NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI20250401

2024年度 SectorAグループの活動まとめ

Cyber Threat Intelligence

April 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。

北朝鮮政府支援のハッキンググループSectorA

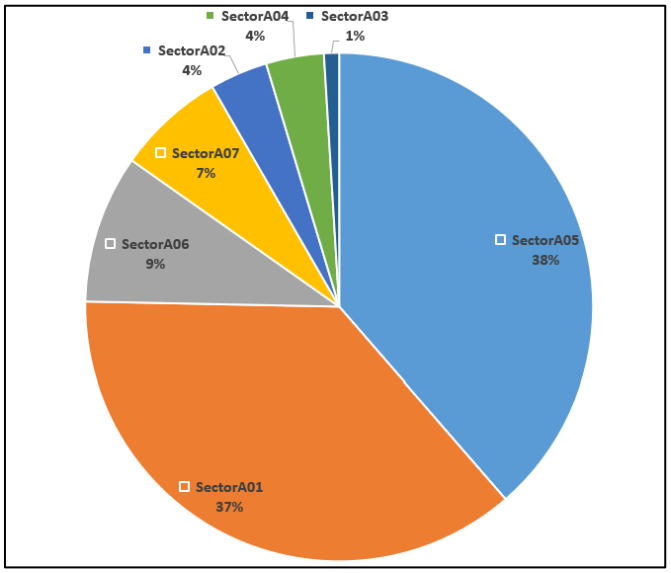
1. セクターAグループ活動

NSHC脅威分析研究所（Threat Research Lab）では、北朝鮮政府支援のハッキンググループであるSectorAグループを、合計7つのサブハッキンググループに分類しています。彼らは韓国に関連する政治、外交活動などの政府活動に関連した高度な情報を収集することを目的としており、世界中を対象にした金銭的な財の確保を目的としたハッキング活動も並行して行っています。

2024年の1年間にわたるSectorAグループの活動を分析した結果、SectorA05グループの活動が最も顕著であり、それに続いてSectorA01グループの活動が活発であることが明らかになりました。

SectorA05 グループは、他のセキュリティ企業によってキムスキ（Kimsuki）として知られるグループであり、主に韓国の政府機関、防衛、外交分野を対象にスピアフィッシングに基づく情報収集活動を活発に行っています。このグループはソーシャルエンジニアリング技術に長けており、国内の主要な問題を積極的に反映したカスタマイズされたマルウェア文書を作成し、バックドアを通じて長期間の侵入を維持する戦略を使用していると見られます。これらの活動は、北朝鮮の政策立案または外交戦略立案のための情報確保を目的としていると推測されます。

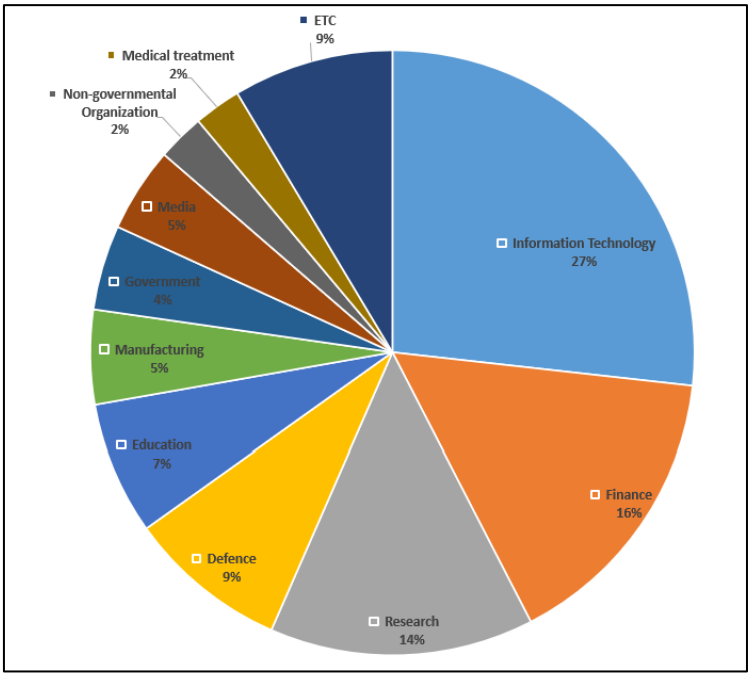
SectorA01 グループは、他のセキュリティ企業によってラザルス（Lazarus）として知られるグループであり、サイバースパイ活動と金銭的利益を目的としたサイバー犯罪を並行して行う複合的な性格の APT（Advanced Persistent Threat）グループです。彼らはサプライチェーン攻撃、ウォータリングホール技法、ゼロデイ脆弱性の悪用など高度な技術を駆使して、金融機関、仮想通貨取引所、防衛産業企業など多様な産業を対象に攻撃を行います。このグループの活動は、外貨獲得のための戦略的手段として活用されていると判断されます。



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

2. 攻撃対象産業群

SectorAグループの攻撃対象産業群を分析した結果、IT（情報技術）産業群と金融産業群を対象としたハッキング活動が最も活発に行われていることが明らかになった。
IT産業群は、ソフトウェア開発会社、セキュリティソリューション企業、クラウドサービスプロバイダーなど、デジタルインフラの核心を構成する分野であり、重要なシステムや機密の内部情報にアクセスできる技術人材を含む構造を備えています。このような特性のため、情報収集および窃取を主な目的とするSectorAグループの主要な攻撃対象となると分析されています。
また、IT企業が提供するサービスやソリューションが外部の顧客企業と広く連携しているため、侵害が発生した場合、サプライチェーンを通じた二次被害につながる可能性が高いという点で、戦略的価値が高い産業群と評価されています。
金融業界は、銀行、証券会社、仮想資産取引所など、資金の流れと密接に関連する機関で構成されており、これらに対する攻撃は直接的な外貨獲得や資金奪取の手段として利用されます。また、さまざまな外部ソリューションや第三者サービスと連携した構造的特性により、サプライチェーン攻撃の潜在的なターゲットとなる可能性も含んでいます。



[図 2: 2024 年 SectorA の攻撃対象となった産業群の統計]

3. 攻撃対象国

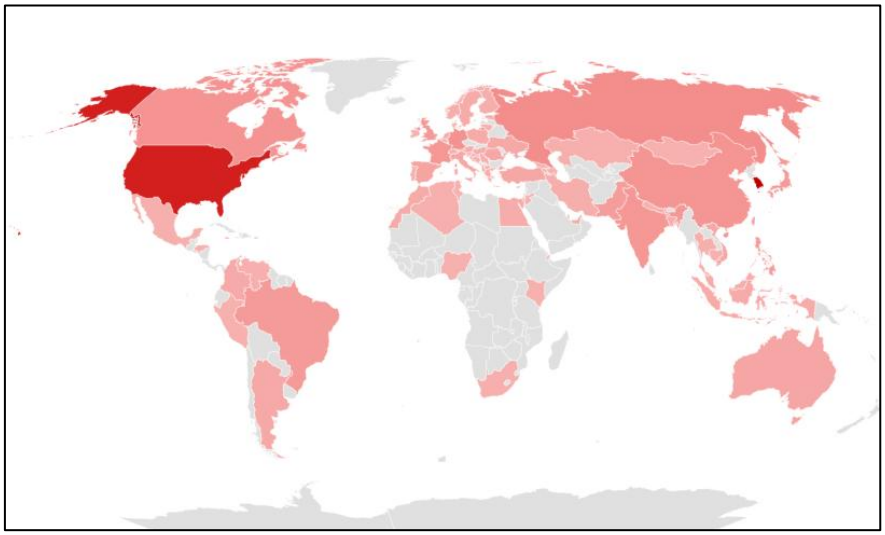
以下は、2024年におけるSectorAグループの攻撃対象国を地図上に視覚化した結果であり、赤色が濃いほど攻撃回数が多かったことを意味します。 分析の結果、SectorAグループは韓国を対象に最も多く攻撃を行い、次いでアメリカが続きました。

このような攻撃対象の選定には、相互の外交関係の特性や、該当国の保有する情報資産の重要性など、さまざまな要因が複合的に作用していると分析される。

まず、韓国はサイバー攻撃活動を行う脅威主体と地理的に近接しており、両国間には長期間にわたる軍事的緊張と監視体制が存在しています。このような安全保障環境の中で、該当グループは政治的・軍事的な利害関係に基づいて韓国を主要なサイバー攻撃の対象として設定しており、これは戦略的情報収集という目的とも密接に関連しています。特に韓国は、彼らの政策立案および戦略方向の設定に参考となる主要な情報を保有しているため、持続的なサイバーアクセスの試みが行われる可能性が高い重要な対象として認識されています。

アメリカが2番目の主要な攻撃対象となった背景には、国際社会においてその脅威主体に関連する外交・安全保障問題に継続的に関与してきた役割があると分析されている。アメリカは様々な同盟国との安全保障協力関係を維持しており、関連政策の形成過程でも継続的に影響力を発揮してきた。それに伴い、SectorAグループはアメリカ国内の政府機関およびその傘下組織が戦略的価値の高い情報資産を保有していると判断し、継続的なサイバー偵察活動を行ってきたと分析されている。

結果として、SectorAグループの攻撃対象は、該当する脅威主体の外交および軍事的関心分野と密接に関連した機関や組織に集中する傾向があります。これらの活動は主に情報収集を通じて政策立案や戦略的判断に必要な資料を確保しようとする目的に関連しており、サイバー空間が既存の情報取得手段を補完する手段として活用されていることを示しています。



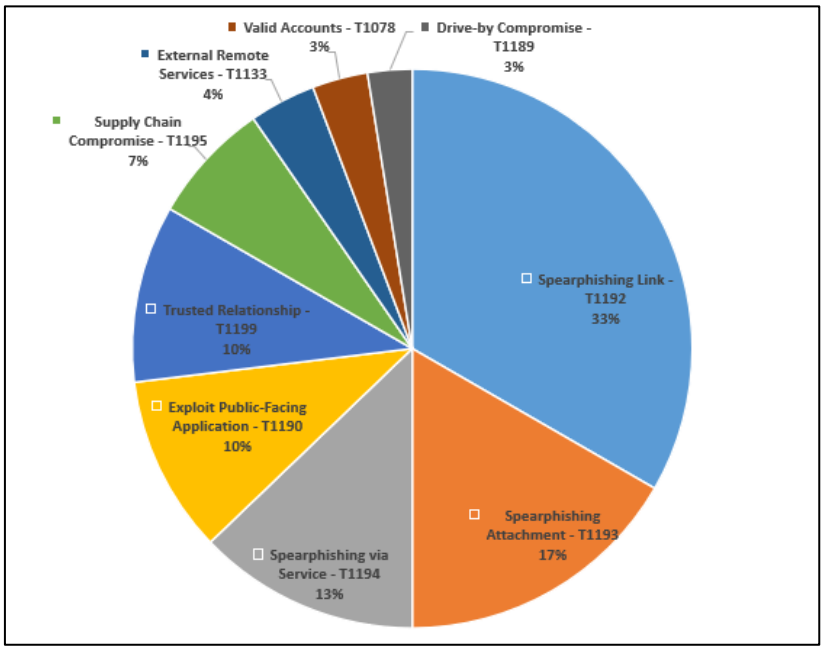
[図 3: SectorA グループの攻撃対象国]

4. 最初の侵入（Initial Access）

2024年、SectorA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、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）」、「悪性リンクを活用した戦術（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・バイア・サービス）」の3つに分類されます。SectorAグループはこの中でリンクを最も多く活用したことが示されています。このような戦術の選択は、感染成功率、柔軟な運用、検出回避を重視する戦略的特性と密接に関連していると考えられます。

技術的な側面では、リンクベースの戦術はユーザーがクリックするだけで悪性ペイロードが配信されたり、攻撃者のサーバーと接続されたりするように設計されることができ、添付ファイル方式よりも感染誘導が比較的簡単です。また、URL短縮サービスや正常なドメインの偽装を通じて静的分析およびフィルタリング検出を効果的に回避できると考えられます。
そして運用の側面でも、該当戦術はメール、メッセンジャー、コラボレーションツールなど様々なチャネルを通じて柔軟に配布が可能で、フィッシングページを通じて資格情報の窃取とMalwareの拡散を同時に行うことができ、攻撃の多機能化を実現することができる。
最後に、この戦術は1つのフィッシングドメインやインフラを複数のキャンペーンで再利用できるため、効率的なインフラ運用と長期的な侵入維持に重点を置くSectorAグループの運営方式に合致しています。



[図 4: SectorA グループ活用初回侵入統計]

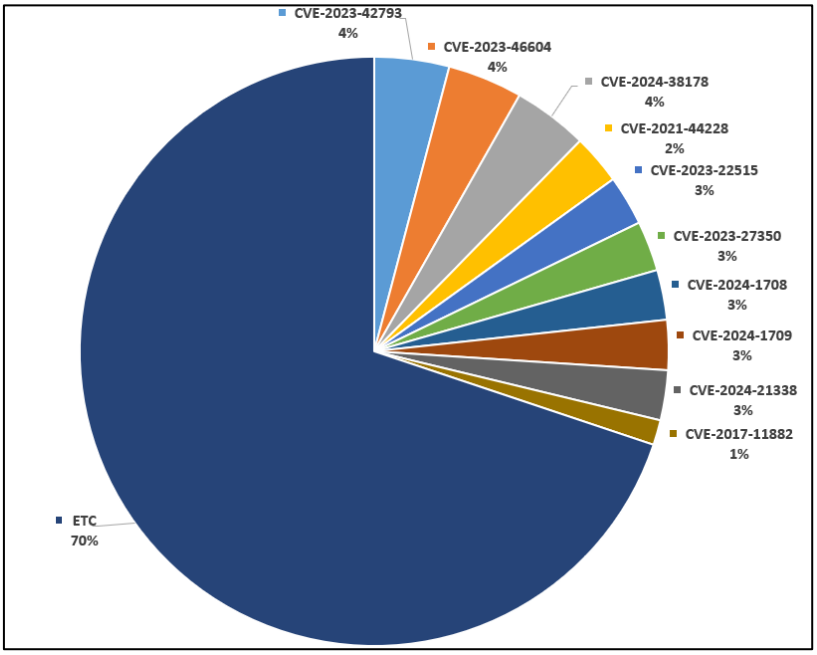
5. 脆弱性（Vulnerability）

脆弱性（Vulnerability）は、ソフトウェアやシステム内のセキュリティ上の欠陥であり、これを悪用すると機密性、完全性、可用性などに影響を与える可能性があります。2024年に確認された脆弱性の悪用事例分析の結果、SectorAグループは単一の脆弱性に依存するのではなく、状況に応じて様々な脆弱性を柔軟に活用する戦略を取っていることが明らかになりました。このような傾向は、攻撃対象の環境やシステム構成に応じて最適な侵入経路を柔軟に選択しようとする戦略的アプローチとして解釈され、単一の脆弱性に依存すると検出と防御に容易にさらされる可能性があるという点を回避しようとする目的も反映されていると考えられます。また、公開され

たPoC（Proof of Concept）コードの有無、脆弱性が存在するシステムの普及率、セキュリティパッチの適用状況など、様々な外部要因を総合的に考慮し、状況に応じて異なる脆弱性を悪用したと分析されています。この中で比較的悪用頻度が高かった主要な脆弱性は「CVE-2023-42793」、「CVE-2023-46604」、「CVE-2024-38178」であることが確認されました。

CVE-2023-42793は、JetBrains TeamCityサーバーで認証を回避し、リモートでコードを実行できる脆弱性です。また、CVE-2023-46604は、Apache ActiveMQで発生するリモートコード実行の脆弱性です。さらに、CVE-2024-38178は、Ivanti Connect SecureおよびPolicy Secureゲートウェイでリモートコマンドを実行可能な脆弱性です。

これらの3つの脆弱性はすべて、未認可の者が直接悪用でき、悪性コマンドを通じてシステム権限を奪取したり、バックドアをインストールするなど、追加の侵入を可能にする共通点を持っています。これらの特性は、APTグループ、特に偵察段階なしで迅速に初期アクセスを達成し、攻撃インフラを密かに構築しようとするSectorAグループの作戦方式に合致します。また、対象システムがセキュリティソリューションや開発インフラ（TeamCity、Ivanti、ActiveMQなど）で構成されているため、広範囲な被害の誘発および持続的な侵入基盤の確保が可能であることから、これらが該当の脆弱性を悪用したと分析されています。



[図 5: SectorA グループが悪用した脆弱性トップ 10]

脆弱性コード	脆弱性分類	脆弱性対象
CVE-2023-42793	Authentication Bypass Vulnerability	JetBrains TeamCity
CVE-2023-46604	Deserialization of Untrusted Data Vulnerability	Apache ActiveMQ
CVE-2024-38178	Scripting Engine Memory Corruption Vulnerability	Microsoft Windows
CVE-2021-44228	Remote Code Execution Vulnerability	Apache Log4j2
CVE-2023-22515	Broken Access Control Vulnerability	Atlassian Confluence Data Center and Server

CVE-2023-27350	Improper Access Control Vulnerability	PaperCut MF/NG
CVE-2024-1708	Information Disclosure Vulnerability	SAP BusinessObjects Business Intelligence Platform
CVE-2024-1709	Authentication Bypass Vulnerability	ConnectWise ScreenConnect
CVE-2024-21338	Exposed IOCTL with Insufficient Access Control Vulnerability	Microsoft Windows Kernel
CVE-2017-11882	Memory Corruption Vulnerability	Microsoft Office
CVE-2017-4946	Information Disclosure Vulnerability	VMware vSphere Data Protection
CVE-2017-5070	Type Confusion Vulnerability	Google Chrome
CVE-2019-0708	Remote Code Execution Vulnerability	Microsoft Remote Desktop Services
CVE-2019-15637	Privilege Escalation Vulnerability	OpenBSD
CVE-2019-7609	Remote Code Execution Vulnerability	Kibana
CVE-2021-20028	SQL Injection Vulnerability	SonicWall Analytics
CVE-2021-20038	Stack-Based Buffer Overflow Vulnerability	SonicWall SMA100
CVE-2021-3018	Cross-Site Scripting (XSS) Vulnerability	Fortinet FortiWeb
CVE-2021-36955	Elevation of Privilege Vulnerability	Windows Print Spooler
CVE-2021-40539	Authentication Bypass Vulnerability	Zoho ManageEngine ADSelfService Plus
CVE-2021-40684	Authentication Bypass Vulnerability	Fortinet FortiOS, FortiProxy, FortiSwitchManager
CVE-2021-41773	Path Traversal and Remote Code Execution Vulnerability	Apache HTTP Server
CVE-2021-43226	Remote Code Execution Vulnerability	Microsoft Exchange Server
CVE-2021-44142	Out-of-Bounds Heap Read/Write Vulnerability	Samba
CVE-2021-45837	Cross-Site Scripting (XSS) Vulnerability	Dolibarr ERP CRM
CVE-2022-21882	Win32k Elevation of Privilege Vulnerability	Microsoft Windows
CVE-2022-22005	Remote Code Execution Vulnerability	Microsoft Exchange Server
CVE-2022-22947	Remote Code Execution Vulnerability	VMware Spring Cloud Gateway
CVE-2022-22965	Remote Code Execution Vulnerability	VMware Spring Framework
CVE-2022-24663	SQL Injection Vulnerability	GLPI
CVE-2022-24664	Local Privilege Escalation Vulnerability	GLPI
CVE-2022-24665	Cross-Site Scripting (XSS) Vulnerability	GLPI
CVE-2022-24785	Directory Traversal Vulnerability	Composer
CVE-2022-24990	Remote Code Execution Vulnerability	Apache OFBiz
CVE-2022-25064	SQL Injection Vulnerability	GLPI
CVE-2022-27925	Remote Code Execution Vulnerability	Zimbra Collaboration Suite
CVE-2022-30190	Remote Code Execution Vulnerability	Microsoft Support Diagnostic Tool (MSDT)
CVE-2022-41352	Remote Code Execution Vulnerability	Zimbra Collaboration Suite
CVE-2022-47966	Remote Code Execution Vulnerability	ManageEngine Products
CVE-2023-0669	Remote Code Execution Vulnerability	Fortra GoAnywhere MFT
CVE-2023-21932	Remote Code Execution Vulnerability	Oracle WebLogic Server

CVE-2023-25690	HTTP Request Smuggling Vulnerability	Apache HTTP Server
CVE-2023-27997	Remote Code Execution Vulnerability	Fortinet FortiOS
CVE-2023-2868	Remote Command Execution Vulnerability	Barracuda Email Security Gateway (ESG)
CVE-2023-28771	Command Injection Vulnerability	Zyxel Firewall Devices
CVE-2023-3079	Type Confusion Vulnerability	Google Chrome
CVE-2023-32315	Authentication Bypass Vulnerability	PaperCut MF/NG
CVE-2023-32784	SQL Injection Vulnerability	GLPI
CVE-2023-33010	Remote Code Execution Vulnerability	Apache RocketMQ
CVE-2023-33246	Authentication Bypass Vulnerability	Progress MOVEit Transfer
CVE-2023-34362	SQL Injection Vulnerability	Progress MOVEit Transfer
CVE-2023-35078	Authentication Bypass Vulnerability	Ivanti Endpoint Manager
CVE-2023-3519	Remote Code Execution Vulnerability	Citrix ADC and Gateway
CVE-2023-38408	Remote Code Execution Vulnerability	OpenSSH
CVE-2023-38743	Cross-Site Scripting (XSS) Vulnerability	GLPI
CVE-2023-41892	Privilege Escalation Vulnerability	Apple macOS
CVE-2024-38106	Information Disclosure Vulnerability	Microsoft Dynamics 365
CVE-2024-4947	Remote Code Execution Vulnerability	Oracle WebLogic Server
CVE-2024-7262	Remote Code Execution Vulnerability	Adobe Acrobat Reader
CVE-2024-7263	Privilege Escalation Vulnerability	Linux Kernel
CVE-2024-7971	SQL Injection Vulnerability	Joomla CMS

[表 1: SectorA グループが悪用した脆弱性リスト]

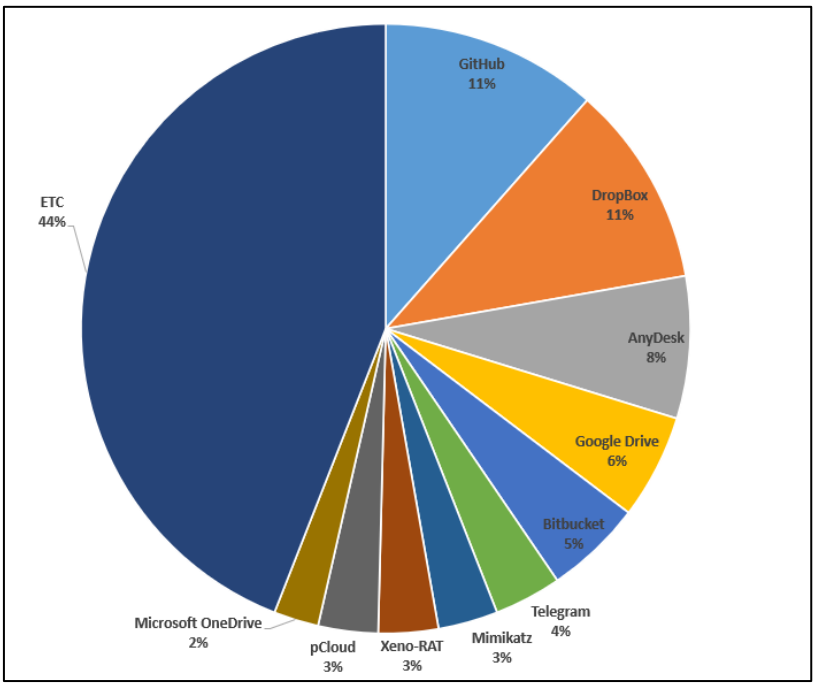
6. オープンソース（Open-Source）およびフリーウェア（Freeware）

オープンソースおよびフリーウェアは、誰でも無料で使用でき、ソースコードが公開されているため、修正および再配布が可能なソフトウェアを意味します。

オープンソースおよびフリーウェアの中で、SectorA グループは GitHub と Dropbox を最も多く悪用したと分析されています。

GitHub は、世界中の開発者がソースコードを共有し、協力できるように支援するコードリポジトリプラットフォームであり、Dropbox はユーザーがファイルを保存し、共有できるクラウドベースのファイルホスティングサービスです。

これらの 2 つのツールは、Malware をホスティングして攻撃対象が直接実行するようにしたり、C2（Command and Control）サーバーのように悪用されてペイロードを配布したり、収集したデータをアップロードする目的でも利用されることがあります。



[Figure 6: SectorA 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 Top10]

2024年 SectorA グループ活動

次は、2024年の1年間に発見されたSectorA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

1 月には、北朝鮮政府の支援を受ける SectorA グループのうち、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 SectorA01、SectorA02、SectorA05、SectorA06、SectorA07 グループです。

SectorA01 グループの活動は、スペイン、アメリカ、ドイツ、ブラジル、フランス、セルビア、バングラデシュ、トルコ、イスラエル、インド、ロシア、スイス、韓国で発見されました。該当グループは、SSH や Telnet ターミナル接続に主に使用される Putty ソフトウェアに偽装した PE（Portable Executable）形式の Malware を使用しました。

SectorA02 グループの活動はアメリカ、ルーマニア、韓国で発見されました。該当グループは統一戦略フォーラム案内文書に偽装した Windows ショートカット（LNK）形式のマルウェアを使用し、最終的に PowerShell コマンドを通じて追加のマルウェアをダウンロードし、メモリ領域で実行します。

SectorA05 グループの活動は、スロバキア、韓国、香港、中国、ロシア、トルコ、タイ、ドイツで行われています。

シンガポールで発見されました。該当グループは、個人や機関が無料で使用できる Foxit PDF リーダーのアップデートファイルに偽装した PE（Portable Executable）形式の Malware を使用しました。

SectorA06 グループの活動はコロンビアで発見されました。該当グループは、Mac OS（macOS）ユーザーを対象に、画像ファイル形式の拡張子（JPG）を使用して画像ファイルに偽装した Mach-O マルウェアを使用しました。

SectorA07 グループの活動はアメリカで発見されました。該当グループは特許料支払い確認証に偽装した Windows ヘルプ（Compiled HTML Help, CHM）ファイル形式のマルウェアを使用し、最終的に PowerShell コマンドを通じて追加のマルウェアをダウンロードおよび実行します。

2月のハッキング活動

北朝鮮政府の支援を受けている SectorA グループの中で、今回の 2 月には合計 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 SectorA01、SectorA05 グループです。

SectorA01 グループの活動はベトナム、ドイツ、アメリカで発見されました。該当グループは、オープンソースのリモート管理/リモートデスクトップソフトウェアである UltraVNC に偽装した PE（Portable Executable）形式のマルウェアを使用しました。

SectorA05 グループの活動は、ハンガリー、韓国、シンガポール、パキスタン、ドイツで発見されました。該当グループは、トレーディング講義資料に偽装した Windows ショートカット（LNK）形式の Malware を使用し、Dropbox の API を利用しました。最終的にダウンロードされた PE（Portable Executable）形式の Malware は、分散サービス拒否攻撃（Distributed Denial of Service, DDoS）、キーロギング、リモート制御機能を持ち、攻撃者サーバーの命令に従って様々な機能を実行します。

3月のハッキング活動

北朝鮮政府の支援を受けている SectorA グループの中で、今年 3 月には合計 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 SectorA01、SectorA02、SectorA05、SectorA07 グループです。

SectorA01 グループの活動は韓国、台湾、アメリカで発見されました。該当グループは公式 Python リポジトリである Python パッケージインデックス（Python Package Index, PyPI）を通じて悪意のある Python パッケージを配布しており、最終的に情報収集、リモート制御機能を持つ Malware を使用しました。

SectorA02 グループの活動は中国、韓国で発見されました。該当グループは北朝鮮人権情報センターの関係者を装ったフィッシングメールを使用し、メールに添付された圧縮ファイル内に存在するセ

キュリティコラム文書に偽装した Windows ショートカット（LNK）形式の Malware の実行を誘導しました。最終的に実行された Malware はヤンデックス（Yandex）、pCloud などのクラウドサービスを使用し、情報収集およびリモート制御機能を果たしました。
SectorA05 グループの活動は、韓国、パキスタン、アメリカ、香港、イギリス、フランス、ルーマニア、ノルウェー、ロシア、中国で発見されました。該当グループは、講義依頼書に偽装した Windows ショートカット（LNK）ファイル形式の Malware を使用し、Dropbox API を通じて追加の Malware を配布しました。
ダウンロードして最終的にオープンソースベースのリモートコントロールツールを使用しました。
SectorA07 グループの活動はロシアと韓国で発見されました。該当グループは仮想通貨取引所を装い、個人情報収集利用同意書に偽装した Windows ショートカット（LNK）形式の Malware の実行を誘導し、VBS（Visual Basic Script）ファイル形式の Malware とバッチ（Batch）スクリプト Malware を使用して情報収集およびコマンド制御に基づくさまざまな機能を実行しました。

4月のハッキング活動

北朝鮮政府の支援を受ける SectorA グループの中で、今月 4 月には合計 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 SectorA01、SectorA05、SectorA07 グループです。
SectorA01 グループの活動は、インド、バングラデシュ、シンガポール、ハンガリーで発見されました。該当グループは、採用関連の職務記述書に偽装した 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、採用に関心のある人々がそのマルウェアを実行するよう誘導しました。最終的に実行されるマルウェアの主な機能は、システム情報を送信し、レジストリ登録を通じて持続性を確保し、攻撃者が伝達する悪意のあるコードを攻撃対象システムで実行できるようにすることです。
SectorA05 グループの活動は韓国で発見されました。該当グループは会議計画書に偽装した Windows ショートカット（LNK）ファイル形式の Malware を使用し、Dropbox API を通じて追加の Malware をダウンロードして使用しました。
SectorA07 グループの活動は韓国で発見されました。該当グループは北朝鮮内部動向に関する文書に偽装した Windows ショートカット（LNK）ファイル形式の Malware を使用し、攻撃対象が Malware を実行すると、AutoIt スクリプトで作成された追加の Malware をダウンロードおよび実行して悪意のある行為を行いました。

5月のハッキング活動

北朝鮮政府の支援を受けている SectorA グループの中で、今年 5 月には合計 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 SectorA01、SectorA02、SectorA04、SectorA05、SectorA07 グループです。

SectorA01 グループの活動は、アメリカ、ポーランド、韓国、フィリピン、ブラジル、ロシア、ドイツ、ウクライナ、トルコ、ルーマニア、アゼルバイジャン、アルゼンチン、アルメニア、イギリス、日本、フランス、カナダ、イタリア、バングラデシュ、パキスタン、モロッコ、シンガポールで発見されました。該当グループは、採用担当者を装い、LinkedIn などの採用プラットフォームでソフトウェア開発者や IT エンジニア職の人材を対象に、採用インタビューやコードレビューのテストを目的として、悪意のあるスクリプトファイルを送信する攻撃活動を行いました。採用テストやソースコードレビューのテストなどのファイル名に偽装した圧縮ファイルには、感染システムの情報やキーボード入力データなどの情報を盗む悪意のある機能のマルウェアスクリプトが含まれていました。

SectorA02 グループの活動は韓国で発見されました。該当グループは訪問者出入名簿に偽装した Windows ショートカット（LNK）ファイルを活用して攻撃活動を行い、攻撃対象システムにインストールされたマルウェアを通じて C2 サーバーから受け取った命令に従い、システム情報の収集、CMD 命令の実行などの悪意のある行為を遂行しました。

SectorA04 グループの活動は韓国で発見されました。該当グループは製造業および建設業、教育機関を対象に、OpenVPN クライアントに偽装したマルウェアが含まれた圧縮ファイルを配布して攻撃活動を行い、攻撃対象システムにインストールされたマルウェアを通じて C2 サーバーから受け取った命令に従い、様々な悪意のある行為を実行しました。

SectorA05 グループの活動は、韓国、インド、スイス、アメリカ、日本で発見されました。該当グループはウェブサーバーを通じてフィッシングメールを送信し、フィッシングメールを通じて韓国のポータルウェブサイトであるネイバーのログインページに偽装したフィッシングウェブサイトに誘導し、ネイバーのメールアカウントとパスワードを盗みました。また、該当グループは同じウェブサーバーを通じてオープンソースプロジェクトで生成された Xeno RAT として知られるリモート制御 Malware を配布し、攻撃対象システムにインストールされた Xeno RAT を通じて C2 サーバーから受け取った命令に従い、様々な悪意のある行為を実行しました。

SectorA07 グループの活動は韓国で発見されました。該当グループは、召喚資料リストに偽装した Windows ショートカットファイル（LNK）を配布して攻撃活動を行い、攻撃対象システムにインストールされた AutoIt スクリプトファイルを通じて悪性行為を行いました。

6月のハッキング活動

北朝鮮政府の支援を受けている SectorA グループの中で、今回の 6 月には合計 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 SectorA01、SectorA02、SectorA05、SectorA07 グループです。

SectorA01 グループの活動は、オーストラリア、アルゼンチン、トルコ、イスラエル、フィリピン、フランス、アラブ首長国連邦、カナダ、ホンジュラス、ウクライナ、エジプト、中国、アメリカ、パキスタン、ルーマニア、ネパール、スウェーデン、キプロス、ジョージア、ブラジル、ロシア、イタリアで発見されました。該当グループは、採用担当者を装い、採用テストやソースコードレビューのテストなどのファイル名に偽装した圧縮ファイルを使用し、圧縮ファイル内の悪意のある目的のスクリプトの実行を誘導しました。

SectorA02 グループの活動は韓国で発見されました。該当グループは申請資格要件確認書に偽装したハングル（HWP）形式の Malware を使用しており、攻撃対象が文書編集のために文書内容部分をダブルクリックすると、内部に含まれたオブジェクトリンク挿入（Object Linking and Embedding, OLE）が動作し、攻撃者のサーバーに接続を試みます。

SectorA05 グループの活動は、韓国、アメリカ、ドイツ、中国で発見されました。該当グループは軍関係者に対して社会工学的アプローチを試み、攻撃対象の大学の先輩後輩を装うなど、直接的な会話を通じて信頼を得た後、メッセンジャーやメールを通じてアンケートに偽装した圧縮ファイルのダウンロードリンクを送信しました。最終的に実行される Malware は、Windows PE（Portable Executable）形式の Malware であり、攻撃者の命令に従って様々な悪意のある機能を実行します。

SectorA07 グループの活動は、エストニア、アメリカ、韓国、ドイツで発見されました。該当グループは、奨学金申請書に偽装した 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、攻撃対象がマルウェアを実行した場合、AutoIt で作成された追加のマルウェアをダウンロードおよび実行して悪意のある行為を行いました。

7月のハッキング活動

北朝鮮政府の支援を受けている SectorA グループの中で、今月 7 月には合計 4 つのハッキンググループの活動が発見されました。それらは SectorA01、SectorA04、SectorA05、SectorA07 グループです。

SectorA01 グループの活動は、フランス、パキスタン、マレーシア、台湾、スペイン、アメリカ、インド、フィリピン、韓国、ベトナム、モロッコ、ブラジル、イスラエル、ボスニア・ヘルツェゴビナで発見されました。該当グループは採用担当者に偽装し、採用テストやソースコードレビューのテストなどのファイル名に偽装した圧縮ファイルを使用し、圧縮ファイル内部の悪意のある目的のスクリプト実行を誘導しました。

SectorA04 グループの活動は韓国で発見されました。該当グループはファイル配布機能を通じてマルウェアを配布するために、企業の集中管理ソリューションを主要なターゲットとし、集中管理ソリューションの制御権を奪取するために脆弱性を悪用しました。

SectorA05 グループの活動は韓国とドイツで発見されました。該当グループは講演依頼書に偽装した Windows ショートカット（LNK）ファイル形式の Malware を使用し、Dropbox API を通じて追加の Malware をダウンロードし、ファイルレス方式で実行する方法を使用しました。
SectorA07 グループの活動は韓国で発見されました。該当グループは、付加価値税修正申告案内書に偽装した Windows ショートカット（LNK）ファイル形式の Malware を使用しており、攻撃対象が Malware 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 Malware が動作し、情報収集および追加の Malware をダウンロードおよび実行します。

8月のハッキング活動

北朝鮮政府の支援を受けている SectorA グループの中で、今月 8 月には合計 6 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 SectorA01、SectorA02、SectorA04、SectorA05、SectorA06、SectorA07 グループです。
SectorA01 グループの活動は、セルビア、インド、ベルギー、パキスタン、ジャマイカ、トルコ、シンガポール、ルーマニア、マレーシア、フィンランド、イスラエル、ロシア、カナダ、アメリカ、アルゼンチン、オーストラリア、中国、フランス、コロンビア、スロベニア、イギリス、エストニア、バングラデシュ、ベトナム、ノルウェー、インドネシア、日本、アラブ首長国連邦、香港、スペイン、クロアチア、ウクライナ、チュニジア、ブラジルで活動しています。
メキシコ、カザフスタン、イタリア、ドイツ、フィリピンで発見されました。該当グループは採用担当者を装い、採用テストやソースコードレビューのテストなどのファイル名で偽装した圧縮ファイルを使用し、圧縮ファイル内部の悪意のある目的のスクリプト実行を誘導しました。
SectorA02 グループの活動は韓国で発見されました。該当グループは、マイクロソフト ウィンドウズ（Microsoft Windows）のスクリプトエンジン（Scripting Engine）に存在する未公開の脆弱性を悪用するスクリプトのマルウェアを配布しました。
SectorA04 グループの活動は日本、アメリカ、ロシア、韓国で発見されました。該当グループは、ワクチンソフトウェア管理システムに存在する未知の脆弱性を悪用し、システムおよびネットワーク接続情報などを収集する機能を果たすマルウェアを拡散しました。
SectorA05 グループの活動は、韓国、アメリカ、中国、オーストラリア、モンゴル、イタリアで発見されました。該当グループは、国会の議事日程通知に偽装した CHM（Microsoft Compiled HTML Help）ファイル形式の Malware を使用し、最終的に正常なソフトウェアを利用した DLL サイドローディング（DLL side-loading）手法を通じて、命令制御機能を実行する DLL Malware を実行します。
SectorA06 グループの活動は、フランス、アルメニア、アメリカ、イギリスで発見されました。該当グループは、暗号通貨に関連する Mac OS（macOS）ユーザーを対象に、ビットコイン価格に関

する文書に偽装した Mach-O マルウェアを使用しました。この Mach-O マルウェアは、攻撃用サーバーから追加のマルウェアをダウンロードおよび実行する機能を持っています。
SectorA07 グループの活動は韓国、カナダで発見されました。該当グループは仮想通貨関連プロジェクトの情報更新を要求する文書に偽装した Windows ショートカット（LNK）ファイル形式の Malware を使用しており、攻撃対象が Malware 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 Malware が動作し、情報収集および追加の Malware をダウンロードおよび実行します。

9月のハッキング活動

9 月には、北朝鮮政府の支援を受ける SectorA グループの中で、合計 6 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 SectorA01、SectorA03、SectorA04、SectorA05、SectorA06、SectorA07 グループです。
SectorA01 グループの活動は、日本、オランダ、カナダ、フィリピン、アメリカ、シンガポール、ロシア、オーストラリア、ポーランド、インド、ベトナム、イギリス、フランス、エジプト、ブラジル、スウェーデン、トルコ、カタール、コロンビア、モロッコ、ベルギー、アラブ首長国連邦、中国、イラン、香港、ヨルダン、リトアニア、韓国、ドイツで発見されました。該当グループは採用担当者に偽装し、採用テストやソースコードレビューのテストなどを行っています。
ファイル名に偽装した圧縮ファイルを使用し、圧縮ファイル内部の悪意のあるスクリプトの実行を誘導しました。
SectorA03 グループの活動は香港とドイツで発見されました。該当グループは XOR アルゴリズムと Base64 アルゴリズムを通じて Malware の動作に使用される文字列を暗号化した DLL ファイル形式の Malware を使用しました。DLL ファイル形式の Malware は、合法的な Windows 写真ギャラリービューアコンポーネントである shimgvw.dll の ImageView_Fullscreen モジュールを悪用し、最終的に実行される Malware はシステム情報の収集および攻撃者が状況に応じて追加の Malware を配信および実行できる機能を持っています。
SectorA04 グループの活動はイタリアとコロンビアで発見されました。該当グループは採用担当者に偽装し、暗号化された PDF ファイルとそれを実行するように設計されたマルウェア PDF リーダーを攻撃対象に送信しました。最終的に実行されるマルウェアは、リモートコマンドの実行、ファイルのダウンロード、データの流出機能を持っています。
SectorA05 グループの活動は、アメリカ、韓国、シンガポール、インド、日本、モロッコ、カナダ、イギリスで発見されました。該当グループは、セキュリティ問題に関する非公開政策懇談会の計画書に偽装した 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、Dropbox API を通じて追加のマルウェアをダウンロードし、ファイルレス方式で実行する方法を使用しました。

SectorA06 グループの活動はオーストリアで発見されました。該当グループは、macOS ユーザーを対象に VoIP アプリケーションソフトウェアである Discord プログラムに偽装した Mach-O マルウェアを使用しました。このマルウェアは、感染したシステムにインストールされた Discord プログラムを置き換え、システムが起動するたびに自動的に実行され、最終的にリモート制御機能を実行する追加のマルウェアを生成して実行します。
SectorA07 グループの活動はアメリカ、韓国、カナダで発見されました。該当グループは、メールアカウントが休眠状態になるという内容で、ポータルサイトのカスタマーセンターから送信されたかのように偽装したスピアフィッシングメールを使用しました。

10月のハッキング活動

北朝鮮政府の支援を受けている SectorA グループの中で、今月 10 月には合計 4 つのハッキンググループの活動が発見されました。それらは SectorA01、SectorA02、SectorA05、SectorA07 グループです。
SectorA01 グループの活動は、アメリカ、アルジェリア、韓国、台湾、中国、オランダ、エジプト、ブラジルで発見されました。該当グループは GitHub に nft_marketplace-main というマルウェアプロジェクトをアップロードし、これを正常な NFT マーケットプレイスプロジェクトに偽装することで、開発者が疑いなくダウンロードするよう誘導しました。最終的に使用されたバックドアは、攻撃対象のシステムにインストールされ、データを長期的に収集する基盤を整え、攻撃者のサーバーと通信して追加の命令を実行し、収集されたデータを送信する機能を果たしました。
SectorA02 グループの活動はカンボジア、イスラエル、韓国、日本で発見されました。該当グループは初期侵入段階で「NGO Income_edit.zip」という圧縮ファイルが添付されたフィッシングメールを使用しました。最終的に使用されたマルウェアは PowerShell ベースのマルウェアであり、攻撃者の命令に従ってファイルを奪取し、レジストリを修正し、予約されたタスクを作成するなどの作業を行いました。
SectorA05 グループの活動は韓国、日本で発見されました。該当グループは、暗号通貨関連の内容の書籍に偽装した Windows ショートカット（LNK）ファイル形式の Malware を使用し、Dropbox API を通じて追加の Malware をダウンロードし、ファイルレス方式で実行する方法を使用しました。
SectorA07 グループの活動は韓国、カナダで発見されました。該当グループはプロジェクト情報確認要求書に偽装した Windows ショートカット（LNK）ファイル形式の Malware を使用しており、攻撃対象が Malware 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 Malware が動作し、情報収集および追加の Malware をダウンロードおよび実行しました。

11月のハッキング活動

北朝鮮政府の支援を受けている SectorA グループの中で、今月 11 月には合計 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 SectorA01、SectorA02、SectorA03、SectorA04、SectorA06 グループです。

SectorA01 グループの活動は、ロシア、中国、トルコ、パキスタン、インドネシア、ブラジル、フランス、ドイツ、アメリカ、インド、クロアチア、ベトナム、シンガポール、スペイン、イラン、マレーシア、イスラエル、イタリア、香港、スイス、日本、ウクライナ、韓国、カナダ、イギリスで発見されました。該当グループは企業のリモートワーク採用プロセスを悪用し、偽の身元を利用して採用された後、敏感なデータを窃取する攻撃を行いました。最終的に使用されたバックドアは、攻撃対象のシステムにインストールされ、データを長期的に収集できる基盤を整え、攻撃者のサーバーと通信して追加の命令を実行し、収集されたデータを送信する機能を果たしました。

SectorA02 グループの活動は韓国、イギリスで発見されました。該当グループは「北ロシア密着後中国政府の対北政策変化」というファイル名を持つ 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、最終的にバックドアマルウェアを使用して攻撃者の命令に従ってファイルを奪取し、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転送しました。

SectorA03 グループの活動は、イラン、ドイツ、日本、ロシアで発見されました。該当グループは、中国大使館の招待状に関連するファイルに偽装した仮想ディスクイメージ（VHDX）を使用し、最終的に使用した Malware は攻撃者の命令に従ってファイルの窃取や画面キャプチャ、追加の Malware のダウンロードおよび実行する機能を備えています。

SectorA04 グループの活動はロシアで発見されました。該当グループは、盗まれた資格情報と Windows アクセス・トークンの改ざんを通じてネットワークの掌握および権限昇格を行い、その後、Play Ransomware を使用する脅威グループと協力してランサムウェア攻撃を進行した状況が確認されました。

SectorA06 グループの活動はイギリス、アメリカで発見されました。該当グループは暗号通貨資産の奪取と機密情報の収集を目的としており、MacOS の環境設定ファイルである Zsh 環境設定ファイル（~/.zshenv）を修正して、システム再起動後もマルウェアが継続的に実行されるように設定しました。

12月のハッキング活動

12 月には、北朝鮮政府の支援を受ける SectorA グループのうち、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 SectorA01、SectorA02、SectorA05、SectorA07 グループです。

SectorA01 グループの活動は韓国で発見されました。該当グループは LinkedIn のようなプラットフォームで採用関連の職員を装い、偽の就職機会を提供する方法で潜在的な被害者に接近しました。最終的に使用されたマルウェアは、コマンド＆コントロール（C2）サーバーと通信し、追加のペイロードをダウンロードしたり、機密データを流出させるために使用されました。
SectorA02 グループの活動は韓国で発見されました。該当グループは「김국성강의자료」というファイル名を持つ Windows ショートカット（LNK）ファイル形式の Malware を使用し、最終的にバックドア Malware を使用して攻撃者の命令に従いファイルを奪取し、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転送しました。
SectorA05 グループの活動は韓国で発見されました。該当グループは、韓国のポータルウェブサイトであるネイバーのログインページに偽装したフィッシングウェブサイトに誘導し、ネイバーのメールアカウントとパスワードを盗もうとしました。
SectorA07 グループの活動はロシアと韓国で発見されました。該当グループは金融取引確認書に偽装した CHM（Compiled HTML Help）ファイル形式の Malware を使用し、最終的に PowerShell コマンドを通じて攻撃者から送信された追加のバッチスクリプト Malware をダウンロードおよび実行します。

特徴点（Adversary Tradecraft）

SectorA グループは 2024 年の前半を通じて持続的かつ多角的なハッキング活動を行い、技術的な精巧さとソーシャルエンジニアリングに基づく偽装手法の組み合わせを通じて複合的なサイバー脅威の様相を示しました。このグループは年間を通じて活動を展開し、ほぼ毎月、多数のサブグループが同時多発的に攻撃を行う構造を通じて、世界的な範囲で攻撃を拡散させました。
主要な攻撃対象国は、韓国をはじめ、アメリカ、ドイツ、フランス、インド、日本、フィリピン、ブラジルなど、アジア、ヨーロッパ、アメリカ全域にわたっています。特に韓国では、毎月繰り返し攻撃の兆候が発見されるほど、集中度の高い様相を示しました。
攻撃ベクターは明確にユーザーの相互作用に基づいて設計されており、採用職務記述書、受講資料、会議議題、政策報告書など日常的で現実感のある文書名に偽装された Malware が多数識別されました。攻撃に利用されたファイル形式も多様に現れ、Windows ショートカット（LNK）、コンパイルヘルプ（CHM）、AutoIt スクリプト、HTA（HTML アプリケーション）、VBS（Visual Basic Script）、PowerShell など、各異なる実行方式を通じてバックドア形式の Malware をインストールし、コマンド＆コントロール（C2, Command and Control）に基づくリモート制御を試みました。特に LNK ファイルを利用したスクリプトベースの Malware は頻繁に観察され、検出回避のための多段階ローディング構造またはファイルレス（Fileless）方式の実行も頻繁に利用されました。
さらに、GitHub や PyPI などの信頼に基づくプラットフォームを通じたサプライチェーン攻撃、OpenVPN や教育機関の管理ソリューションを悪用した侵入試行、Discord や Telegram などのソー

シャルプラットフォームを迂回チャネルとして活用した事例が発見されており、これは攻撃者の技術的な柔軟性と拡張性のある侵入戦略を示しています。
ほとんどのマルウェアは、システム情報、キーボード入力、ログイン資格情報などの機密情報を収集する機能を含んでおり、追加のマルウェアのダウンロードやコマンド実行などの能力を通じて、長期的な侵入および偵察に基づく脅威の持続性を確保していると分析されています。

洞察（Analyst Insights）

SectorA グループのハッキング活動は、短期的な金銭的利益を目的とした単純な侵入ではなく、戦略的な情報収集と組織内での長期的な拠点確保を目的とした精密なサイバー作戦の性格を強く持っています。
特に 2024 年の 1 年間に見せた活動の様相は、周期的、連続的、そして多様化された攻撃構造を通じて侵入対象組織の検知および対応能力を継続的に試している点で、脅威の深刻性が大きいです。ユーザーインタラクションに基づくスクリプト実行、多段階ローディングおよび回避戦略、そして実生活に似た文書名の偽装戦術は、既存の検知システムを困難にし、単純な技術的対応よりもセキュリティ意識と対応システム全般の高度化が必要な環境を作り出しています。さらに、Windows、macOS などの多様なオペレーティングシステムを対象に特化されたマルウェアを開発し、該当プラットフォームのエコシステムを考慮した偽装戦略を併行している点で、技術基盤の適応性と精密性が非常に高いと評価されます。
また、一部のサブグループはオープンソースプロジェクト、リモートワークシステム、採用プラットフォームなどの信頼に基づくエコシステムを積極的に悪用しており、その結果、サプライチェーンセキュリティの範囲が単一のソリューションに限定されず、開発者アカウントやコミュニティ運営システム全体に拡大しています。
攻撃対象はまた、技術職群、政府関連機関、軍、外交、教育など特定の職群または産業群を狙った精密打撃構造を持っており、組織別のセキュリティポリシーの細分化および役割に基づくセキュリティアプローチがさらに求められます。特に韓国は年間 12 ヶ月すべてで攻撃の状況が識別されており、ほとんどの下位グループが韓国を主要な攻撃対象に含めている点は、持続的な偵察が進行中であり、戦略的侵入の試みが長期的に計画されていることを示唆しています。
このような脅威環境に対応するためには、検出システムの自動化および高度化だけでなく、脅威インテリジェンスに基づく先制対応戦略、攻撃の戦術・技法・手順（TTP）に関する常時分析システム、そして組織内部のユーザーのセキュリティ意識の強化および対応シミュレーションシステムの整備が同時に推進される必要があります。
SectorA グループの攻撃は、技術、戦術、戦略の観点から精巧に構成された脅威であり、これに対抗するためには、従来の対応を超えた多層的かつ全方位的なサイバーセキュリティ戦略が求められます。

Recommendation

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

1. 脆弱性保護（Exploit Protection)

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

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

2. 脆弱性のスキャニング（Vulnerability Scanning)

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

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

3. セキュリティ認識教育（User Training)

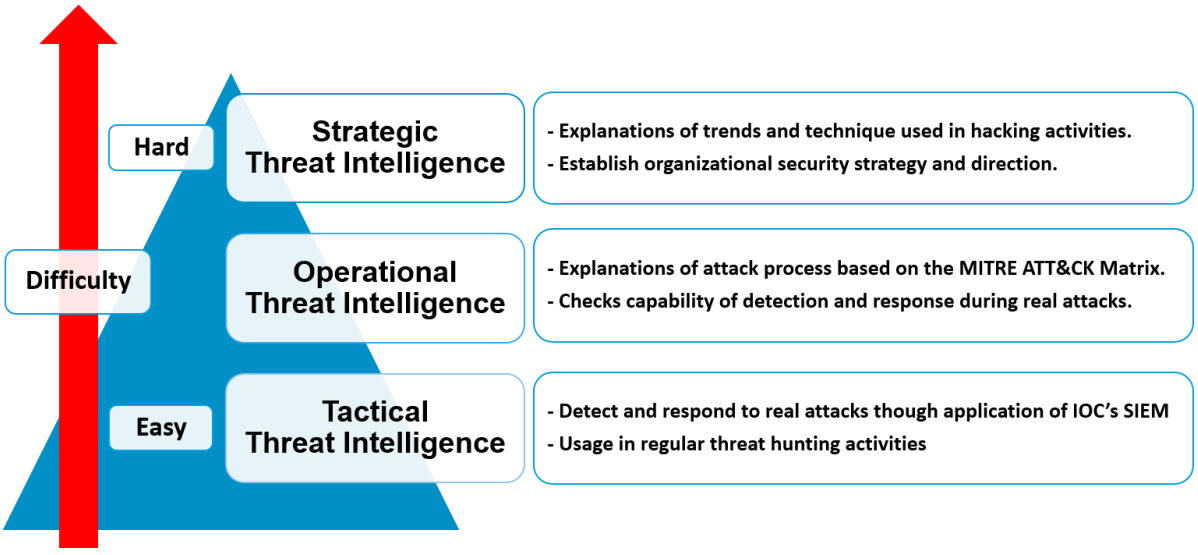
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

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

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

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

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



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

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

5. ネットワークにおける脅威緩和

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

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

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

2) ネットワーク細分化（Network Segmentation)

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

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

6. ユーザーアカウントの脅威緩和

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

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

2) アカウント使用政策 (Account Use Policies)

アカウントのセキュリティ設定に関した政策設定の検討が必要

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

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

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

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

7. エンドポイントの脅威緩和

1) ソフトウェアアップデート(Update Software)

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

2) OSの構成（Operating System Configuration)

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

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

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

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

4) 実行防止（Execution Prevention)

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

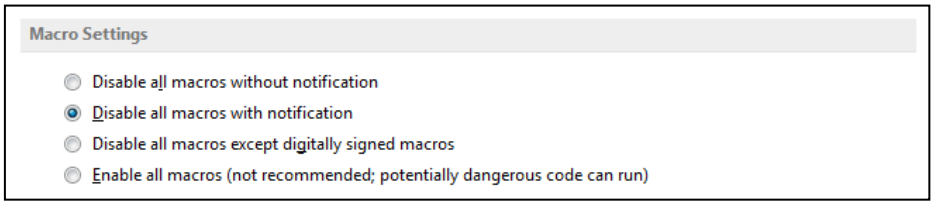
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

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

Program)

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

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



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

6) コード署名 (Code Signing)

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

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

7) アンチウイルス (Antivirus)

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

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

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

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

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

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

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

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

10) 企業モバイル政策 (Enterprise Policy)

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

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

Appendix

SectorAグループ関連の脅威イベントリスト

TimeStamp	ThreatRecon Platform Event Name	ThreatRecon Platform
2024-01-04	SectorA05 abused Remote Desktop Services	https://cti.nshc.net/events/view/6907
2024-01-04	SectorA06 used Mac Malware disguised as a JPG file	https://cti.nshc.net/events/view/6913
2024-01-10	SectorA05 used Malware disguised as a PKI software installer	https://cti.nshc.net/events/view/6926
2024-01-11	SectorA05 used Malware disguised as a Anti-Virus software file	https://cti.nshc.net/events/view/6931
2024-01-15	SectorA01 used Malware disguised as a Putty utility	https://cti.nshc.net/events/view/6956
2024-01-16	SectorA02 used LNK Malware disguised as a circular PDF	https://cti.nshc.net/events/view/6959
2024-01-17	SectorA01 used the DLL-Side Loading technique	https://cti.nshc.net/events/view/6968
2024-01-19	SectorA01 used Malware disguised as a NPM package loader modules	https://cti.nshc.net/events/view/7088
2024-01-22	SectorA02 used Malware in a targeted attack against news media experts	https://cti.nshc.net/events/view/7009
2024-01-24	SectorA05 used JSE Malware disguised as a travel expense statement	https://cti.nshc.net/events/view/7319
2024-01-25	SectorA01 used VNC Malware disguised as data from a multinational company	https://cti.nshc.net/events/view/7028
2024-01-25	SectorA05 used CHM Malware disguised as cryptocurrency key information	https://cti.nshc.net/events/view/7026
2024-01-30	SectorA05 used LNK Malware disguised as lecture materials	https://cti.nshc.net/events/view/7095
2024-02-01	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7084
2024-02-01	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7280
2024-02-02	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7318
2024-02-07	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7122
2024-02-08	SectorA01 used a new Domains	https://cti.nshc.net/events/view/7121
2024-02-08	SectorA05 used JavaScript Malware disguised as an internet shopping order statement	https://cti.nshc.net/events/view/7120
2024-02-08	SectorA05 used Malware disguised as a Internet Explorer update file	https://cti.nshc.net/events/view/7142
2024-02-14	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7150
2024-02-15	SectorA01 used Malware disguised as legitimate software	https://cti.nshc.net/events/view/7155
2024-02-15	SectorA05 used VBS Malware variants	https://cti.nshc.net/events/view/7317

2024-02-16	SectorA05 used Malware disguised as a security program required to access the website	https://cti.nshc.net/events/view/7156
2024-02-16	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7168
2024-02-19	SectorA01 used Malware disguised as AmazonVNC	https://cti.nshc.net/events/view/7193
2024-02-21	SectorA01 used PyPI to distribute malicious Python packages	https://cti.nshc.net/events/view/7174
2024-02-21	SectorA05 used open-source remote access tool (RAT) developed in C#	https://cti.nshc.net/events/view/7172
2024-02-21	SectorA07 used MSI Malware disguised as software used by the Ministry of Foreign Affairs	https://cti.nshc.net/events/view/7175
2024-02-22	SectorA02 used LNK Malware disguised as Security Column	https://cti.nshc.net/events/view/7184
2024-02-23	SectorA05 used LNK Malware disguised as a lecture request	https://cti.nshc.net/events/view/7195
2024-02-23	SectorA05 used ScreenConnect Vulnerability to distribute Cobalt Strike	https://cti.nshc.net/events/view/7605
2024-02-26	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7196
2024-02-26	SectorA05 used Malware disguised as a image file	https://cti.nshc.net/events/view/7216
2024-02-26	SectorA07 used SCR Malware variants	https://cti.nshc.net/events/view/7320
2024-02-27	SectorA05 used Phishing webpage	https://cti.nshc.net/events/view/7215
2024-02-28	SectorA01 used Social Engineering Techniques via Social Network	https://cti.nshc.net/events/view/7234
2024-02-28	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7252
2024-02-29	SectorA01 used Malware variants	https://cti.nshc.net/events/view/7246
2024-02-29	SectorA05 used PowerShell Malware variants	https://cti.nshc.net/events/view/7314
2024-02-29	SectorA05 used HWP Malware disguised as Research Proposal	https://cti.nshc.net/events/view/10011
2024-03-01	SectorA05 used BAT Malware variants	https://cti.nshc.net/events/view/7316
2024-03-03	SectorA01 used macOS Malware variants	https://cti.nshc.net/events/view/7273
2024-03-04	SectorA01 exploited Windows Kernel vulnerability	https://cti.nshc.net/events/view/7271
2024-03-04	SectorA07 used LNK Malware disguised as a Personal Information Collection and Use Agreement	https://cti.nshc.net/events/view/7303
2024-03-05	SectorA05 exploited ConnectWise ScreenConnect vulnerability	https://cti.nshc.net/events/view/7276
2024-03-06	SectorA05 used Spear Phishing email disguised as a Request to attend a Congressional Research Service meeting	https://cti.nshc.net/events/view/7290
2024-03-07	SectorA05 used LNK Malware disguised as a Trading Lesson Plans	https://cti.nshc.net/events/view/7301
2024-03-10	SectorA05 used Malware variants	https://cti.nshc.net/events/view/7312
2024-03-11	SectorA07 exploited MeshAgent remote devices tool	https://cti.nshc.net/events/view/7323

2024-03-12	SectorA05 used Spear Phishing email disguised as a request policy advisory	https://cti.nshc.net/events/view/7342
2024-03-12	SectorA07 used LNK malware disguised as a Personal Information Collection and Use Agreement	https://cti.nshc.net/events/view/7339
2024-03-14	SectorA04 used Apache ActiveMQ Vulnerability to distribute Malware	https://cti.nshc.net/events/view/7454
2024-03-14	SectorA05 used new Domains	https://cti.nshc.net/events/view/7363
2024-03-14	SectorA07 used LNK malware disguised as a Enforcement Decree of the Act on the Protection of Virtual Asset Users	https://cti.nshc.net/events/view/7354
2024-03-18	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7397
2024-03-19	SectorA01 used Malware variants	https://cti.nshc.net/events/view/7396
2024-03-19	SectorA05 used Malware disguised as a applications for Urban Railway corporations	https://cti.nshc.net/events/view/7384
2024-03-20	SectorA02 used Malware that uses Cloud storage APIs	https://cti.nshc.net/events/view/7422
2024-03-20	SectorA05 used VBS Malware variants	https://cti.nshc.net/events/view/7401
2024-03-22	SectorA05 used Xeno-RAT variants	https://cti.nshc.net/events/view/7411
2024-03-25	SectorA02 used CHM Malware disguised as a National Insurance contribution history guide	https://cti.nshc.net/events/view/7429
2024-03-25	SectorA07 used LNK malware disguised as a Personal Information Collection and Use Agreement	https://cti.nshc.net/events/view/7669
2024-03-28	SectorA01 used LNK Malware disguised as Job Description	https://cti.nshc.net/events/view/7455
2024-03-28	SectorA05 used LNK Malware disguised as a Meeting plan	https://cti.nshc.net/events/view/7464
2024-03-29	SectorA05 used Malware disguised as a VPN Operational Satisfaction Questionnaire	https://cti.nshc.net/events/view/7463
2024-04-03	SectorA01 used Python Malware extract and decrypt passwords from Web Browers	https://cti.nshc.net/events/view/7526
2024-04-05	SectorA01 used Nukesped Malware variants	https://cti.nshc.net/events/view/7547
2024-04-05	SectorA07 used LNK Malware disguised as an Internal trends and prices related to North Korea market controls	https://cti.nshc.net/events/view/7542
2024-04-05	SectorA07 used CHM malware disguised as a Payment Confirmation	https://cti.nshc.net/events/view/7563
2024-04-08	SectorA05 used Malware disguised as a Software development project document	https://cti.nshc.net/events/view/7550
2024-04-16	SectorA05 used Phishing Email with web beacons inserted	https://cti.nshc.net/events/view/7614
2024-04-16	SectorA05 used a multi-stage attack using Cloud service APIs	https://cti.nshc.net/events/view/7617

2024-04-18	SectorA01 used Malware disguised as a job offer	https://cti.nshc.net/events/view/7625
2024-04-19	SectorA01 used macOS Malware variants	https://cti.nshc.net/events/view/7633
2024-04-19	SectorA01 used macOS Malware variants	https://cti.nshc.net/events/view/7651
2024-04-19	SectorA05 used VBS Malware disguised as a Essay on Resolution of Korean Forced Labor Claims	https://cti.nshc.net/events/view/7634
2024-04-19	SectorA05 used a phishing email automation tool	https://cti.nshc.net/events/view/7648
2024-04-19	SectorA05 used LNK Malware variant	https://cti.nshc.net/events/view/8296
2024-04-20	SectorA04 used Word Malware disguised as a Seafood fairs	https://cti.nshc.net/events/view/7650
2024-04-22	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7661
2024-04-22	SectorA05 used HTA Malware variants	https://cti.nshc.net/events/view/7663
2024-04-22	SectorA06 used MacOS malware disguised as PDF Viewer	https://cti.nshc.net/events/view/7662
2024-04-23	SectorA01 used Script Malware disguised as a job interview	https://cti.nshc.net/events/view/7664
2024-04-23	SectorA01 used Python Malware to distribute RAT	https://cti.nshc.net/events/view/7696
2024-04-23	SectorA02 used LNK Malware disguised as visitor access roster	https://cti.nshc.net/events/view/7586
2024-04-23	SectorA05 used Phishing webpage disguised as Naver login webpage	https://cti.nshc.net/events/view/7657
2024-04-23	SectorA05 used Malware to hijack Anti-Virus updates to distribute CoinMiner	https://cti.nshc.net/events/view/7671
2024-04-24	SectorA01 used a new Domains	https://cti.nshc.net/events/view/7678
2024-04-24	SectorA01 used Script Malware disguised as a casino template source code	https://cti.nshc.net/events/view/7680
2024-04-24	SectorA01 used Script Malware disguised as a Cryptoweb source code	https://cti.nshc.net/events/view/7685
2024-04-24	SectorA07 used LNK Malware disguised as a source of funds statement	https://cti.nshc.net/events/view/7697
2024-04-25	SectorA01 used a malicious NPM package to target software developers	https://cti.nshc.net/events/view/7716
2024-04-25	SectorA06 used Malware variants	https://cti.nshc.net/events/view/7690
2024-04-26	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7702
2024-04-26	SectorA05 used a new Domains	https://cti.nshc.net/events/view/7710
2024-04-29	SectorA01 used Script Malware disguised as a Blockchain Game source code	https://cti.nshc.net/events/view/7713
2024-04-30	SectorA01 used Script Malware variants	https://cti.nshc.net/events/view/8035
2024-05-01	SectorA05 used a new Domains	https://cti.nshc.net/events/view/8283
2024-05-02	SectorA05 used a new Domains	https://cti.nshc.net/events/view/8033
2024-05-03	SectorA05 used LNK Malware disguised as a Planning for the Congressional Research Service Policy Roundtable	https://cti.nshc.net/events/view/8073
2024-05-06	SectorA01 used Script Malware disguised as a Blockchain project source code	https://cti.nshc.net/events/view/8067

2024-05-07	SectorA01 used a new Domains	https://cti.nshc.net/events/view/8074
2024-05-07	SectorA07 used MSI Malware disguised as a Property Duty Certificate Preparation Software	https://cti.nshc.net/events/view/8075
2024-05-08	SectorA01 used JavaScript-based Stealer Malware	https://cti.nshc.net/events/view/8076
2024-05-08	SectorA01 used Script Malware disguised as a Product source code	https://cti.nshc.net/events/view/8082
2024-05-09	SectorA01 used Script Malware disguised as an Online Game source code	https://cti.nshc.net/events/view/8085
2024-05-09	SectorA05 used Malware disguised as a AutoUpdate file	https://cti.nshc.net/events/view/8080
2024-05-10	SectorA01 used Script Malware disguised as a Poker game source code	https://cti.nshc.net/events/view/8098
2024-05-10	SectorA01 used Script Malware disguised as Play to Earn game	https://cti.nshc.net/events/view/8101
2024-05-10	SectorA05 used Social Engineering Techniques to deliver Malware	https://cti.nshc.net/events/view/8083
2024-05-11	SectorA01 used a new Domains	https://cti.nshc.net/events/view/8112
2024-05-11	SectorA06 used Malware variants	https://cti.nshc.net/events/view/8097
2024-05-12	SectorA05 used Script malware disguised as a Interview document	https://cti.nshc.net/events/view/8099
2024-05-13	SectorA01 used Script Malware disguised as a Cryptocurrency project source code	https://cti.nshc.net/events/view/8114
2024-05-13	SectorA01 used Script Malware targeted attack against Software developers	https://cti.nshc.net/events/view/8124
2024-05-13	SectorA05 used Word Malware disguised as a Resume	https://cti.nshc.net/events/view/8115
2024-05-13	SectorA05 used a web server to distribute malware and send phishing emails	https://cti.nshc.net/events/view/8145
2024-05-13	SectorA06 used Malware variants	https://cti.nshc.net/events/view/8107
2024-05-14	SectorA05 used a Phishing Email disguised as an invitation to lunch with the Deputy Minister of Foreign Affairs	https://cti.nshc.net/events/view/8144
2024-05-14	SectorA06 used Malware variants	https://cti.nshc.net/events/view/8122
2024-05-16	SectorA01 used Script Malware disguised as a Cryptocurrency project source code	https://cti.nshc.net/events/view/8146
2024-05-16	SectorA04 used Malware disguised as a VPN Client	https://cti.nshc.net/events/view/8135
2024-05-16	SectorA05 used GNUBOARD Vulnerability to build a phishing email server	https://cti.nshc.net/events/view/8142
2024-05-16	SectorA05 used Malware disguised as Windows Defender	https://cti.nshc.net/events/view/8134
2024-05-16	SectorA06 used Malware variants	https://cti.nshc.net/events/view/8143
2024-05-16	SectorA07 used LNK Malware variants	https://cti.nshc.net/events/view/8159
2024-05-16	SectorA07 used LNK Malware variants	https://cti.nshc.net/events/view/8238

2024-05-17	SectorA05 used Malware disguised as a Defense Industries job position description	https://cti.nshc.net/events/view/8171
2024-05-17	SectorA07 used LNK malware disguised as a Guidance for amended VAT returns	https://cti.nshc.net/events/view/8163
2024-05-17	SectorA07 used LNK malware disguised as a Guide to amended VAT returns	https://cti.nshc.net/events/view/8346
2024-05-19	SectorA05 used Malware variants	https://cti.nshc.net/events/view/8165
2024-05-20	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/8182
2024-05-20	SectorA05 used Phishing domains disguised as Enterprise company	https://cti.nshc.net/events/view/8166
2024-05-21	SectorA01 used Malware variants	https://cti.nshc.net/events/view/8177
2024-05-21	SectorA01 used Script Malware disguised as a Web server source code	https://cti.nshc.net/events/view/8183
2024-05-21	SectorA01 used Malware variants	https://cti.nshc.net/events/view/8189
2024-05-21	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/8191
2024-05-21	SectorA01 used JavaScript Malware variants	https://cti.nshc.net/events/view/8192
2024-05-21	SectorA07 used Malware disguised as a Excel	https://cti.nshc.net/events/view/8200
2024-05-22	SectorA01 used Script Malware disguised as a Blockchain Engine Source Code	https://cti.nshc.net/events/view/8199
2024-05-22	SectorA01 used Cryptocurrencies wallet addresses	https://cti.nshc.net/events/view/8226
2024-05-22	SectorA07 used LNK malware disguised as a Cryptocurrency Circulation Documentation	https://cti.nshc.net/events/view/8201
2024-05-23	SectorA05 used Malware disguised as a Defense Industries job position description	https://cti.nshc.net/events/view/8228
2024-05-23	SectorA05 used LNK Malware disguised as a police notices	https://cti.nshc.net/events/view/8210
2024-05-24	SectorA01 used Script Malware disguised as a Cryptocurrency node source code	https://cti.nshc.net/events/view/8229
2024-05-24	SectorA02 used ROKRAT variant	https://cti.nshc.net/events/view/8227
2024-05-24	SectorA02 used HWP Malware disguised as a Research Grant Eligibility Verification Form	https://cti.nshc.net/events/view/8250
2024-05-25	SectorA01 used macOS Malware variant	https://cti.nshc.net/events/view/8230
2024-05-27	SectorA05 used Phishing email disguised as a Important notifications about personal data breaches	https://cti.nshc.net/events/view/8225
2024-05-27	SectorA05 used RAT Malware variants	https://cti.nshc.net/events/view/8235
2024-05-27	SectorA05 used Malware variants	https://cti.nshc.net/events/view/8245
2024-05-27	SectorA05 used Android malware variant	https://cti.nshc.net/events/view/8246
2024-05-27	SectorA05 used Malware that runs in memory	https://cti.nshc.net/events/view/8240
2024-05-27	SectorA05 used Malware that utilizes the ADS(Alternate Data Stream) area	https://cti.nshc.net/events/view/8241
2024-05-28	SectorA01 used Script Malware disguised as a test project source code	https://cti.nshc.net/events/view/8247

2024-05-28	SectorA01 used Malware disguised as a Tank game	https://cti.nshc.net/events/view/8242
2024-05-28	SectorA05 used a Phishing Page disguised as a portal site to steal accounts	https://cti.nshc.net/events/view/8257
2024-05-29	SectorA01 used Script Malware variants	https://cti.nshc.net/events/view/8259
2024-05-29	SectorA05 used Microsoft Office vulnerabilities to distribute keylogger malware	https://cti.nshc.net/events/view/8258
2024-05-30	SectorA01 used Script Malware disguised as a Crypto Trading Platform source code	https://cti.nshc.net/events/view/8269
2024-05-30	SectorA01 used Script Malware disguised as a cryptocurrency tracking and investment platform source code	https://cti.nshc.net/events/view/8285
2024-05-30	SectorA01 used an open source remote management tool to steal data	https://cti.nshc.net/events/view/8274
2024-05-30	SectorA05 exploited Data Loss Prevention software	https://cti.nshc.net/events/view/8256
2024-05-30	SectorA05 used Script Malware disguised as a Reuters Interview documents	https://cti.nshc.net/events/view/8267
2024-05-31	SectorA01 used Script Malware disguised as a Centralized cryptocurrency exchanges source code	https://cti.nshc.net/events/view/8289
2024-05-31	SectorA01 used Python Malware disguised as a beautifultext Library for Python 3	https://cti.nshc.net/events/view/8290
2024-05-31	SectorA07 used MSI Malware disguised as a statistical software	https://cti.nshc.net/events/view/8314
2024-06-01	SectorA05 used Malware variants	https://cti.nshc.net/events/view/8288
2024-06-02	SectorA05 used Word Malware disguised as a Request for advice	https://cti.nshc.net/events/view/8295
2024-06-03	SectorA05 used Malware disguised as Job Description	https://cti.nshc.net/events/view/8293
2024-06-03	SectorA05 used Phishing webpage disguised as Naver login webpage	https://cti.nshc.net/events/view/8287
2024-06-03	SectorA07 used LNK Malware disguised as a scholarship application	https://cti.nshc.net/events/view/8292
2024-06-04	SectorA05 used Word Malware disguised as a Request for advice	https://cti.nshc.net/events/view/8306
2024-06-05	SectorA05 used LNK Malware disguised as a lecture request	https://cti.nshc.net/events/view/8310
2024-06-05	SectorA05 used Spear Phishing email disguised as a Written interview requests on the topic of peace on the Korean Peninsula	https://cti.nshc.net/events/view/8308
2024-06-05	SectorA05 used Phishing webpage disguised as a Important notifications about privacy incidents	https://cti.nshc.net/events/view/8326
2024-06-06	SectorA05 used Script Malware variant	https://cti.nshc.net/events/view/8341

2024-06-06	SectorA07 used LNK Malware disguised as a North Korean Human Rights NGO Strategic Activities Support Application	https://cti.nshc.net/events/view/8323
2024-06-07	SectorA01 used Script Malware disguised as a sports platform source code	https://cti.nshc.net/events/view/8340
2024-06-07	SectorA05 used Script Malware disguised as a document describing a job position within General Dynamics	https://cti.nshc.net/events/view/8337
2024-06-07	SectorA05 used PowerShell malwares	https://cti.nshc.net/events/view/8339
2024-06-07	SectorA05 used Malware variants	https://cti.nshc.net/events/view/8332
2024-06-09	SectorA05 used Script Malware disguised as a Stress Questionnaire	https://cti.nshc.net/events/view/8335
2024-06-10	SectorA01 used Malware disguised as a SumatraPDF software	https://cti.nshc.net/events/view/8342
2024-06-11	SectorA05 used Phishing webpage disguised as Naver login webpage	https://cti.nshc.net/events/view/8343
2024-06-11	SectorA05 used new Domains	https://cti.nshc.net/events/view/8371
2024-06-11	SectorA05 used Script Malware disguised as a Questionnaires	https://cti.nshc.net/events/view/8374
2024-06-12	SectorA01 used Script Malware disguised as a blockchain technology source code	https://cti.nshc.net/events/view/8380
2024-06-12	SectorA01 used Malware variants	https://cti.nshc.net/events/view/8379
2024-06-13	SectorA01 used Script Malware disguised as a test source code	https://cti.nshc.net/events/view/8397
2024-06-13	SectorA01 used Python Malware extract passwords from Web Browers	https://cti.nshc.net/events/view/8398
2024-06-13	SectorA01 used Phishing attack disguised as a job opportunity	https://cti.nshc.net/events/view/8400
2024-06-14	SectorA05 used Script Malware variants	https://cti.nshc.net/events/view/8409
2024-06-16	SectorA01 used Malware variants	https://cti.nshc.net/events/view/8408
2024-06-17	SectorA05 used Script Malware disguised as a Questionnaire	https://cti.nshc.net/events/view/8406
2024-06-18	SectorA07 used LNK malware disguised as a Guide to amended VAT returns	https://cti.nshc.net/events/view/8410
2024-06-19	SectorA05 used Malware disguised as a Defense Industries job position description	https://cti.nshc.net/events/view/8447
2024-06-20	SectorA01 used Malware variants	https://cti.nshc.net/events/view/8432
2024-06-20	SectorA02 used Ruby Malware variants	https://cti.nshc.net/events/view/8437
2024-06-20	SectorA05 used Malware variants	https://cti.nshc.net/events/view/8433
2024-06-20	SectorA06 used MacOS malware disguised as Internal PDF Viewer app	https://cti.nshc.net/events/view/8434
2024-06-21	SectorA01 used Malware variants	https://cti.nshc.net/events/view/8440
2024-06-21	SectorA04 exploits Centralized Management solutions vulnerabilities	https://cti.nshc.net/events/view/8438

2024-06-21	SectorA05 used Phishing email disguised as a Discuss the security situation in South Korea and the North Korean nuclear threat	https://cti.nshc.net/events/view/8436
2024-06-21	SectorA05 used Malware disguised as a Auto update file	https://cti.nshc.net/events/view/8465
2024-06-22	SectorA05 used Android malware variants	https://cti.nshc.net/events/view/8464
2024-06-23	SectorA05 used Malware variants	https://cti.nshc.net/events/view/8466
2024-06-24	SectorA01 used Script Malware variants	https://cti.nshc.net/events/view/8467
2024-06-24	SectorA04 exploited ERP(Enterprise Resource Planning) Software to distribute Malwares	https://cti.nshc.net/events/view/8446
2024-06-26	SectorA05 used Script Malware disguised as a Review Report	https://cti.nshc.net/events/view/8482
2024-06-26	SectorA05 used Backdoor Malware variants	https://cti.nshc.net/events/view/8477
2024-06-27	SectorA05 exploited Google Chrome extension	https://cti.nshc.net/events/view/8486
2024-06-27	SectorA07 used LNK malware disguised as a Guide to amended VAT returns	https://cti.nshc.net/events/view/8488
2024-06-28	SectorA01 poses as recruiter to distribute Python malware	https://cti.nshc.net/events/view/8495
2024-06-28	SectorA01 used Malware disguised as a AutoMapper library	https://cti.nshc.net/events/view/8511
2024-06-28	SectorA07 used a new Domains	https://cti.nshc.net/events/view/8512
2024-06-28	SectorA07 used a new Domains	https://cti.nshc.net/events/view/8531
2024-07-01	SectorA01 used Script Malware disguised as a Cryptocurrency project source code	https://cti.nshc.net/events/view/8500
2024-07-02	SectorA01 used Malware variants	https://cti.nshc.net/events/view/8504
2024-07-02	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/8507
2024-07-02	SectorA01 used Script Malware disguised as a Chess game source code	https://cti.nshc.net/events/view/8540
2024-07-02	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/8541
2024-07-02	SectorA04 used TigerRAT Malware variant	https://cti.nshc.net/events/view/8501
2024-07-02	SectorA05 used a new Domains	https://cti.nshc.net/events/view/8502
2024-07-02	SectorA05 used Malware variants	https://cti.nshc.net/events/view/8503
2024-07-02	SectorA05 used PowerShell malwares variants	https://cti.nshc.net/events/view/8542
2024-07-03	SectorA01 used Malware disguised as a Task Scheduler Service library	https://cti.nshc.net/events/view/8522
2024-07-04	SectorA05 used LNK Malware variants	https://cti.nshc.net/events/view/8550
2024-07-05	SectorA01 used Script Malware disguised as a Web application source code	https://cti.nshc.net/events/view/8563
2024-07-05	SectorA01 used PyPI to distribute malicious Python packages	https://cti.nshc.net/events/view/8551
2024-07-05	SectorA01 used Malware disguised as a AmazonVNC Viewer software	https://cti.nshc.net/events/view/8565
2024-07-05	SectorA06 used Malware disguised as a PDF Viewer software	https://cti.nshc.net/events/view/8564

2024-07-08	SectorA01 used the NPM Packages to distribute Malware	https://cti.nshc.net/events/view/8596
2024-07-08	SectorA05 used Phishing email disguised as a Request an interview	https://cti.nshc.net/events/view/8538
2024-07-10	SectorA05 used Malware variants	https://cti.nshc.net/events/view/8574
2024-07-11	SectorA01 used Malware targeted attack against Government agency in South Korea	https://cti.nshc.net/events/view/8571
2024-07-12	SectorA05 used PowerShell Malware variants	https://cti.nshc.net/events/view/8614
2024-07-14	SectorA01 used Malware disguised as Proper Console Snap software	https://cti.nshc.net/events/view/8632
2024-07-15	SectorA01 used a new Domains	https://cti.nshc.net/events/view/8619
2024-07-15	SectorA01 used macOS Malware disguised as a MiroTalk video calling service	https://cti.nshc.net/events/view/8618
2024-07-15	SectorA01 used Malware variant	https://cti.nshc.net/events/view/8663
2024-07-15	SectorA05 used LNK Malware disguised as a Speaker Request Form	https://cti.nshc.net/events/view/8633
2024-07-16	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/8667
2024-07-16	SectorA05 used Word Malware disguised as a Speaker Request Form	https://cti.nshc.net/events/view/8664
2024-07-16	SectorA07 used a new Domains	https://cti.nshc.net/events/view/8634
2024-07-17	SectorA01 used Script Malware disguised as a NFT Marketplace Template	https://cti.nshc.net/events/view/8668
2024-07-17	SectorA05 exploited GitHub Repository service	https://cti.nshc.net/events/view/8627
2024-07-17	SectorA05 used LNK Malware disguised as a job application form	https://cti.nshc.net/events/view/8628
2024-07-17	SectorA05 used Word Malware disguised as a Advisory request form	https://cti.nshc.net/events/view/8650
2024-07-18	SectorA07 used LNK Malware disguised as a List of chat software	https://cti.nshc.net/events/view/8639
2024-07-19	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/8726
2024-07-20	SectorA01 used DLL Malware variant	https://cti.nshc.net/events/view/8731
2024-07-22	SectorA01 used Script Malware disguised as a Defi Exchange Test source code	https://cti.nshc.net/events/view/8715
2024-07-22	SectorA05 used Phishing webpage disguised as a Universities webpages	https://cti.nshc.net/events/view/8671
2024-07-22	SectorA05 used Android malware variants	https://cti.nshc.net/events/view/8729
2024-07-22	SectorA07 used LNK malware disguised as a Requests from financial authorities to verify project information	https://cti.nshc.net/events/view/8674
2024-07-24	SectorA01 used a new Domains	https://cti.nshc.net/events/view/8678
2024-07-24	SectorA05 used Script Malware variants	https://cti.nshc.net/events/view/8686
2024-07-24	SectorA05 used new Domains	https://cti.nshc.net/events/view/8691
2024-07-24	SectorA05 used PowerShell malwares	https://cti.nshc.net/events/view/8842

2024-07-24	SectorA07 used Spear Phishing email disguised as a Request to verify project information	https://cti.nshc.net/events/view/8831
2024-07-25	SectorA01 used the NPM Packages to distribute Malware	https://cti.nshc.net/events/view/8793
2024-07-25	SectorA05 used a new Domains	https://cti.nshc.net/events/view/8743
2024-07-26	SectorA01 used DLL Malware variants	https://cti.nshc.net/events/view/8843
2024-07-26	SectorA04 used the infrastructure for cyber-attack activities	https://cti.nshc.net/events/view/8689
2024-07-26	SectorA04 used an exploit to gain initial access	https://cti.nshc.net/events/view/8694
2024-07-26	SectorA04 targets sensitive military information and the intellectual property of defense	https://cti.nshc.net/events/view/8733
2024-07-26	SectorA05 used DLL Malware variant	https://cti.nshc.net/events/view/8692
2024-07-26	SectorA05 used a new Domains	https://cti.nshc.net/events/view/8734
2024-07-26	SectorA05 used a new Domains	https://cti.nshc.net/events/view/8753
2024-07-27	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/8844
2024-07-29	SectorA01 used Script Malware disguised as a Cryptocurrency project source code	https://cti.nshc.net/events/view/8845
2024-07-29	SectorA05 used Malware variants	https://cti.nshc.net/events/view/8841
2024-07-29	SectorA05 used LNK Malware disguised as a Cryptocurrency exchanges documents	https://cti.nshc.net/events/view/8884
2024-07-30	SectorA01 used Malware variant	https://cti.nshc.net/events/view/8870
2024-07-31	SectorA01 used DLL Malware variants	https://cti.nshc.net/events/view/8795
2024-07-31	SectorA01 used the NPM Packages to distribute Malware	https://cti.nshc.net/events/view/8785
2024-07-31	SectorA01 used Script Malware disguised as a job interview	https://cti.nshc.net/events/view/8788
2024-07-31	SectorA05 used PowerShell Malware variant	https://cti.nshc.net/events/view/8773
2024-07-31	SectorA05 used PowerShell Malware variant	https://cti.nshc.net/events/view/8869
2024-07-31	SectorA07 used LNK Malware disguised as Meeting Materials	https://cti.nshc.net/events/view/8770
2024-08-01	SectorA01 used Malware disguised as a Free Conference Call Services software	https://cti.nshc.net/events/view/8871
2024-08-01	SectorA05 used Malware variants	https://cti.nshc.net/events/view/8796
2024-08-04	SectorA01 used Script Malware disguised as a 3DWorld Tectera project source code	https://cti.nshc.net/events/view/8883
2024-08-05	SectorA05 used Malware disguised as a Internet Explorer service update	https://cti.nshc.net/events/view/9049
2024-08-06	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/8931
2024-08-06	SectorA04 used Malware variants	https://cti.nshc.net/events/view/8929
2024-08-06	SectorA05 used a new Domains	https://cti.nshc.net/events/view/8812
2024-08-06	SectorA05 used a new Domains	https://cti.nshc.net/events/view/8817
2024-08-08	SectorA01 used Malware variants	https://cti.nshc.net/events/view/8930

2024-08-09	SectorA05 used phishing attacks targeting university	https://cti.nshc.net/events/view/8846
2024-08-10	SectorA01 used Script Malware disguised as a Mobilespace booking project source code	https://cti.nshc.net/events/view/8937
2024-08-13	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/8979
2024-08-13	SectorA01 used Malware variants	https://cti.nshc.net/events/view/9046
2024-08-13	SectorA05 used CHM Malware disguised as meeting agenda	https://cti.nshc.net/events/view/8874
2024-08-13	SectorA06 used various Crypto Wallet	https://cti.nshc.net/events/view/8909
2024-08-14	SectorA01 used MacOS malware disguised as Free Conference Call Services app	https://cti.nshc.net/events/view/8978
2024-08-14	SectorA02 exploited Windows Scripting Engine vulnerability	https://cti.nshc.net/events/view/8882
2024-08-14	SectorA04 exploited an Antivirus software management server vulnerability	https://cti.nshc.net/events/view/8900
2024-08-14	SectorA05 used a WebShell Domains	https://cti.nshc.net/events/view/8904
2024-08-15	SectorA01 used Nukesped Malware variants	https://cti.nshc.net/events/view/8976
2024-08-16	SectorA05 used Script Malware disguised as a Animation document	https://cti.nshc.net/events/view/8899
2024-08-16	SectorA05 used Malware disguised as Software update files	https://cti.nshc.net/events/view/8902
2024-08-16	SectorA06 used MacOS malware disguised as Bitcoin Price Information	https://cti.nshc.net/events/view/8949
2024-08-17	SectorA01 used Script Malware disguised as a Metaverse project source code	https://cti.nshc.net/events/view/8980
2024-08-18	SectorA01 used Nukesped Malware variants	https://cti.nshc.net/events/view/8977
2024-08-18	SectorA04 used TigerRAT Malware variants	https://cti.nshc.net/events/view/8974
2024-08-18	SectorA05 used LightShell Malware variants	https://cti.nshc.net/events/view/8975
2024-08-19	SectorA01 used MSI Malware disguised as Conference Call Services software	https://cti.nshc.net/events/view/8936
2024-08-19	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9047
2024-08-20	SectorA01 used Malware variants	https://cti.nshc.net/events/view/9045
2024-08-21	SectorA05 used LNK Malware disguised as a plan for a private policy meeting	https://cti.nshc.net/events/view/8981
2024-08-21	SectorA05 distributed a variant of the open-source RAT Malware	https://cti.nshc.net/events/view/8948
2024-08-22	SectorA05 used PowerShell malwares	https://cti.nshc.net/events/view/9042
2024-08-22	SectorA06 used a new Domains	https://cti.nshc.net/events/view/8952
2024-08-22	SectorA06 used a new Domains	https://cti.nshc.net/events/view/8969
2024-08-22	SectorA07 used Malware variants	https://cti.nshc.net/events/view/8950
2024-08-23	SectorA01 used Nukesped Malware variants	https://cti.nshc.net/events/view/9041
2024-08-23	SectorA01 used Script Malware disguised as a Chess player project source code	https://cti.nshc.net/events/view/9043

2024-08-25	SectorA01 used Script Malware disguised as a Casino game project source code	https://cti.nshc.net/events/view/9000
2024-08-26	SectorA03 exploits Google Chromium vulnerabilities to distribute malware	https://cti.nshc.net/events/view/8987
2024-08-26	SectorA05 used LNK Malware disguised as a construction company invoice	https://cti.nshc.net/events/view/8993
2024-08-26	SectorA05 used a new Domains	https://cti.nshc.net/events/view/10205
2024-08-27	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/9050
2024-08-27	SectorA01 used Script Malware disguised as a Moonverse project source code	https://cti.nshc.net/events/view/9051
2024-08-28	SectorA03 used MHTML malware that exploited vulnerabilities in Kingsoft WPS Office	https://cti.nshc.net/events/view/9008
2024-08-28	SectorA05 used Spear Phishing email disguised as a Request a lecture on Understanding Northeast Asia and North Korea for Peaceful Reunification	https://cti.nshc.net/events/view/9004
2024-08-28	SectorA05 used Phishing webpage disguised as Naver login webpage	https://cti.nshc.net/events/view/9016
2024-08-28	SectorA07 used Phishing webpage disguised as Naver login webpage	https://cti.nshc.net/events/view/9015
2024-08-29	SectorA01 used Script Malware disguised as a Real Estate project source code	https://cti.nshc.net/events/view/9353
2024-08-30	SectorA01 exploited Google Chromium vulnerability	https://cti.nshc.net/events/view/9036
2024-08-30	SectorA05 used Malware disguised as a Speaking engagement requests	https://cti.nshc.net/events/view/9038
2024-08-30	SectorA05 used Malware disguised as a Speaking engagement request form	https://cti.nshc.net/events/view/9034
2024-09-01	SectorA01 used the NPM Packages to distribute Malware	https://cti.nshc.net/events/view/9040
2024-09-01	SectorA07 used LNK malware variants	https://cti.nshc.net/events/view/9059
2024-09-02	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/9352
2024-09-04	SectorA01 used Malware disguised as a Node.js-based web game project	https://cti.nshc.net/events/view/9099
2024-09-04	SectorA01 used Script Malware disguised as a Metaverse project source code	https://cti.nshc.net/events/view/9349
2024-09-04	SectorA05 used Malware disguised as a Speaking engagement requests	https://cti.nshc.net/events/view/9106
2024-09-04	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9380
2024-09-05	SectorA01 used Script Malware disguised as a ReferralReactJS source code	https://cti.nshc.net/events/view/9351
2024-09-05	SectorA05 used MSC Malware variants	https://cti.nshc.net/events/view/9140
2024-09-05	SectorA07 used LNK Malware variants	https://cti.nshc.net/events/view/9124
2024-09-06	SectorA01 used Script Malware disguised as a Metaverse project source code	https://cti.nshc.net/events/view/9355

2024-09-06	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/9356
2024-09-06	SectorA05 used Word Malware disguised as a Request for advice	https://cti.nshc.net/events/view/9381
2024-09-06	SectorA05 used Phishing webpage disguised as Naver login webpage	https://cti.nshc.net/events/view/9348
2024-09-08	SectorA01 used Malware disguised as a Putty utility	https://cti.nshc.net/events/view/9180
2024-09-08	SectorA01 used Malware variant	https://cti.nshc.net/events/view/9358
2024-09-08	SectorA01 used Malware variants	https://cti.nshc.net/events/view/9379
2024-09-08	SectorA04 used Malware variants	https://cti.nshc.net/events/view/9357
2024-09-09	SectorA01 used Malware disguised as Software Update	https://cti.nshc.net/events/view/9450
2024-09-09	SectorA01 used macOS Malware variants	https://cti.nshc.net/events/view/9451
2024-09-09	SectorA01 used Script Malware disguised as a Decentralized Finance project source code	https://cti.nshc.net/events/view/9489
2024-09-09	SectorA01 used Malware variant	https://cti.nshc.net/events/view/9490
2024-09-09	SectorA04 used Remote Administration Tool	https://cti.nshc.net/events/view/9452
2024-09-09	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9178
2024-09-09	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9491
2024-09-09	SectorA05 used VBS Malware variant	https://cti.nshc.net/events/view/9492
2024-09-09	SectorA06 used MacOS malware disguised as Discord apps	https://cti.nshc.net/events/view/9449
2024-09-10	SectorA01 used Malware variants	https://cti.nshc.net/events/view/9196
2024-09-10	SectorA01 used Malware variants	https://cti.nshc.net/events/view/9197
2024-09-10	SectorA03 used Malware variants	https://cti.nshc.net/events/view/9219
2024-09-10	SectorA05 used Phishing webpage disguised as a Universities webpages	https://cti.nshc.net/events/view/9388
2024-09-11	SectorA05 used a new Domains	https://cti.nshc.net/events/view/9290
2024-09-11	SectorA05 used a new Domains	https://cti.nshc.net/events/view/9291
2024-09-12	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9234
2024-09-12	SectorA05 used MSC Malware disguised as an advisory document	https://cti.nshc.net/events/view/9292
2024-09-13	SectorA01 used Malware variants	https://cti.nshc.net/events/view/9243
2024-09-13	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9493
2024-09-15	SectorA01 used Script Malware disguised as a Faucet project source code	https://cti.nshc.net/events/view/9637
2024-09-16	SectorA06 used MacOS Malware disguised as pre-employment test	https://cti.nshc.net/events/view/9386
2024-09-17	SectorA05 used a new Domains	https://cti.nshc.net/events/view/9474
2024-09-18	SectorA01 used Malware disguised as Fake recruiter coding test	https://cti.nshc.net/events/view/9390
2024-09-18	SectorA01 used MSI Malware disguised as conference call service software	https://cti.nshc.net/events/view/9473

2024-09-18	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/9715
2024-09-18	SectorA04 used a modified version of SumatraPDF to execute malicious PDF	https://cti.nshc.net/events/view/9391
2024-09-19	SectorA01 used MacOS malware disguised as a OSX-PDF-Viewer	https://cti.nshc.net/events/view/9495
2024-09-19	SectorA01 distributed Stealer Malware via a GitHub phishing site	https://cti.nshc.net/events/view/9448
2024-09-19	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9314
2024-09-19	SectorA05 used Malware disguised as a Speaking engagement requests	https://cti.nshc.net/events/view/9931
2024-09-20	SectorA01 used Malware variant	https://cti.nshc.net/events/view/9494
2024-09-20	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/9496
2024-09-20	SectorA07 used PowerShell malware variants	https://cti.nshc.net/events/view/9354
2024-09-21	SectorA01 used Script Malware variants	https://cti.nshc.net/events/view/9623
2024-09-21	SectorA02 used Malware variants	https://cti.nshc.net/events/view/9376
2024-09-21	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9378
2024-09-23	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/9622
2024-09-23	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9438
2024-09-23	SectorA05 used Script Malware variant	https://cti.nshc.net/events/view/9497
2024-09-23	SectorA05 used PowerShell Malware variants	https://cti.nshc.net/events/view/9508
2024-09-23	SectorA05 used PowerShell Malware variants	https://cti.nshc.net/events/view/9624
2024-09-24	SectorA01 used fake IT worker identities to secure a job	https://cti.nshc.net/events/view/9571
2024-09-24	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9468
2024-09-25	SectorA05 used XML Malware disguised as Essay	https://cti.nshc.net/events/view/9540
2024-09-26	SectorA01 used Malware variants	https://cti.nshc.net/events/view/9525
2024-09-26	SectorA01 used Malware variants	https://cti.nshc.net/events/view/9657
2024-09-26	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9527
2024-09-26	SectorA05 used keylogger Malware variants	https://cti.nshc.net/events/view/9566
2024-09-26	SectorA05 used MSC Malware disguised as a Zoom Meeting app	https://cti.nshc.net/events/view/9655
2024-09-26	SectorA05 used LNK Malware disguised as a subsidy application inquiry form	https://cti.nshc.net/events/view/9619
2024-09-28	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/9656
2024-09-28	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9577
2024-09-30	SectorA05 used a new Domains	https://cti.nshc.net/events/view/9629
2024-09-30	SectorA05 used new Domains	https://cti.nshc.net/events/view/9667
2024-10-01	SectorA05 used Script malwares	https://cti.nshc.net/events/view/9877
2024-10-02	SectorA01 used Malware variants	https://cti.nshc.net/events/view/9647
2024-10-02	SectorA01 used Malware in financially motivated attacks	https://cti.nshc.net/events/view/9666
2024-10-03	SectorA02 used LNK Malware disguised as an NGO income Report	https://cti.nshc.net/events/view/9714

2024-10-03	SectorA05 used PowerShell malwares	https://cti.nshc.net/events/view/9875
2024-10-04	SectorA05 used a new Domains	https://cti.nshc.net/events/view/9713
2024-10-07	SectorA05 used a new Domains	https://cti.nshc.net/events/view/9724
2024-10-08	SectorA01 used Script Malware variants	https://cti.nshc.net/events/view/9763
2024-10-08	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/9873
2024-10-08	SectorA05 used MSC Malware disguised as a Zoom Meeting app	https://cti.nshc.net/events/view/9840
2024-10-08	SectorA07 used LNK Malware disguised as a Request to verify project information	https://cti.nshc.net/events/view/9781
2024-10-09	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9728
2024-10-09	SectorA05 used MSC Malware disguised as a Interview questionnaires	https://cti.nshc.net/events/view/9872
2024-10-10	SectorA05 used a new Domains	https://cti.nshc.net/events/view/9753
2024-10-10	SectorA05 used Phishing email disguised as a Interim income tax payments for corporations ending in December	https://cti.nshc.net/events/view/9760
2024-10-11	SectorA01 used Malware variants	https://cti.nshc.net/events/view/9777
2024-10-11	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/9834
2024-10-11	SectorA01 used Script Malware disguised as a CryptoView project source code	https://cti.nshc.net/events/view/9874
2024-10-11	SectorA06 used Malware variants	https://cti.nshc.net/events/view/9769
2024-10-11	SectorA07 used LNK malware disguised as a COVID-19 case status document	https://cti.nshc.net/events/view/9820
2024-10-12	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9790
2024-10-13	SectorA01 used Script Malware disguised as a BrangeDeFi project source code	https://cti.nshc.net/events/view/9835
2024-10-13	SectorA01 used Malware to target linux payment switches for ATM attacks	https://cti.nshc.net/events/view/9863
2024-10-13	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9807
2024-10-13	SectorA06 used Malware variants	https://cti.nshc.net/events/view/9803
2024-10-14	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/10204
2024-10-14	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9815
2024-10-14	SectorA05 used LNK Malware Disguised as a Travel Recommendation Essay	https://cti.nshc.net/events/view/9823
2024-10-14	SectorA05 used LNK Malware Disguised as a Crypto Trading Guide	https://cti.nshc.net/events/view/9832
2024-10-14	SectorA05 used PowerShell Malware variants	https://cti.nshc.net/events/view/9871
2024-10-14	SectorA06 used Malware variants	https://cti.nshc.net/events/view/9812
2024-10-15	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/10241
2024-10-15	SectorA06 used Malware variants	https://cti.nshc.net/events/view/9829
2024-10-16	SectorA02 exploited Windows Scripting Engine vulnerability	https://cti.nshc.net/events/view/9926
2024-10-16	SectorA06 used Malware variants	https://cti.nshc.net/events/view/9851

2024-10-16	SectorA07 used a new Domains	https://cti.nshc.net/events/view/9898
2024-10-17	SectorA01 used Malicious NPM Package Disguised as NFT Marketplace Project	https://cti.nshc.net/events/view/10031
2024-10-17	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/10158
2024-10-17	SectorA05 used a new Domains	https://cti.nshc.net/events/view/9967
2024-10-17	SectorA06 used Malware variants	https://cti.nshc.net/events/view/9880
2024-10-18	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9913
2024-10-18	SectorA06 used Malware variants	https://cti.nshc.net/events/view/9915
2024-10-18	SectorA07 used JSE Malware disguised as Explorer	https://cti.nshc.net/events/view/10034
2024-10-19	SectorA01 used Script Malware disguised as a Blockchain wallet integration project source code	https://cti.nshc.net/events/view/10186
2024-10-19	SectorA01 used Script Malware disguised as a World map app source code	https://cti.nshc.net/events/view/10242
2024-10-19	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9938
2024-10-19	SectorA06 used Malware variants	https://cti.nshc.net/events/view/9936
2024-10-20	SectorA01 used Malware variant	https://cti.nshc.net/events/view/10243
2024-10-20	SectorA06 used Malware variants	https://cti.nshc.net/events/view/9959
2024-10-21	SectorA05 used Malware variants	https://cti.nshc.net/events/view/9986
2024-10-21	SectorA06 used Malware variants	https://cti.nshc.net/events/view/9976
2024-10-22	SectorA01 used Script Malware variants	https://cti.nshc.net/events/view/10210
2024-10-22	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/10717
2024-10-22	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10003
2024-10-23	SectorA01 used Malware variants	https://cti.nshc.net/events/view/10016
2024-10-23	SectorA01 used Malware disguised as software associated with job postings	https://cti.nshc.net/events/view/10073
2024-10-23	SectorA01 used Malware disguised as a Tank game	https://cti.nshc.net/events/view/10135
2024-10-23	SectorA02 exploited Windows Scripting Engine Vulnerability	https://cti.nshc.net/events/view/10296
2024-10-23	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10014
2024-10-24	SectorA01 used malicious NPM packages	https://cti.nshc.net/events/view/10128
2024-10-24	SectorA01 used macOS Malware variants	https://cti.nshc.net/events/view/10720
2024-10-24	SectorA05 used LNK Malware variants	https://cti.nshc.net/events/view/10057
2024-10-24	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10045
2024-10-25	SectorA05 used Script Malware variant	https://cti.nshc.net/events/view/10718
2024-10-25	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10061
2024-10-26	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10084
2024-10-27	SectorA01 used Script Malware disguised as a Decentralized Application project source code	https://cti.nshc.net/events/view/10719
2024-10-27	SectorA05 used Malware variants	https://cti.nshc.net/events/view/10106
2024-10-27	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10103
2024-10-28	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10113
2024-10-28	SectorA07 used LNK malware variants	https://cti.nshc.net/events/view/10721

2024-10-29	SectorA05 used Spoofed Domains for Naver and Apple Phishing Campaigns	https://cti.nshc.net/events/view/10290
2024-10-29	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10148
2024-10-30	SectorA01 used Malware variants	https://cti.nshc.net/events/view/10178
2024-10-30	SectorA04 used Play Ransomware	https://cti.nshc.net/events/view/10187
2024-10-30	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10165
2024-10-31	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/10332
2024-10-31	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10194
2024-11-01	SectorA01 used Malware variants	https://cti.nshc.net/events/view/10225
2024-11-01	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/10723
2024-11-01	SectorA05 used Malware variants	https://cti.nshc.net/events/view/10226
2024-11-01	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10223
2024-11-02	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10247
2024-11-03	SectorA05 used Malware variants	https://cti.nshc.net/events/view/10262
2024-11-03	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10265
2024-11-04	SectorA01 used Fake Identities to Secure Remote Jobs	https://cti.nshc.net/events/view/10292
2024-11-04	SectorA01 used Script Malware disguised as a BTC transfer app project source code	https://cti.nshc.net/events/view/10333
2024-11-04	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/10516
2024-11-04	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/10722
2024-11-04	SectorA02 used LNK Malware disguised as Security Column	https://cti.nshc.net/events/view/10289
2024-11-04	SectorA05 used Malware variants	https://cti.nshc.net/events/view/10279
2024-11-04	SectorA05 used Word Malware disguised as a Cloud security guide	https://cti.nshc.net/events/view/10724
2024-11-04	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10275
2024-11-05	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/10728
2024-11-05	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10287
2024-11-07	SectorA05 used MSC Malware variants	https://cti.nshc.net/events/view/10732
2024-11-07	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10323
2024-11-07	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10324
2024-11-07	SectorA06 used Malware Disguised as Fake Crypto News to Target macOS Users	https://cti.nshc.net/events/view/10375
2024-11-07	SectorA07 used LNK malware variants	https://cti.nshc.net/events/view/10727
2024-11-08	SectorA01 used Script Malware disguised as a WePark-Network project source code	https://cti.nshc.net/events/view/10729
2024-11-08	SectorA04 used Malware variants	https://cti.nshc.net/events/view/10354
2024-11-08	SectorA05 used Malware variants	https://cti.nshc.net/events/view/10365
2024-11-09	SectorA04 used Malware variants	https://cti.nshc.net/events/view/10398
2024-11-10	SectorA01 used Script Malware disguised as a Software project source code	https://cti.nshc.net/events/view/10514
2024-11-10	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10418

2024-11-11	SectorA01 used Malware disguised as a 3CX DesktopApp	https://cti.nshc.net/events/view/10733
2024-11-11	SectorA02 used Malware variants	https://cti.nshc.net/events/view/10440
2024-11-11	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10435
2024-11-12	SectorA01 used Flutter Framework to Obfuscate Malware in macOS Applications	https://cti.nshc.net/events/view/10502
2024-11-12	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10458
2024-11-13	SectorA01 used Extended Attributes to Conceal Malicious Components	https://cti.nshc.net/events/view/10605
2024-11-13	SectorA03 Used Malware Disguised as a Chinese Embassy Invitation	https://cti.nshc.net/events/view/10592
2024-11-13	SectorA05 used Script Malware variant	https://cti.nshc.net/events/view/10953
2024-11-13	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10470
2024-11-13	SectorA06 used a new Domains	https://cti.nshc.net/events/view/10503
2024-11-14	SectorA01 Used GitHub to Deliver Malware in Targeted Developer Attacks	https://cti.nshc.net/events/view/10611
2024-11-14	SectorA01 used Script Malware variants	https://cti.nshc.net/events/view/10734
2024-11-14	SectorA01 Exploited Fake North Korean IT Workers to Conduct Phishing Campaigns	https://cti.nshc.net/events/view/10595
2024-11-14	SectorA02 used LNK malware disguised as a China's North Korea policy changes after North Korea meeting report	https://cti.nshc.net/events/view/10511
2024-11-14	SectorA04 used Malware variants	https://cti.nshc.net/events/view/10499
2024-11-14	SectorA05 used Malware variants	https://cti.nshc.net/events/view/10486
2024-11-14	SectorA05 exploited GitHub Repository service	https://cti.nshc.net/events/view/10574
2024-11-14	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10488
2024-11-15	SectorA01 used macOS Malware variants	https://cti.nshc.net/events/view/10906
2024-11-15	SectorA01 used Script Malware disguised as a WePark-Network project source code	https://cti.nshc.net/events/view/10952
2024-11-15	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10533
2024-11-17	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10584
2024-11-18	SectorA04 used Malware variants	https://cti.nshc.net/events/view/10905
2024-11-18	SectorA05 used MSC Malware disguised as Response from the Department of Defense	https://cti.nshc.net/events/view/10967
2024-11-19	SectorA01 used Malware variant	https://cti.nshc.net/events/view/10637
2024-11-20	SectorA01 used MacOS malware disguised as Free Conference Call Services app	https://cti.nshc.net/events/view/10966
2024-11-20	SectorA02 used Malware variants	https://cti.nshc.net/events/view/10629
2024-11-20	SectorA02 used Phishing email disguised as a Electronic Notification Service	https://cti.nshc.net/events/view/10638
2024-11-20	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10623
2024-11-20	SectorA06 used Script malware variants	https://cti.nshc.net/events/view/10965

2024-11-21	SectorA01 Used Social Engineering Tactics to Deploy LCPDot Malware	https://cti.nshc.net/events/view/10709
2024-11-21	SectorA05 used Malware variants	https://cti.nshc.net/events/view/10658
2024-11-21	SectorA05 used Spear Phishing Email disguised as Martial Law Doc	https://cti.nshc.net/events/view/13134
2024-11-21	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10648
2024-11-22	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10690
2024-11-23	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/10813
2024-11-23	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/10814
2024-11-23	SectorA01 used Script Malware disguised as a Payment project source code	https://cti.nshc.net/events/view/10816
2024-11-23	SectorA01 used Malware variant	https://cti.nshc.net/events/view/10963
2024-11-23	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10739
2024-11-24	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10760
2024-11-25	SectorA05 used LNK Malware variants	https://cti.nshc.net/events/view/11112
2024-11-25	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11115
2024-11-25	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10776
2024-11-26	SectorA03 used cloud storage and file manipulation techniques	https://cti.nshc.net/events/view/10819
2024-11-26	SectorA05 used Malware variants	https://cti.nshc.net/events/view/10809
2024-11-26	SectorA06 used Malware variants	https://cti.nshc.net/events/view/10803
2024-11-27	SectorA05 used Malware variants	https://cti.nshc.net/events/view/10831
2024-11-28	SectorA05 used LNK Malware variants	https://cti.nshc.net/events/view/11111
2024-11-30	SectorA01 used Malware variant	https://cti.nshc.net/events/view/10991
2024-11-30	SectorA04 used Malware variants	https://cti.nshc.net/events/view/10989
2024-11-30	SectorA05 used Malware variants	https://cti.nshc.net/events/view/10894
2024-12-01	SectorA01 used Script Malware disguised as a project source code	https://cti.nshc.net/events/view/10987
2024-12-01	SectorA04 used Malware variants	https://cti.nshc.net/events/view/10917
2024-12-02	SectorA05 used Malware variants	https://cti.nshc.net/events/view/10948
2024-12-02	SectorA05 used a new Domains	https://cti.nshc.net/events/view/10980
2024-12-02	SectorA05 used PowerShell Malware variants	https://cti.nshc.net/events/view/11348
2024-12-02	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11349
2024-12-03	SectorA05 used Word Malware variants	https://cti.nshc.net/events/view/11341
2024-12-04	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11004
2024-12-04	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11009
2024-12-05	SectorA01 used Malware variant	https://cti.nshc.net/events/view/11339
2024-12-05	SectorA01 used Malware variant	https://cti.nshc.net/events/view/11346
2024-12-05	SectorA01 used Malware variant	https://cti.nshc.net/events/view/11350
2024-12-05	SectorA03 used Malware variants	https://cti.nshc.net/events/view/11019
2024-12-06	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11056
2024-12-07	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11065
2024-12-07	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11067

2024-12-07	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11073
2024-12-08	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11085
2024-12-08	SectorA01 used Script Malware disguised as a NFL Game Information project source code	https://cti.nshc.net/events/view/11117
2024-12-08	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/11338
2024-12-08	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11079
2024-12-09	SectorA02 used Malware variants	https://cti.nshc.net/events/view/11097
2024-12-09	SectorA02 used LNK Malware disguised as a Course resources	https://cti.nshc.net/events/view/11214
2024-12-09	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11096
2024-12-09	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11102
2024-12-11	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/11301
2024-12-11	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/11314
2024-12-11	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11315
2024-12-11	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11142
2024-12-12	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11312
2024-12-12	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11316
2024-12-12	SectorA02 used Malware variant	https://cti.nshc.net/events/view/11300
2024-12-13	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11201
2024-12-13	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11204
2024-12-13	SectorA02 used Malware variants	https://cti.nshc.net/events/view/11199
2024-12-13	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11184
2024-12-14	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11234
2024-12-14	SectorA01 used Script Malware disguised as a Hoody Gang project source code	https://cti.nshc.net/events/view/11305
2024-12-14	SectorA05 used MSC Malware disguised as a Zoom Meeting app	https://cti.nshc.net/events/view/11299
2024-12-15	SectorA05 used PowerShell malwares	https://cti.nshc.net/events/view/11313
2024-12-17	SectorA01 used Malware variants	https://cti.nshc.net/events/view/11686
2024-12-17	SectorA05 used Phishing webpage disguised as Naver login webpage	https://cti.nshc.net/events/view/11307
2024-12-18	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11328
2024-12-19	SectorA01 used macOS Malware variants	https://cti.nshc.net/events/view/11685
2024-12-19	SectorA01 used Script Malware variants	https://cti.nshc.net/events/view/11689
2024-12-19	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11399
2024-12-20	SectorA07 used CHM malware disguised as a financial transaction confirmation	https://cti.nshc.net/events/view/11401
2024-12-20	SectorA07 used LNK malware disguised as a Cover letter	https://cti.nshc.net/events/view/11692
2024-12-21	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11419
2024-12-23	SectorA04 used SmallTiger Malware to Target Centralized Solutions	https://cti.nshc.net/events/view/11481
2024-12-23	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11465

2024-12-23	SectorA07 used LNK Malware variants	https://cti.nshc.net/events/view/11497
2024-12-25	SectorA01 Used Malware for Data Theft and Cryptocurrency Wallet Key Extraction	https://cti.nshc.net/events/view/11619
2024-12-25	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11508
2024-12-26	SectorA01 used Malware disguised as Messenger installer	https://cti.nshc.net/events/view/11624
2024-12-27	SectorA01 used JavaScript malware disguised as a Betting Site multichain project source code	https://cti.nshc.net/events/view/11627
2024-12-28	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/11630
2024-12-29	SectorA01 used Python Malware variants	https://cti.nshc.net/events/view/11626
2024-12-30	SectorA01 used JavaScript malware disguised as a Euron presale source code	https://cti.nshc.net/events/view/11628
2024-12-30	SectorA05 used Malware variants	https://cti.nshc.net/events/view/11605

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.