性もさらに高まると考えられます。

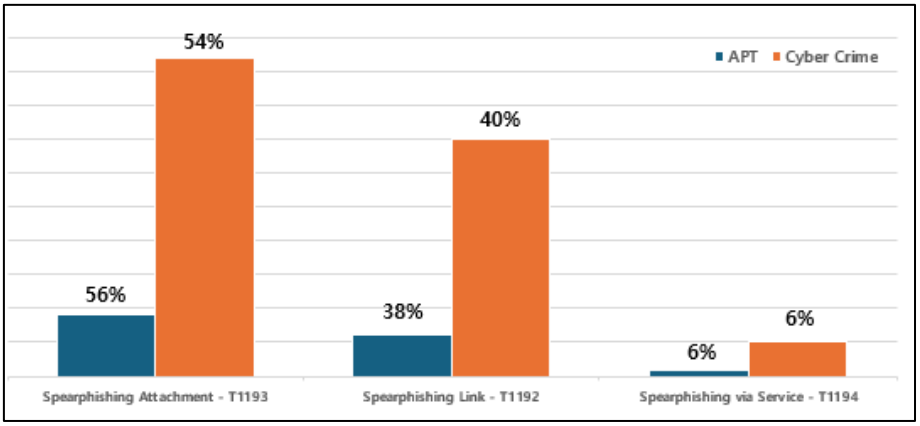


[図 4: ハッキンググループが活用した最初の侵入戦術]

APTグループとサイバー犯罪グループが最も多く使用した戦術として確認されたフィッシングは、攻撃対象が悪意のある行為を実行するように誘導する方法に応じて、次の3つの手法に分類することができます。

- **フィッシング添付ファイル：**ハッキンググループがメールなどに悪意のあるファイルを添付し、攻撃対象がそれを開くように誘導する手法です。悪意のあるファイルのタイプの中で、悪意のある文書を例に挙げると、マクロ機能や脆弱性を悪用したマルウェアが含まれており、実行されるとシステムを感染させる方式です。
- **フィッシングリンク：**ハッキンググループが悪意のあるリンクを含むメール、メッセージ、またはソーシャルメディアコンテンツを送信し、攻撃対象がそれをクリックするように誘導する手法です。攻撃対象がリンクをクリックすると、悪意のあるファイルが自動的にダウンロードされたり、フィッシングページを通じてアカウント情報が盗まれる形で攻撃が行われることがあります。
- **サービスを利用したスピアフィッシング：**ハッキンググループがサードパーティサービスを悪用してフィッシングメッセージを送信する手法です。例えば、ソーシャルメディアで攻撃対象と長期間会話を交わし信頼を築いた後、マルウェアファイルを実行させたり、悪意のあるサイトに接続して悪意のある行為を実行させる手法です。

このように 3 つの手法で分類された手法を基準に APT グループとサイバー犯罪グループのフィッシングサブ手法を分析した結果、[図 5]のようにリンクおよび添付ファイルベースのフィッシング手法が主要な攻撃手段として使用されていることが確認できる。特にリンクおよび添付ファイルベースのフィッシング手法が広く活用されている理由は、大量のメールを自動化システムを通じて迅速に送信でき、攻撃に必要なリソースが少ないためであると考えられる。



[図 5: ハッキンググループのフィッシング戦術サブ技法]

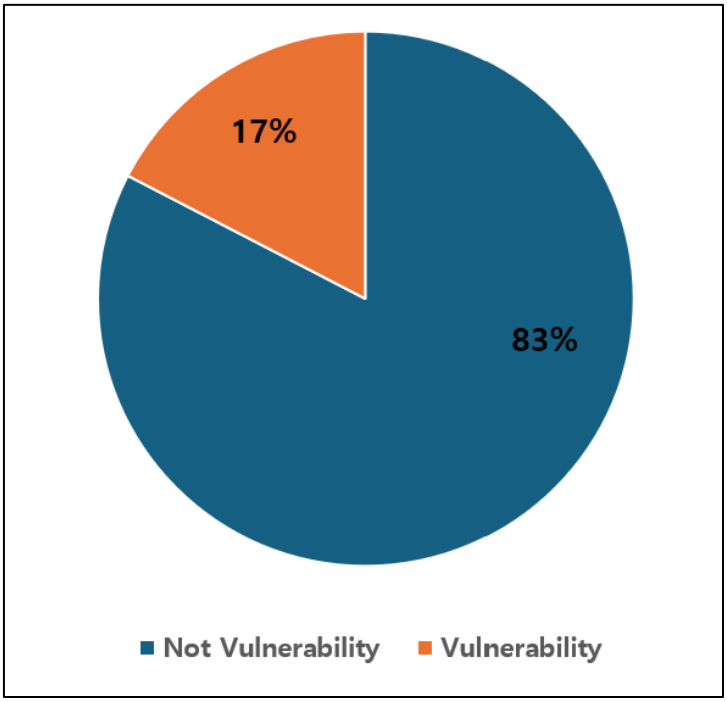
2. 脆弱性（Vulnerability）

脆弱性（Vulnerability）は、システムやソフトウェアにおいて悪意のある目的で悪用される可能性のあるセキュリティ上の弱点を意味します。2025年上半期にAPTグループとサイバー犯罪グループが金融業界を対象に行った攻撃事例を分析した結果、全体の攻撃事例のうち17%が脆弱性に関連していることが確認されました。

割合で見ると 17%は少ない数字に見えるかもしれませんが、脆弱性に基づく攻撃が成功した場合、その影響度は大きいです。これは、脆弱性を悪用すると、権限昇格（Privilege Escalation）、横移動（Lateral Movement）、リモートコード実行（Remote Code Execution）などの追加攻撃が体系的に行われる可能性があるためです。また、新しい脆弱性が公開されると、ハッキンググループはそれを迅速に悪用してゼロデイ（Zero-day）攻撃を行うため、セキュリティパッチが適用される前までは脆弱性に対する防御が難しい状況が発生する可能性があります。つまり、既存のセキュリティシステムが検知できない状態で攻撃が行われる可能性が高く、ハッキンググループがパッチ前に十分な時間を持って被害を拡散させることができる点で、大きな脅威となると考えられます。

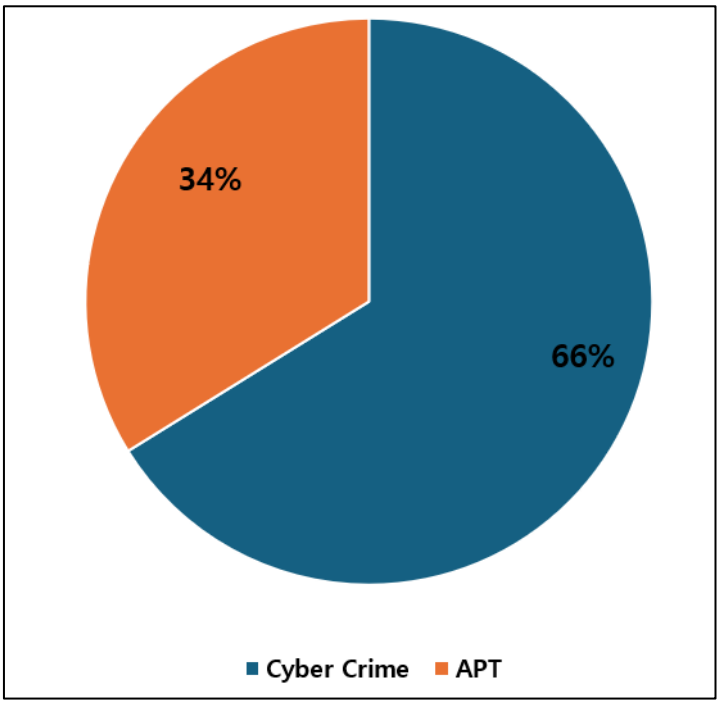
金融業界は大規模な資金取引や機密性の高い顧客情報を扱うため、たった一つの脆弱性が悪用されても、企業ネットワークへの長期的な侵入、顧客データの流出、システムの麻痺など、致命的な結果につながる可能性が高いと判断されます。

これらの点を考慮すると、脆弱性に関連する脅威イベントが全体の17%と少ない数値に見えるかもしれませんが、脆弱性の影響力と危険性は無視できないため、脆弱性に関連するデータの分析も必要です。それに基づき、脆弱性に関連する脅威イベントを分析した結果を説明したいと思います。



[図 6: 脆弱性に関連する脅威イベントの割合]

脆弱性を悪用したハッキンググループの割合を分析した結果、APTグループは34%、サイバー犯罪グループは66%であることが判明しました。つまり、サイバー犯罪グループが脆弱性を相対的により頻繁に活用している様子が明らかになり、これは彼らが大規模な拡散と金銭的利益を追求する戦略的特性と結びついています。続く内容では、金融業界を対象にAPTグループとサイバー犯罪グループが活用した脆弱性の種類と特徴を考察します。



[図 7: 脆弱性を悪用したハッキンググループの割合]

金融産業を対象としたAPTグループの攻撃では、合計22種類の脆弱性が確認され、「CVE-2017-0199（Microsoft OfficeおよびWordPadのリモートコード実行脆弱性（Remote Code Execution, RCE））」、「CVE-2017-11882（Microsoft Office Remote Code Execution, RCE）」など、過去から最近まで発表された多数の脆弱性が利用されました。ただし、特定の脆弱性に対する集中的な利用の様相は観察されませんでした。これは、攻撃者が特定の脆弱性に長期間依存するのではなく、目標環境や攻撃ベクターに応じて異なる脆弱性を選択的に利用していることを示唆しています。

脆弱性	脆弱性タイプ	脆弱性のターゲット
CVE-2017-0199	Remote Code Execution Vulnerability	Microsoft Office / WordPad
CVE-2017-11882	Remote Code Execution Vulnerability	Microsoft Office (Equation Editor)
CVE-2017-12611	Remote Code Execution Vulnerability	Apache Struts 2
CVE-2017-6742	Remote Code Execution Vulnerability	Cisco IOS and IOS XE (SNMP)
CVE-2017-9805	Remote Code Execution Vulnerability	Apache Struts 2 REST Plugin
CVE-2019-0708	Remote Code Execution Vulnerability	Microsoft Windows RDP (Remote Desktop Services)
CVE-2020-12641	SQL Injection Vulnerability	D-Link DSR-150/250/500/1000 Routers
CVE-2020-13965	SQL Injection Vulnerability	D-Link DSR-150/250/500/1000 Routers
CVE-2020-35730	Cross-Site Scripting Vulnerability	Roundcube Webmail
CVE-2021-26855	Authentication Bypass Vulnerability	Microsoft Exchange Server (ProxyLogon)
CVE-2021-38647	Remote Code Execution Vulnerability	Microsoft Open Management Infrastructure (OMI, Linux agents in Azure)
CVE-2021-44026	SQL Injection Vulnerability	Metabase (Business Intelligence Tool)
CVE-2022-30190	Remote Code Execution Vulnerability	Microsoft Windows Support Diagnostic Tool (MSDT)
CVE-2022-38028	Remote Code Execution Vulnerability	Microsoft Windows Group Policy (GpScript)
CVE-2023-23397	Privilege Escalation Vulnerability (NTLM Relay via Reminder)	Microsoft Outlook
CVE-2023-38831	Remote Code Execution Vulnerability (ZIP Archive Exploit)	WinRAR

CVE-2023-48022	Remote Code Execution Vulnerability	Webmin
CVE-2024-23692	SQL Injection Vulnerability	WordPress Plugin “LayerSlider”
CVE-2024-24919	Authentication Bypass / Information Disclosure Vulnerability	Check Point Security Gateways (VPN)
CVE-2024-43451	Remote Code Execution Vulnerability	Microsoft Word
CVE-2025-4427	SQL Injection Vulnerability	WordPress Plugin “Paid Memberships Pro”

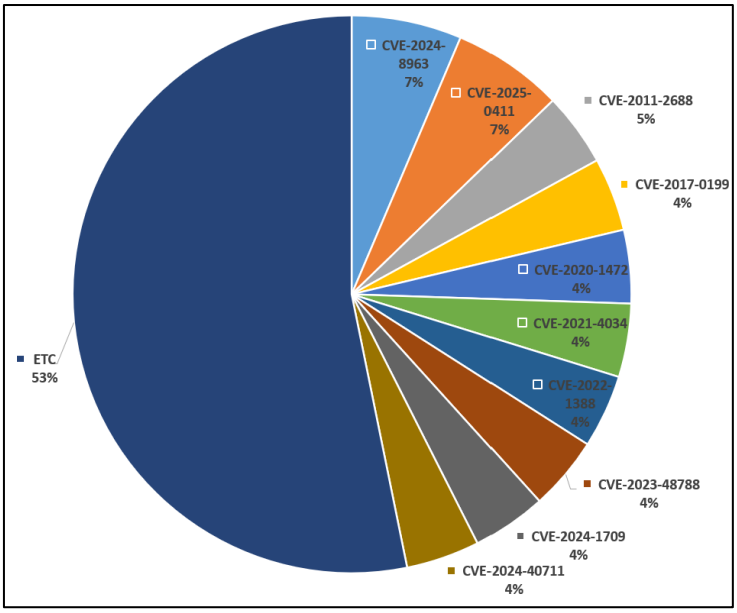
[表 1: APT グループが悪用した脆弱性の全リスト]

金融産業を対象としたサイバー犯罪グループのハッキング活動では、合計30種類の脆弱性が確認され、彼らが最も多く悪用した脆弱性を分析した結果、「CVE-2024-8963」（Ivanti Cloud Services Applianceのパストラバーサル脆弱性）と「CVE-2025-0411」（7-Zipの「Mark-of-the-Web」回避脆弱性）であると分析されている。

CVE-2024-8963は、Ivanti CSA（Cloud Services Appliance）バージョン4.6以前で発生するパストラバーサル（Path Traversal）の脆弱性であり、リモートの認証されていない攻撃者がウェブリクエストパラメータを利用してシステムの重要なファイルにアクセスしたり、制限された機能を実行したりすることができます。

一方、CVE-2025-0411はアーカイブ解凍プログラムである7-Zip（バージョン24.09以前）で発生した「Mark-of-the-Web (MotW)」保護機能の回避脆弱性であり、悪意を持って操作された圧縮ファイルでMotWが正しく伝播されないため、ユーザーがファイルを開くとユーザー権限内で任意のコードが実行可能となります。

2つの脆弱性はどちらも、リモート攻撃を通じてマルウェアペイロードの注入や任意のコード実行が可能であり、認証の回避やユーザー操作を通じてシステムの制御権を奪取できる点で高リスクに分類されます。



[図 8: サイバー犯罪グループが悪用した脆弱性]

脆弱性	脆弱性タイプ	脆弱性のターゲット
CVE-2024-8963	Path Traversal Vulnerability	Ivanti Cloud Services Appliance (CSA)
CVE-2025-0411	Protection Mechanism Failure	7-Zip
CVE-2025-29824	Use-After-Free Vulnerability	Microsoft Windows CLFS Driver
CVE-2025-24983	Use-After-Free Vulnerability	Microsoft Windows Win32k Kernel
CVE-2024-40711	Deserialization Remote Code Execution Vulnerability	Veeam Backup & Replication
CVE-2024-1709	Authentication Bypass Vulnerability	ConnectWise ScreenConnect
CVE-2023-48788	SQL Injection Vulnerability	Fortinet FortiClient EMS
CVE-2022-1388	Authentication Bypass Vulnerability	F5 BIG-IP
CVE-2021-4034	Local Privilege Escalation Vulnerability	polkit pkexec (Linux)
CVE-2020-1472	Elevation of Privilege Vulnerability	Microsoft Windows Netlogon (Domain Controller)
CVE-2011-2688	SQL Injection Vulnerability	Apache mod_authnz_external (mysql-auth.pl)
CVE-2025-24472	Authentication Bypass Vulnerability	Fortinet FortiOS / FortiProxy
CVE-2025-0108	Authentication Bypass Vulnerability	Palo Alto Networks PAN-OS (Management Web Interface)
CVE-2024-9680	Use-After-Free Vulnerability	Mozilla Firefox / Thunderbird
CVE-2024-8190	OS Command Injection Vulnerability	Ivanti Cloud Services Appliance (CSA)
CVE-2024-55591	Authentication Bypass Vulnerability	Fortinet FortiOS / FortiProxy
CVE-2024-50623	Unrestricted File Upload/Download Vulnerability	Cleo Harmony / VLTrader / LexiCom
CVE-2024-49039	Elevation of Privilege Vulnerability	Microsoft Windows Task Scheduler
CVE-2024-41713	Path Traversal Vulnerability	Mitel MiCollab (NuPoint Unified Messaging)
CVE-2024-23897	Arbitrary File Read Vulnerability	Jenkins (CLI)
CVE-2024-10914	OS Command Injection Vulnerability	D-Link NAS (DNS-320/320LW/325/340L)
CVE-2023-4473	OS Command Injection Vulnerability	Zyxel NAS (NAS326 / NAS542)
CVE-2023-36884	Remote Code Execution Vulnerability	Microsoft Office / Windows HTML
CVE-2023-3519	Remote Code Execution Vulnerability	Citrix NetScaler ADC / Gateway

CVE-2023-20269	Authentication Protection Weakness Vulnerability	Cisco ASA / Firepower Threat Defense
CVE-2021-46229	OS Command Injection Vulnerability	D-Link DI-7200GV2
CVE-2020-9054	OS Command Injection Vulnerability	Zyxel NAS / Firewall
CVE-2020-3259	Information Disclosure Vulnerability	Cisco ASA / Firepower Threat Defense
CVE-2020-24581	OS Command Execution Vulnerability	D-Link DSL-2888A
CVE-2017-0199	Remote Code Execution Vulnerability	Microsoft Office / WordPad
CVE-2024-8963	Path Traversal Vulnerability	Ivanti Cloud Services Appliance (CSA)
CVE-2025-0411	Protection Mechanism Failure (Mark-of-the-Web Bypass) Vulnerability	7-Zip
CVE-2025-29824	Use-After-Free Vulnerability	Microsoft Windows CLFS Driver
CVE-2025-24983	Use-After-Free Vulnerability	Microsoft Windows Win32k Kernel
CVE-2024-40711	Deserialization Remote Code Execution Vulnerability	Veeam Backup & Replication
CVE-2024-1709	Authentication Bypass Vulnerability	ConnectWise ScreenConnect
CVE-2023-48788	SQL Injection Vulnerability	Fortinet FortiClient EMS
CVE-2022-1388	Authentication Bypass Vulnerability	F5 BIG-IP
CVE-2021-4034	Local Privilege Escalation Vulnerability	polkit pkexec (Linux)
CVE-2020-1472	Elevation of Privilege Vulnerability	Microsoft Windows Netlogon (Domain Controller)
CVE-2011-2688	SQL Injection Vulnerability	Apache mod_authnz_external (mysql-auth.pl)

[表 2: サイバー犯罪グループが悪用した脆弱性の全リスト]

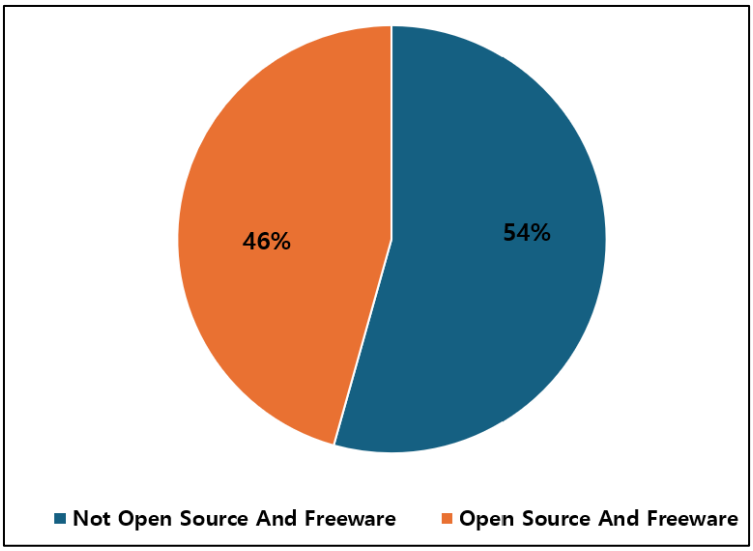
3. オープンソース（Open Source）およびフリーウェア（Freeware）

オープンソース（Open Source）およびフリーウェア（Freeware）は、ソースコードが公開されているか、無料で提供されているソフトウェアを意味し、ハッキンググループはこれを悪用して様々なマルウェア行為を行っています。

2025 年上半期に APT グループとサイバー犯罪グループが金融業界を対象に実施した攻撃事例を分析した結果、全体の 46%の攻撃事例がオープンソースおよびフリーウェアに関連していることが確認され、合計 118 のツールが悪用されたと分析されました。

これらのツールは、セキュリティソリューションによって正常なソフトウェアとして認識される可能性が高く、検出を困難にすることがあります。また、市販のハッキングツールは高額でライセンスの

制限があるためアクセスしにくく、購入過程で取引の痕跡が残るリスクがありますが、オープンソースやフリーウェアは追加の費用なしで誰でも簡単にアクセスでき、身元の露出を最小限に抑えたまま使用できるため、攻撃に利用される可能性が高いです。



[図 9: オープンソースおよびフリーウェアに関連する脅威イベントの割合]

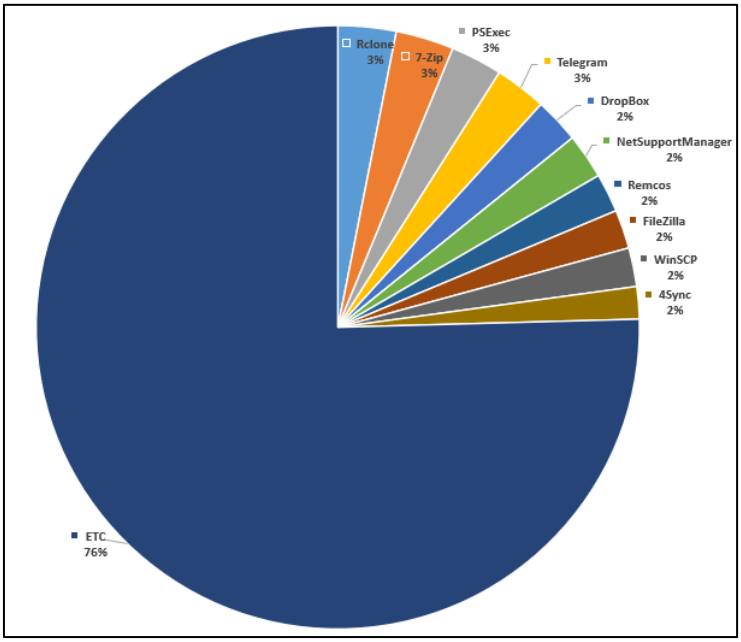
2025年上半期にAPTグループとサイバー犯罪グループが金融業界を対象に行った攻撃事例を分析した結果、Rclone、7-Zip、PsExecが頻繁に悪用されていることが確認されました。Rclone、7-Zip、PsExecはそれぞれ異なる機能を持つ合法的なユーティリティですが、共通して攻撃者の悪意ある行為を効果的に支援できる点で頻繁に悪用されています。

Rcloneはクラウドストレージ間の同期とデータ転送を自動化する目的で使用され、攻撃者はこれを利用して収集したデータを外部サーバーやクラウドストレージに目に見えない形で流出させることができます。

7-Zipは高性能な圧縮および暗号化機能を提供するツールであり、攻撃者は大量の情報を1つのファイルにまとめて暗号化し、痕跡を最小限に抑えた状態で送信するために利用します。

PsExec は、Microsoft が提供するシステム管理ツールであり、リモートコマンド実行機能を通じて、被害者の内部ネットワーク内の他のシステムへの横方向移動（Lateral Movement）や権限昇格（Privilege Escalation）に使用されます。

これらのツールはすべてマルウェアとして分類されるわけではなく、正常な運用環境でも一般的に使用されるため、セキュリティソリューションによる検出を困難にします。特に金融業界のように機密データが集中している環境では、攻撃者が侵害の事実を長期間隠蔽し、内部拠点を拡大するのに非常に有利な手段として機能する可能性があります。



[図 10: ハッキング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 Top 5]

ツール名	ツール機能
Rclone	クラウド間ファイル同期ツール
7-Zip	ファイル圧縮・解凍ユーティリティ
PsExec	リモートシステムコマンド実行ツール
Telegram	メッセージングアプリケーション
DropBox	クラウドベースのファイル保存・共有サービス
NetSupportManager	リモート制御・監視サポートソフトウェア
Remcos	リモート制御機能を備えた RAT ツール
FileZilla	FTP/SFTP クライアントプログラム
WinSCP	SFTP ベースのファイル転送クライアント
4Sync	オンラインファイルバックアップ・同期サービス

[表 3: ハッキング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 Top 5]

2025年上半期のサイバーセキュリティ侵害とインシデント

2025 年上半期に大衆メディアを通じて知られた金融産業分野の事故のうち、因果関係が確認された代表的な事例 11 件を選定し、その内容は以下の通りである。

1月の事故事例

2025 年 1 月 23 日、シンガポールに拠点を置く暗号通貨の中央化取引所 Phemex のホットウォレットが不正アクセスを受け、約 6,900 万ドル相当の暗号資産が流出しました。ETH、SOL、XRP、BTC など 16 のブロックチェーンにわたって発生し、ハッカーは迅速に資産を凍結できないトークンに変換して移動しました。当初は約 2,900 万ドルと報道されましたが、PeckShield などの分析結果により最終的に 6,900 万ドル以上と確認されました。コールドウォレットは安全であり、取引所は入出金を一時停止し、Proof of Reserves を公開し、被害を受けたユーザーに対する補償計画を発表する予定です。今回の事故はプライベートキー管理の脆弱性が主な原因と分析されています。

- **Explained: The Phemex Hack (January 2025)**
  https://www.halborn.com/blog/post/explained-the-phemex-hack-january-2025

2月の事故事例

2025 年 2 月、ByBit 暗号通貨取引所がハッキングされ、約 15 億ドル相当のデジタル資産が奪われた後、北朝鮮政権と関連があると推定されるハッキング組織ラザルスグループが、そのうち少なくとも 3 億ドルを回収不可能なアドレスに転送したと報じられました。専門家たちは、この組織が自動化ツールと熟練した人材を利用してほぼ 24 時間運営し、資金の流れを隠蔽し洗浄する精巧な構造を持っていると判断しています。ByBit は、全体の資金の約 20%が「ブラックアウト」状態で、回収の可能性が非常に低いと述べました。

- **North Korean hackers cash out hundreds of millions from $1.5bn ByBit hack**
  https://www.bbc.com/news/articles/c2kgndwwd7lo

4月の事故事例

2025 年 4 月初旬、オーストラリアの主要年金基金がクレデンシャルスタッフィング攻撃を受け、相互に関連した複数のアカウントへのログイン試行がありました。被害対象には、AustralianSuper、Rest、Hostplus、Australian Retirement Trust、Insignia などが含まれます。AustralianSuper では約 600 のアカウントが侵害され、そのうち 4 人から合計 50 万オーストラリアドル相当の年金が流出しました。Rest では約 8,000 人の会員情報が漏洩しましたが、資金の損失はありませんでした。他の基金もログイン異常を検知しましたが、金銭的な被害はありませんでした。政府と業界の規制当局が対策を講じており、ASFA は事件対応と今後のセキュリティ対応を強化するための協力体制を構築していると発表しました。

- **$500,000 stolen in Australian super fund data breach**

https://www.theguardian.com/australia-news/2025/apr/04/australian-super-funds-compromised-cybersecurity-data-breach-hack

2025 年 4 月 28 日、保険代理店(GA)プラットフォーム提供業者であるジネクソンのソリューションがハッキングされ、ハッカーがハナ損害保険の子会社であるハナ金融ファインドとユーファースト保険代理店の管理者アカウントに実際にログインした状況が確認されました。金融監督院は関連する GA システムに対して分離隔離措置および管理強化命令を出し、ダークウェブなどで少なくとも 7 つの GA 管理者アカウント情報が流出した状況も確認されました。現在、顧客情報の流出の有無を調査中であり、事実が確認された場合には顧客通知および相談センター設置などの対応も準備中です。

- **「『ハッキング攻撃』で GA プラットフォームが突破された…ハナ金融ファインド・ユーファースト管理者としてログイン」**
  https://www.etnews.com/20250428000141

5月の事故事例

仮想資産取引所 Coinbase は、2025 年 5 月 11 日にサイバー脅威者から一部の顧客アカウントデータが流出したという脅迫メールを受け取り、調査の結果、ログイン認証情報やパスワードは流出していないものの、名前・住所・メールアドレスなどが「少数の顧客グループ」に対して露出したことを確認しました。ハッカーたちは米国外にいるカスタマーサポートの一部スタッフを買収し、このような情報を奪取しましたが、Coinbase は該当スタッフを即座に解雇し、2,000 万ドルの身代金要求を拒否しました。代わりに被害を受けた顧客に補償し、犯人を摘発した場合に支払う 2,000 万ドルの報奨金を提供し、米国司法省および規制当局と協力しています。今回の事故による予想コストは 1 億 8,000 万ドルから 4 億ドルに達し、Coinbase はセキュリティ体制の強化措置を進めています。

- **Coinbase warns of up to $400 million hit from cyberattack**
  https://www.reuters.com/business/coinbase-says-cyber-criminals-stole-account-data-some-customers-2025-05-15/

2025 年 5 月 16 日未明 4 時頃、KB ライフ生命は旧型 MDM（モバイルデバイス管理）サーバーでサイバー侵害事故を把握しましたが、該当サーバーは実際には 4 月 30 日にサービスが終了している状態でした。その後、22 日午後になってこれを認識し、直ちにサーバーを隔離し、ネットワークアクセスを遮断しました。該当サーバーから在職者および一部退職者の社員番号、携帯電話番号、会社のメールアドレス、端末情報などが大量に流出したことが確認され、会社は金融セキュリティ院と共同

で精密分析および被害規模の把握を進めており、従業員には連絡先の盗用やなりすましメールに注意を促し、業務アカウントのパスワード変更を案内しました。

- **「KB ライフ生命の役職員情報が流出…MDM サーバーがサイバー攻撃を受けた」**
  https://www.thepublic.kr/news/articleView.html?idxno=264544

6月の事故事例

2025 年 6 月初旬、アメリカの税務代理業者である Optima Tax Relief が Chaos ランサムウェア組織による二重恐喝（ダブルエクストーション）攻撃を受け、内部サーバーが暗号化され、約 69GB のデータが流出したと報告されました。流出したデータには、企業情報や顧客のケースファイルが含まれており、社会保障番号（SSN）、住所、電話番号などの個人識別情報（PII）が含まれていると推定されています。

- **Chaos ransomware hits Optima Tax Relief, leaks 69GB of data**
  https://www.foxnews.com/tech/chaos-ransomware-hits-optima-tax-relief-leaks-69gb-data

2025 年 6 月 12 日、米国の保険会社 Aflac のネットワークで疑わしい活動が検出され、数時間以内に即座に遮断されました。ランサムウェアは存在せず、正常な運営が維持されました。調査の初期段階で、顧客とその家族、従業員、代理人を含む社会保障番号、保険請求情報、健康情報などの機密個人データが流出する可能性が確認されました。Aflac は迅速な対応として、24 ヶ月間の無料クレジットモニタリング・アイデンティティ保護サービスを提供し、調査を進めています。この攻撃は、保険業界を狙った巧妙なサイバー犯罪キャンペーンの一環と評価されています。

- **Aflac customer data breached by cybercriminals in latest hit on US insurance industry**
  https://nypost.com/2025/06/20/business/aflac-customer-data-breached-by-cybercriminals-in-hit-to-us-insurers/

2025 年 6 月 17 日、Gonjeshke Darande として知られるハッカーグループが、イラン国営銀行である Bank Sepah の内部データを削除したと主張しています。攻撃後、ウェブサイトや ATM などのサービスが停止し、ハッカーはこの銀行が IRGC の資金と関連していると述べました。

- **Suspected Israeli hackers claim to destroy data at Iran's Bank Sepah**

https://www.reuters.com/world/middle-east/suspected-israeli-hackers-claim-destroy-data-irans-bank-sepah-2025-06-17/

2025 年 6 月 18 日、ハッカーグループ Gonjeshke Darande（「Predatory Sparrow」）は、イラン最大の暗号通貨取引所 Nobitex のホットウォレットから約 9,000 万ドル相当の暗号資産を奪取し、アクセス不可能な「burn」アドレスに送信して事実上焼却したと主張しています。彼らは、Nobitex がイラン政府の制裁回避と IRGC 関連の資金調達に関与していたことを攻撃の動機として明らかにしました。

- **Hackers reportedly wipe out $90 million from largest Iranian cryptocurrency exchange**
  https://www.pbs.org/newshour/world/hackers-reportedly-wipe-out-90-million-from-largest-iranian-cryptocurrency-exchange

2025 年 6 月 30 日、ブラジル中央銀行と金融機関をつなぐサービスプロバイダーである C&M Software の人事担当者 João Nazareno Roque が、内部システムへのアクセス権をサイバー犯罪者に約 2,700 ドルで販売し、ハッカーが C&M システムに侵入しました。その結果、6 つの金融機関の中央銀行預金口座から約 1 億 4,000 万ドル（8 億レアル）が不正に送金されました。その後、約 3,000 万～4,000 万ドルがビットコイン、イーサ、USDT に変換され、ラテンアメリカの OTC 取引所を通じて洗浄されました。ブラジル連邦警察は Roque を逮捕し、約 2 億 7,000 万レアル（約 5,000 万ドル）相当の資産を凍結するなど、捜査が進行中です。

- **Employee arrested after Brazil's central bank service provider hacked for US $140 million**
  https://www.bitdefender.com/en-au/blog/hotforsecurity/employee-arrested-after-brazils-central-bank-service-provider-hacked-for-us-140-million

結論

NSHC 脅威分析研究所（Threat Research Lab）では、金融業界を対象とするハッキンググループの動向をより体系的に把握し、対応戦略を策定するために、ThreatRecon プラットフォームの脅威データを活用して、2025 年上半期の金融業界関連のハッキンググループの活動情報を分析しました。攻撃手法を調べると、APT グループとサイバー犯罪グループの両方が最初の侵入段階でフィッシング手法を最も多く利用していることが分析されました。フィッシング攻撃は、ユーザーの心理を巧妙

に操作してミスを誘発する方法で行われ、一度のミスでアカウントの乗っ取りや Malware 感染が発生する可能性があるため、攻撃成功率が高いのが特徴です。また、脆弱性の悪用事例を調べた結果、APT グループは特定の脆弱性を集中的に使用するのではなく、全般的に様々な脆弱性を悪用しており、サイバー犯罪グループは「CVE-2024-8963(Ivanti Cloud Services Appliance のパストラバーサル脆弱性)」と「CVE-2025-0411(7-Zip の「Mark-of-the-Web」回避脆弱性)」を主に悪用していることが分析されました。2025 年上半期の間に合計 118 のオープンソースおよびフリーウェアツールが攻撃に悪用され、その中で Rclone、7-Zip、PsExec が頻繁に利用されたことが分析されました。これは、ハッキンググループが商用ツールを利用して検出を回避し、攻撃を精巧化していることを示しています。

ハッキンググループの攻撃による被害を最小化し、効果的に対応するためには、彼らの最近の攻撃手法やツール、戦術などを綿密に分析し、それに基づいて事前予防および検知・対応体制を構築する必要があります。ハッキンググループが活用する攻撃手法とツールに関する深層的な情報を含むサイバー脅威インテリジェンス（Cyber Threat Intelligence, CTI）を確保すれば、最近の脅威動向をリアルタイムで反映し、より能動的で戦略的なセキュリティ対応が可能となります。このような CTI 情報を活用してユーザーのセキュリティ意識を強化し、フィッシング検知技術を導入する一方、多要素認証（MFA）などのセキュリティ対策を適用してアカウントの乗っ取りや内部侵入を防ぐ必要があります。また、継続的な脆弱性モニタリングと迅速なパッチ適用を通じてセキュリティ脆弱性を最小化することが必須であり、ハッキンググループが悪用するツールの特性を把握し、それを検知できるセキュリティモニタリング体制を強化しなければなりません。

本報告書の分析を通じて、金融業界が直面している主要なサイバー脅威をより明確に理解し、それに基づいて実質的なセキュリティ戦略を策定することが重要です。

Recommendation

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

1. 脆弱性保護（Exploit Protection)

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

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

2. 脆弱性のスキャニング（Vulnerability Scanning)

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

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

3. セキュリティ認識教育（User Training)

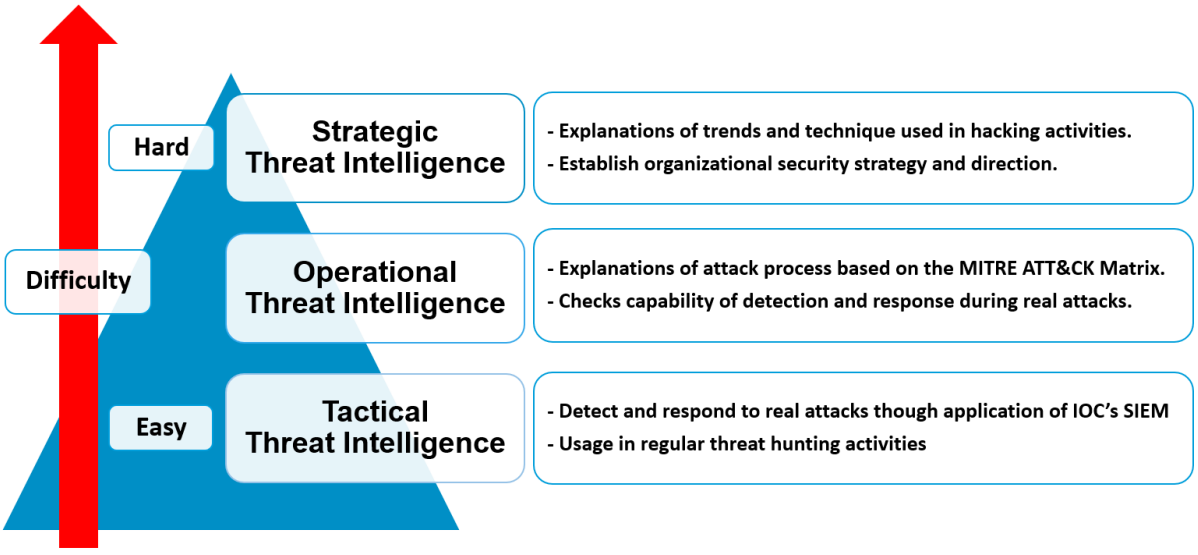
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

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

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

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

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



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

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

5. ネットワークにおける脅威緩和

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

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

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

2) ネットワーク細分化（Network Segmentation)

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

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

6. ユーザーアカウントの脅威緩和

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

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

2) アカウント使用政策 (Account Use Policies)

アカウントのセキュリティ設定に関した政策設定の検討が必要

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

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

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

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

7. エンドポイントの脅威緩和

1) ソフトウェアアップデート(Update Software)

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

2) OSの構成（Operating System Configuration)

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

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

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

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

4) 実行防止（Execution Prevention)

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

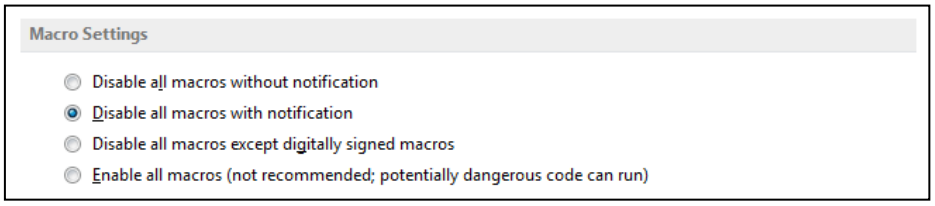
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

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

Program)

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

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



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

6) コード署名 (Code Signing)

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

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

7) アンチウイルス (Antivirus)

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

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

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

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

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

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

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

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

10) 企業モバイル政策 (Enterprise Policy)

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

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

Appendix

金融業界関係の脅威イベントリスト

TimeStamp	ThreatRecon Platform Event Name	ThreatRecon Platform
2025-01-08	Threat Actor used RansomHub Ransomware	https://cti.nshc.net/events/view/12153
2025-01-10	Threat Actor used Spear Phishing email disguised as Invoice	https://cti.nshc.net/events/view/12380
2025-01-15	Threat Actor used phishing email disguised as an Upcoming shipment arrivals	https://cti.nshc.net/events/view/12532
2025-01-16	SectorJ21 used Program Compatibility Assistant and New Domains to steal the data	https://cti.nshc.net/events/view/11830
2025-01-17	Threat Actor used IoT botnet for DDoS attacks	https://cti.nshc.net/events/view/12294
2025-01-20	Threat Actor used Android Malware disguised as SBI Reward App	https://cti.nshc.net/events/view/12994
2025-01-21	SectorU01 used ISO malware disguised as a Invitation	https://cti.nshc.net/events/view/12540
2025-01-22	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/12151
2025-01-23	SectorA07 used LNK malware disguised as a Announcement of the Civil Party Government Meeting on the Cryptocurrency Business Inspection Plan	https://cti.nshc.net/events/view/12462
2025-01-23	SectorJ196 used Infostealer Malware targeting NFTs and Crypto	https://cti.nshc.net/events/view/12447
2025-01-23	Threat Actor used Backdoor Malware disguised as a Junos Automation Script Service	https://cti.nshc.net/events/view/12221
2025-01-24	Threat Actor used Phishing email disguised as a Shipment tracking email notifications	https://cti.nshc.net/events/view/12624
2025-01-27	SectorC01 exploited Zero-Day vulnerabilities and targeted Phishing attacks to Target Ukraine	https://cti.nshc.net/events/view/12444
2025-01-28	Threat Actor used Lynx Ransomware	https://cti.nshc.net/events/view/12338
2025-01-28	Threat Actor used Malware disguised as Request for quotation	https://cti.nshc.net/events/view/12319
2025-01-28	Threat Actor used Phishing Domains to steal credentials	https://cti.nshc.net/events/view/12343
2025-01-29	Threat Actor used Malware to distribute Lockbit Ransomware	https://cti.nshc.net/events/view/12295
2025-01-31	Threat Actor used Phishing email disguised as a Payment documents	https://cti.nshc.net/events/view/12597
2025-01-31	Threat Actor used Phishing Pages to Hijack High-Profile X Accounts	https://cti.nshc.net/events/view/12463

2025-02-03	SectorM141 used VallyRAT malware with DLL side-loading technique	https://cti.nshc.net/events/view/12470
2025-02-03	Threat Actor used a new Domains for command and control	https://cti.nshc.net/events/view/12534
2025-02-04	Threat Actor exploited 7-Zip vulnerability to distribute SmokeLoader malware	https://cti.nshc.net/events/view/12469
2025-02-05	SectorA05 used LNK Malware disguised as a Whole life insurance letter	https://cti.nshc.net/events/view/12619
2025-02-05	SectorJ110 distributed Loader Malware via payment-related phishing emails	https://cti.nshc.net/events/view/12617
2025-02-05	Threat Actor used Phishing email for Crypto scam	https://cti.nshc.net/events/view/12498
2025-02-05	Threat Actor used Spear Phishing Email Attack to distribute SVG malware	https://cti.nshc.net/events/view/12628
2025-02-06	Threat Actor used a new Domains impersonating various cryptocurrency-related entities	https://cti.nshc.net/events/view/12538
2025-02-07	Threat Actor used Android Malware disguised as Bank Apps	https://cti.nshc.net/events/view/12648
2025-02-10	Threat Actor exploited Ivanti CSA vulnerability CVE-2024-8963	https://cti.nshc.net/events/view/12609
2025-02-11	SectorJ04 exploited Cleo Multiple Products Vulnerability to distribute Cl0p Ransomware	https://cti.nshc.net/events/view/12653
2025-02-12	Threat Actor used Phishing PDFs disguised as CAPTCHA on Webflow CDN	https://cti.nshc.net/events/view/12736
2025-02-13	SectorA05 used LNK files disguised as Legitimate Documents	https://cti.nshc.net/events/view/12729
2025-02-14	Threat Actor used SEO Poisoning to Redirect Indian Gov Sites	https://cti.nshc.net/events/view/12770
2025-02-18	Threat Actor used Stealer Malware disguised as Bitdefender Updater	https://cti.nshc.net/events/view/12778
2025-02-20	SectorB01 used Shadowpad Malware and Ransomware in Manufacturing Attack	https://cti.nshc.net/events/view/12800
2025-02-20	SectorJ85 used Phishing Domains and Ransomware	https://cti.nshc.net/events/view/12860
2025-02-23	SectorA01 used Python RCE disguised as Stock Simulator Tool	https://cti.nshc.net/events/view/13364
2025-02-23	SectorJ205 used new Domains for Endurance Ransomware	https://cti.nshc.net/events/view/12888
2025-02-28	SectorG01 used Bandook and Poco RAT Malware being distributed via a PDF file	https://cti.nshc.net/events/view/13156
2025-02-28	Threat Actor used SapphireRAT disguised as legal documents	https://cti.nshc.net/events/view/13029
2025-03-02	SectorA01 used JavaScript Malware	https://cti.nshc.net/events/view/13171
2025-03-03	SectorE05 used Word malware disguised as a Monetary policy report	https://cti.nshc.net/events/view/13155

2025-03-05	Threat Actor used Loader Malware Disguised as Go Libraries	https://cti.nshc.net/events/view/13137
2025-03-05	Threat Actor used new Domains and Malware for Ransomware	https://cti.nshc.net/events/view/13135
2025-03-05	Threat Actor used phishing email disguised as a Purchase order	https://cti.nshc.net/events/view/13173
2025-03-06	SectorJ203 used Malware to distribute Medusa Ransomware	https://cti.nshc.net/events/view/13176
2025-03-07	Threat Actor used Phishing email disguised as a Electronic Tax Invoice	https://cti.nshc.net/events/view/13417
2025-03-08	Threat Actor used SVG Phishing Files to Evade Office 365 Security	https://cti.nshc.net/events/view/13225
2025-03-10	SectorA01 exploited reentrancy vulnerability in Bybit's smart contract	https://cti.nshc.net/events/view/13487
2025-03-10	SectorA01 used Script Malware disguised as a Lumanagi DEX Platform source code	https://cti.nshc.net/events/view/13295
2025-03-11	SectorA01 used DNS Pivoting in Bybit Crypto Heist Investigation	https://cti.nshc.net/events/view/13352
2025-03-12	SectorB01 used ShadowPad for Data Theft in Manufacturing Sector	https://cti.nshc.net/events/view/13365
2025-03-12	SectorJ203 leveraged Vulnerabilities and open-source tools to deploy Medusa Ransomware	https://cti.nshc.net/events/view/13409
2025-03-13	SectorJ199 used PowerShell Malware to steal data	https://cti.nshc.net/events/view/13197
2025-03-13	Threat Actor used BRUTED for Credential Stuffing on Edge Devices	https://cti.nshc.net/events/view/13496
2025-03-14	Threat Actor used SocGholish Malware for RansomHub Ransomware Deployment	https://cti.nshc.net/events/view/13410
2025-03-17	Threat Actor used Malware on WordPress Sites for Web Redirects	https://cti.nshc.net/events/view/13585
2025-03-18	Threat Actor exploited Windows Shortcut File to distribute Malware	https://cti.nshc.net/events/view/13584
2025-03-19	SectorJ159 distributed RAT Malware via phishing mails	https://cti.nshc.net/events/view/13687
2025-03-20	SectorJ01 used Python Backdoor Malware	https://cti.nshc.net/events/view/13609
2025-03-24	SectorJ215 distributed Malware via fake podcasts	https://cti.nshc.net/events/view/14638
2025-03-24	Threat Actor used Android Malware disguised as Banking Apps	https://cti.nshc.net/events/view/13904
2025-03-25	SectorJ72 used new TLD Domains for C2 infrastructure	https://cti.nshc.net/events/view/13739
2025-03-25	Threat Actor used Mirai Botnet based GorillaBot for Global Cyber Attacks	https://cti.nshc.net/events/view/16543
2025-03-26	SectorB01 used SparrowDoor Backdoor Disguised via DLL Side-Loading	https://cti.nshc.net/events/view/13763

2025-03-26	SectorD01 used C# Malware disguised as PDF against Iraqi entities	https://cti.nshc.net/events/view/14006
2025-03-28	Threat Actor used ClickFix Captcha to Deliver Qakbot Malware	https://cti.nshc.net/events/view/13881
2025-03-28	Threat Actor used Grandoreiro Trojan impersonating Tax Agency in Phishing	https://cti.nshc.net/events/view/14099
2025-03-30	Threat Actor used new Domains for VanHelsing Ransomware	https://cti.nshc.net/events/view/13875
2025-03-31	SectorA01 used GolangGhost Malware disguised as job interview process	https://cti.nshc.net/events/view/13879
2025-04-01	SectorJ149 distributed Malware via phishing email	https://cti.nshc.net/events/view/13913
2025-04-01	Threat Actor used Android Malware disguised as Banking App	https://cti.nshc.net/events/view/13939
2025-04-02	Threat Actor used new Domains for Hunters International Ransomware	https://cti.nshc.net/events/view/14074
2025-04-03	Threat Actor distributed Phishing Domains via emails impersonating Coinbase Wallet migration notices	https://cti.nshc.net/events/view/14024
2025-04-08	SectorJ210 exploited CLFS vulnerability to distribute Ransomware	https://cti.nshc.net/events/view/14131
2025-04-08	SectorJ85 used Phishing Domains and RAT Malware disguised as login pages	https://cti.nshc.net/events/view/14145
2025-04-10	SectorJ220 sold Smishing Kits via Telegram	https://cti.nshc.net/events/view/14197
2025-04-10	Threat Actor used Smishing Tactics Disguised as Toll Notifications	https://cti.nshc.net/events/view/14242
2025-04-14	SectorA05 used MySpy Malware and RDPWrap for Persistent Access	https://cti.nshc.net/events/view/14425
2025-04-14	SectorB53 used BPFDoor Backdoor for Espionage on Linux Servers	https://cti.nshc.net/events/view/14369
2025-04-14	Threat Actor used Cisco Vulnerability and Tools for Akira Ransomware	https://cti.nshc.net/events/view/14582
2025-04-15	Threat Actor used Malicious PyPI Package to Hijack Crypto Credentials	https://cti.nshc.net/events/view/14375
2025-04-15	Threat Actor used Phishing Pages disguised as Employee Portals	https://cti.nshc.net/events/view/14408
2025-04-17	Threat Actor using Compromised WordPress Pages to distribute Malware	https://cti.nshc.net/events/view/14844
2025-04-22	Threat Actor used NFC Fraud Tools to Exploit Mobile Wallets Globally	https://cti.nshc.net/events/view/14607
2025-04-24	SectorA01 used Exploited Innorix Agent Vulnerability in S.Korea	https://cti.nshc.net/events/view/14641
2025-04-24	SectorA07 used LNK Malware disguised as a Proposal PDF	https://cti.nshc.net/events/view/14642

2025-04-24	Threat Actor used Backdoor Malware to steal credit card data	https://cti.nshc.net/events/view/14627
2025-04-29	Threat Actor distributed Malware via phishing emails disguised as order confirmations	https://cti.nshc.net/events/view/14982
2025-04-29	Threat Actor used Phishing Emails Disguised as Feedback Links	https://cti.nshc.net/events/view/14757
2025-04-30	SectorJ49 distributed Malware via phishing emails	https://cti.nshc.net/events/view/14944
2025-05-01	Threat Actor used Phishing disguised as IT Helpdesk Portals	https://cti.nshc.net/events/view/14795
2025-05-02	SectorJ85 used Fake Login Page to steal credentials	https://cti.nshc.net/events/view/14945
2025-05-02	Threat Actor used Android Malware disguised as ICICI Bank app	https://cti.nshc.net/events/view/14768
2025-05-06	Threat Actor used Lampion Infostealer disguised via ClickFix Lures	https://cti.nshc.net/events/view/14975
2025-05-06	Threat Actor used Phishing Domains to steal credentials	https://cti.nshc.net/events/view/15022
2025-05-06	Threat Actor used Phishing SVGs disguised as legit document files	https://cti.nshc.net/events/view/15016
2025-05-07	Threat Actor used Loader Malware for Agenda Ransomware	https://cti.nshc.net/events/view/15026
2025-05-07	Threat Actor used Nitrogen Ransomware	https://cti.nshc.net/events/view/15023
2025-05-07	Threat Actor used Phishing email disguised as a Intellectual Property Infringement Notice	https://cti.nshc.net/events/view/15893
2025-05-08	SectorA01 used OtterCookie Malware in Contagious Interview Campaign	https://cti.nshc.net/events/view/15244
2025-05-08	Threat Actor used Phishing disguised as Social Security Statements	https://cti.nshc.net/events/view/15112
2025-05-09	Threat Actor used Bitmap-Steganography to Hide Agent Tesla Malware	https://cti.nshc.net/events/view/15132
2025-05-13	SectorJ113 used Malware targeted attack against Finance sector	https://cti.nshc.net/events/view/15263
2025-05-15	Threat Actor used Phishing Sites to Target Kuwaiti Telecom Sectors	https://cti.nshc.net/events/view/15399
2025-05-16	Threat Actor used ModiLoader Malware disguised as Turkish Bank Email	https://cti.nshc.net/events/view/15378
2025-05-19	SectorM153 exploited CVE-2023-48022 for AI server breach	https://cti.nshc.net/events/view/15531
2025-05-20	SectorE04 used Word malware disguised as cybersecurity advisories	https://cti.nshc.net/events/view/15520
2025-05-20	Threat Actor used Malware disguised as Chatbot Plugin	https://cti.nshc.net/events/view/15487
2025-05-20	Threat Actor used Pure Malware disguised as RAR Email Attachments	https://cti.nshc.net/events/view/15522

2025-05-21	SectorB86 used RCE Exploit on Ivanti EPMM for Data Exfiltration	https://cti.nshc.net/events/view/15555
2025-05-21	Threat Actor distributed RMM Tools via phishing emails	https://cti.nshc.net/events/view/15695
2025-05-22	Threat Actor used ClickFix to deliver Rhadamanthys Infostealer	https://cti.nshc.net/events/view/15663
2025-05-22	Threat Actor used Lummastealer in Genesis Market Extension Attack	https://cti.nshc.net/events/view/15552
2025-05-23	SectorH03 used Ares RAT disguised as legitimate Indian domains	https://cti.nshc.net/events/view/15588
2025-05-23	Threat Actor used Phishing email disguised as a FedEx Import Tax Invoice	https://cti.nshc.net/events/view/15972
2025-05-28	Threat Actor distributed Malware via fake recruitment email	https://cti.nshc.net/events/view/15814
2025-05-28	Threat Actor used Zanubis Android Malware disguised as tax app	https://cti.nshc.net/events/view/15709
2025-05-30	Threat Actor used Phishing email disguised as a Copyright Reference Cooperation	https://cti.nshc.net/events/view/15876
2025-06-02	Threat Actor used Phishing Pages on Glitch Disguised with Fake CAPTCHAs	https://cti.nshc.net/events/view/15851
2025-06-03	SectorA01 used Fake Job Offers to Deploy OtterCookie Malware	https://cti.nshc.net/events/view/15922
2025-06-04	SectorJ231 used CHAINVERB Malware disguised as Signed Documents	https://cti.nshc.net/events/view/16048
2025-06-04	Threat Actor used Phishing email disguised as a Financial Monitoring Department Notice	https://cti.nshc.net/events/view/16080
2025-06-05	Threat Actor used Phishing email disguised as a DHL KOREA Billing Guide	https://cti.nshc.net/events/view/16103
2025-06-06	Threat Actor used distributed Malware and Lockbit Ransomware via zip file disguised as a reconciliation report	https://cti.nshc.net/events/view/15954
2025-06-09	Threat Actor used LNK Malware via transfer screenshot zip	https://cti.nshc.net/events/view/16046
2025-06-09	Threat Actor used ShadowPad Malware in Global Cyberespionage Campaign	https://cti.nshc.net/events/view/16016
2025-06-11	Threat Actor used new Domains for Black Basta Ransomware	https://cti.nshc.net/events/view/16084
2025-06-12	Threat Actor used Fog Ransomware and GC2 Tool in Asian Attack	https://cti.nshc.net/events/view/16065
2025-06-13	SectorJ01 used Phishing Domains for NetSupport RAT Delivery	https://cti.nshc.net/events/view/16097
2025-06-13	Threat Actor used Phishing email disguised as a Purchase order number	https://cti.nshc.net/events/view/16432

2025-06-16	SectorM47 exploited Microsoft Windows LNK zero-day vulnerability	https://cti.nshc.net/events/view/16417
2025-06-17	Threat Actor used RapperBot Botnet for DDoS and Extortion Activities	https://cti.nshc.net/events/view/16254
2025-06-18	Threat Actor used Tor and Docker API for XMRig Crypto Mining	https://cti.nshc.net/events/view/16245
2025-06-21	SectorA06 used Infostealer disguised as Zoom audio repair tool	https://cti.nshc.net/events/view/16360
2025-06-24	Threat Actor used Open Source Tools	https://cti.nshc.net/events/view/16523
2025-06-25	SectorS01 used WebDAV Exploit Disguised as Microsoft File Access	https://cti.nshc.net/events/view/16425
2025-06-27	SectorS01 used Phishing Disguised as Colombian Bank Login Pages	https://cti.nshc.net/events/view/16452

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.