STRIKE TEAM

レポート

Operation Phantom Circuit

北朝鮮による世界規模のデータ窃取攻撃

SecurityScorecard

背景

STRIKE の「Operation 99」の調査において、2024 年 9 月から稼働していると見られる複数のコマンド アンド コントロール（C2）サーバーが確認されました。こうしたサーバーは、ペイロードの構造や難読化の手法にばらつきがあるものの、攻撃全体で一貫した実装を共有していました。その主な目的は、ペイロードを配信し、ポート 1224 を介して感染したシステムとの通信を維持することのように見えました。しかし、さらに深く分析すると、別の活動層があることがわかりました。

窃取されたデータがどのように処理されたのか、こうしたサーバーの管理にどのようなインフラが利用されたのか、といった重大な疑問点は、これまで未解決のままでした。今回の調査により、Lazarus のキャンペーンを一元管理する、C2 インフラ内に隠された管理システムを発見しました。

この隠れた管理レイヤーの発見によって、Lazarus の攻撃の仕組みに関する重要な情報が得られました。各 C2 サーバーは、React アプリケーションと Node.js API で構築された **Web ベースの管理プラットフォーム**をホストしていました。このプラットフォームは単なるインターフェースではなく、包括的なシステムであり、攻撃者はこれを利用して次のことが可能になりました。

- 窃取したデータを正確に整理・管理する。
- 侵害したシステムを直接監視する。
- ペイロードの配信やその他の攻撃オペレーションを中央ハブから制御する。

攻撃者が検知を回避するためにペイロードや難読化の手法を変えていた場合でも、この管理層は、分析したすべての C2 サーバーで一貫していました。

サプライチェーン攻撃

Lazarus は、難読化されたバックドアを埋め込むことで、正規のソフトウェアパッケージを改竄し、開発者を騙してこれらの危険なパッケージを実行させることが確認されています。一般人の目にはわからないため、被害者に気づかれず、巧妙に実行されます。こうしたパッケージには、暗号通貨アプリから認証ソリューションまで、あらゆる種類のソフトウェアが含まれている可能性があります。

全世界への拡大

今回の分析から、Lazarus は全世界の暗号通貨業界と開発者をターゲットにした世界規模の攻撃を組織的に行っていたことが明らかになりました。この攻撃によって、何百人もの被害者がペイロードをダウンロードして実行し、その間に窃取されたデータは密かに平壌へ送信されていました。

平壌との関係

Team Cymru の Netflow データを使用し、時間的なトラフィックパターンを分析することで、STRIKE は高い確信をもってこの活動の発信源を平壌と特定しました。Lazarus グループは、多層的な難読化戦略を取り入れて、その出自を隠蔽し、攻撃を管理していました。攻撃の流れは次のとおりです。

1. **初回の接続：**攻撃の起点となる接続を開始した北朝鮮の IP アドレスが 6 件確認されました。
2. **VPN の難読化：**攻撃者は **Astrill VPN エンドポイント**を経由してトラフィックをルーティングし、商用サービスを利用して実際の地理的発信源を隠蔽していました。
3. **プロキシリレー：**VPN からのトラフィックは、ロシア・ハサンの登録情報を持つ **Sky Freight Limited** の中間プロキシ層を経由して移動しました。この追加層は、悪意のあるトラフィックと正当なネットワーク活動を混在させていました。
4. **コマンド アンド コントロール（C2）サーバー：**難読化されたトラフィックは最終的に、Stark Industries のサーバーでホストされている C2 インフラに到達しました。これらのサーバーによって、ペイロードの配信、感染端末の管理、データの窃取がしやすい状態になっていました。

この多層化されたインフラは、6 件の北朝鮮の IP アドレスを C2 サーバーに直接紐づけており、Lazarus グループが北朝鮮国内からの攻撃の管理を担っていることを裏付けています。

重要な調査結果

- STRIKE チームは、標的型攻撃の調整に使用された作戦インフラの特定に成功しました。高い信頼性で、Astrill VPN からのトラフィックをプロキシを通じて目的地の C2 にルーティングする役割を果たしたのはこのネットワークであると考えられます。
- Lazarus は、Astrill VPN の出口ポイントとプロキシの高度なネットワークを使用して、C2 サーバーを管理しながらトラフィックを隠蔽しています。STRIKE は、VPN を経由して北朝鮮の平壌にある 6 件の異なる IP アドレスへの接続にたどり着くことができました。
- この作戦は、Lazarus が正規のソフトウェアに悪質なコードを埋め込むという、ソフトウェアサプライチェーン攻撃の明らかな証拠です。2024 年 9 月から 2025 年 1 月までの標的型攻撃が確認されました。最新の攻撃では、世界全体で 233 件の被害がありました。
- Lazarus は、窃取したデータとペイロードの配信を管理するために、高度な React アプリケーションと API を開発していました。このアプリケーションはすべての C2 サーバーに展開され、ポート 1245 で管理されました。

攻撃者の工作インフラ

Lazarus のオペレーターは、これらの C2 と関連資産を管理するための工作インフラを維持していました。そこで、攻撃者がインフラを制御している場所を特定するために、C2 サーバーへの接続を見つけることから調査を開始しました。1245 や 3389（リモートデスクトップ）などの管理ポートを介して C2 に接続する、中間プロキシネットワークを特定しました。

WHOIS やその他の公開記録によると、この中間プロキシネットワークの IP は、ロシア・ハサンの登録情報をもつ

Sky Freight Limited に登録されています。後述しますが、実際にはこれらは Oculus Proxy ネットワークに割り当てられています。

```
inetnum:        83.234.227.0 - 83.234.227.255
netname:        SKYFREIGHT-NET
descr:          (MS009388) Skyfreight_Limited,
descr:          Hasan, Russia
country:        RU
admin-c:        KTTK-RIPE
tech-c:         KTTK-RIPE
status:         ASSIGNED PA
mnt-by:         TRANSTELECOM-MNT
created:        2023-06-02T15:31:08Z
last-modified:  2023-06-02T15:31:08Z
```

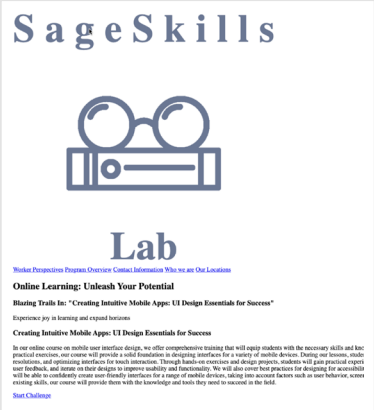
攻撃者は IP アドレス 83[.]234[.]227[.]50 から複数の C2 サーバーを管理していることが確認されました。この IP は、1 月 17 日から 1 月 18 日にかけて、ポート 1245 経由で最新の C2 サーバー 94[.]131[.]9[.]32 に接続しており、本稿執筆時点でも稼働中です。さらに、12 月 26 日から 1 月 16 日にかけて、ポート 1224、1245、2248、2252（C2 専用ポート）、3389（RDP）で 185[.]153[.]182[.]241 に接続した履歴が残っています。また、12 月 26 日から 1 月 17 日にかけて、ポート 1224、1245、3389 で 5[.]253[.]43[.]122 と接続を確立しています。どちらのサーバーも、この活動に関連した標的型攻撃に使用されました。

攻撃者は、リモートデスクトッププロトコル（RDP）経由で数回（12 月 30 日、1 月 6 日、1 月 10 日）にわたり 185[.]153[.]182[.]241 にアクセスし、RDP セッションを 10 日間維持しました。C2 サーバー 5[.]253[.]43[.]122 が関与した Operation 99 では、攻撃者は 12 月 26 日から 1 月 15 日の間に十数回、RDP 経由でログインしました。

この活動を念頭に置くと、高い信頼性で、IP アドレス 83[.]234[.]227[.]50 は、複数の異なる C2 サーバーに接続されていることからも、Lazarus グループが制御する中間プロキシとして機能していると判断されます。

さらに分析を進めると、12 月 2 日から 12 月 10 日の間に、同じ IP 範囲から別の IP、83[.]234[.]227[.]49 が、ポート 3389、1224、1245 経由で別の Lazarus 制御サーバー（45[.]128[.]52[.]14）に接続していることが判明しました。この C2 は Stark Industries のインフラでホストされており、2024 年 11 月に Codementor プラットフォーム上で Lazarus の存在が公に報告された攻撃と関連する Operation99 と同様の活動を示していました。

さらに詳細に調査したところ、もう一つの Lazarus C2 サーバーが発見され（86[.]104[.]74[.]51）、2024 年 11 月の大半は稼働していたことが明らかになりました。このサーバーも Stark Industries のインフラでホストされており、2024 年 9 月下旬にドメイン sageskills-uk[.]com に解決し、正規の組織 skillsage.uk になりすましていました。C2 サーバーは、ロシアでホストされている同じ中間プロキシの出口ポイントからアクセスされていました。


SageSkills

Lab

Worker Perspectives Program Overview Contact Information Who we are Our Locations

Online Learning: Unleash Your Potential

Blazing Trails In: "Creating Intuitive Mobile Apps: UI Design Essentials for Success"

Experience joy in learning and expand horizons

Creating Intuitive Mobile Apps: UI Design Essentials for Success

In our online course on mobile user interface design, we offer comprehensive training that will equip students with the necessary skills and knc practical exercises, our course will provide a solid foundation in designing interfaces for a variety of mobile devices. During our lessons, stude resolutions, and optimizing interfaces for touch interaction. Through hands-on exercises and design projects, students will gain practical experi user feedback, and iterate on their designs to improve usability and functionality. We will also cover best practices for designing for accessibilit will be able to confidently create user-friendly interfaces for a range of mobile devices, taking into account factors such as user behavior, scree existing skills, our course will provide them with the knowledge and tools they need to succeed in the field.

Start Challenge

攻撃者が使用したコーディング学習サイトのランディングページのアーカイブ

IP アドレス 83[.]234[.]227[.]53 は、2024 年 11 月 8 日と 2024 年 11 月 29 日にポート 1224、1245、3389 で Sageskills のウェブサイト（既知の Lazarus C2 サーバー）への接続が確認されています。さらに、IP アドレス 83[.]234[.]227[.]49 も、2024 年 11 月 7 日から 2024 年 11 月 11 日にかけて、同じポートで同じサーバーに接続していたことが確認されています。

中間プロキシ

さまざまな C2 サーバーへの接続が確認されているソース IP は、トラフィックをマスクするように設計された中間プロキシのネットワークを形成しています。このレイヤーは、ISP のプロキシを利用して、接続の真の発信元を隠蔽します。

C2 サーバーへの接続が確認された IP アドレス 83[.]234[.]227[.]50 は、Oculus Proxy エンドポイントにリンクされていると見られます。同様に、83[.]234[.]227[.]49 も Oculus Proxy インフラに関連しています。攻撃者は、このインフラに 83.234.227.49 ～ 83.234.227.53 を独占的に使用しています。

こうした調査結果からは、攻撃者が Oculus Proxy ネットワーク内の特定のプロキシエンドポイントを故意に悪用し、トラフィックをさらに隠蔽していることが示唆されます。この手口は、匿名層を追加し、アトリビューションと検出の活動を複雑化し、攻撃者が監視を回避し、作戦上の安全を確保するために商業プロキシサービスを戦略的に使用していることを示しています。

Astrill VPN への接続

STRIKE は、C2 サーバーへの接続に使用された IP は単なるリレー/プロキシであり、真の発信元を難読化するために使用されたものであると確信しています。攻撃者はプロキシを使用して VPN に接続した後にセカンダリーセッションを確立していたため、実際の接続元は隠蔽されていました。

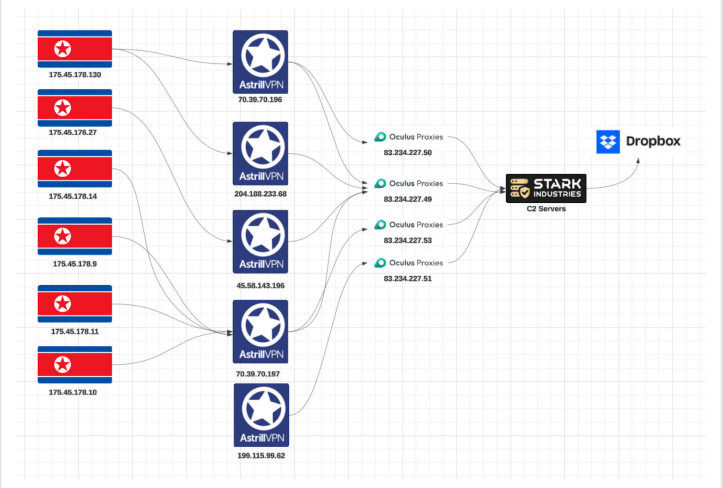
2024 年 11 月の Sageskills 攻撃において、11 月 1 日から 11 月 6 日の間、Astrill VPN の IP アドレス（70.39.70.196）から 83[.]234[.]227[.]53 への接続が確認されました。Virus Total によると、Astrill の IP アドレスは DPRK IT Worker スキームとリンクしており、当初は信頼性が低いと考えられましたが、分析の結果、Lazarus が使用する出口ポイントである可能性が高いことが分かりました。

12 月には、同じ Astrill の IP が 83[.]234[.]227[.]50 にも接続されており、C2 サーバーへの通信が確認されています。直近に検出された攻撃では、2025 年 1 月 23 日に別の Astrill VPN IP アドレスがプロキシ 83[.]234[.]227[.]53 に接続し、同日に C2 サーバー 94[.]131[.]9[.]32 に接続していることが確認されています。北朝鮮は過去に Astrill VPN を使用しており、特定の IT 労働者スキームで確認されています。

北朝鮮との接点を追跡

北朝鮮は、唯一割り当てられたアドレス空間である北朝鮮の IP 範囲 175.45.176.0/22 から Astrill VPN を大幅に使用しているものと見られます。下記は、C2 インフラの管理を目的として、ロシアでプロキシ経由のトラフィックルーティングに関与した特定の IP の分析です。

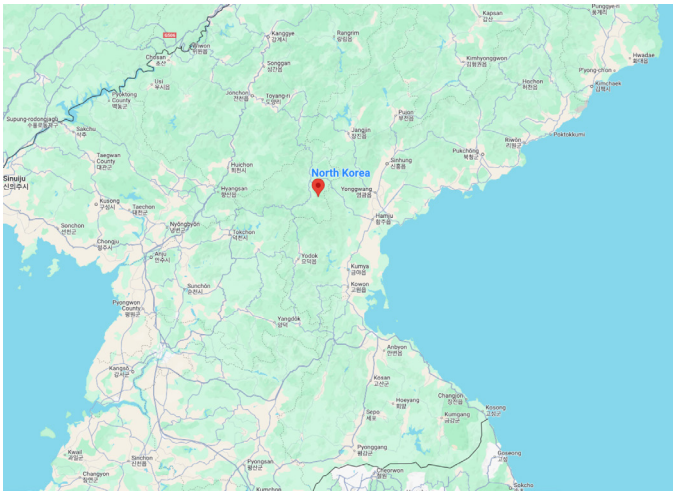
2024 年 12 月、北朝鮮の IP アドレス（175.45.178.130）が Astrill VPN（70.39.70.196）に接続していることが確認され、作戦による攻撃と C2 サーバーへの接続の時期と一致しています。注目すべき点は、2024 年 12 月 2 日、北朝鮮の IP が VPN に接続した直後、Astrill



攻撃インフラ

VPN が 83[.]234[.]227[.]49 のプロキシサーバーへの接続を確立したことです。同日、VPN は C2 サーバー（5[.]253[.]43[.]122）に接続し、北朝鮮の IP、VPN、プロキシ、C2 サーバーを結びつける明確な一連の活動を確立し、北朝鮮の IP がトラフィックの真の発信元であることを特定しました。

これらの調査結果は、作戦インフラの連携を裏付け、この攻撃の開始に北朝鮮の IP が関与していたことを示す直接的な証拠となります。北朝鮮の IP から VPN へ、プロキシを経由して最終的に C2 サーバーに接続するという時間的な整合性からは、工作活動の効率を維持しながらトラフィックの発信元を隠蔽するために、難読化層を故意に使用していることが明確にわかります。この接続パターンは、攻撃者が北朝鮮の国家レベルのアクターであることを強く裏付けるアトリビューションであり、その手口が極めて巧妙であることを示しています。



北朝鮮の推定発信源

工作インフラの時間的分析

今回確認されたサイバー攻撃は、北朝鮮によるもので、2024 年 11 月から 2025 年 1 月にかけて、コマンド アンド コントロール（C2）サーバーを管理する重要なファシリテーターとしてプロキシが使用されていることが明らかになりました。攻撃者は、83.234.227.49、83.234.227.53、83.234.227.51 などのプロキシを使用して、複数の C2 サーバーへの接続をルーティングおよび管理し、攻撃者発信のトラフィックを確実に難読化しました。これらのプロキシは仲介者となり、攻撃者のインフラを防御し、匿名性を高める役割を担っていました。この攻撃は、175.45.178.130、175.45.178.14、175.45.178.10 を含む北朝鮮の IP と直接関係しており、北朝鮮の資産（閉鎖的な国であり、閉鎖的なネットワークであるため可能性は低い）を経由して行われたか、または北朝鮮国内から直接調整されたことを示唆しています。複数のプロキシを同時に使用して異なる C2 サーバーを管理しているということは、工作活動上の安全確保とネットワーク管理に対する高度な理解があることを反映しています。

活動のピークは 2024 年 12 月で、プロキシの使用レベルが高まりました。その目的は、185.153.182.241、86.104.74.51、5.253.43.122 のサーバーを含む C2 インフラとの通信を円滑化することです。70.39.70.196 や 45.58.143.196 といった Astrill VPN の IP を使用することで、接続元をマスキングし、アトリビューションや検出をさらに複雑化しました。

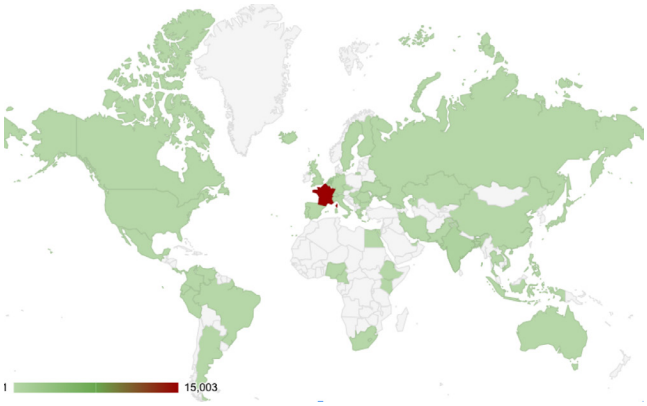
タイムラインを重複させ、地理的に分散したプロキシを通じて C2 を管理し、安全な VPN チャネルを活用する攻撃者の戦略は、レジリエンスを確保し、検出を最小限に抑えることを目的とした巧妙な作戦を示すものです。管理されたプロキシを経由して故意に通信をルーティングすることで、攻撃者が防護策を回避しながらインフラの制御を維持することを重視していることが明確になりました。

Dropbox のデータ窃取

12 月の攻撃期間中、185.153.182.241 の C2 サーバーが複数の Dropbox IP に繰り返し接続していることが確認されました。この活動は、攻撃者が窃取したデータを Dropbox のロケーションに転送している可能性が高いと考えられます。これらの接続は、C2 サーバーをクライアントとして 2024 年 12 月 4 日から 2024 年 12 月 30 日の間に発生し、総接続時間は 5 時間 14 分でした。同様のパターンは、2024 年 12 月 16 日から 2024 年 12 月 26 日の間に接続を確立した C2 サーバー 5.253.43.122 でも確認されました。この挙動は 11 月の攻撃でも確認され、86.104.74.51 の C2 サーバーが 2024 年 11 月 8 日から 2024 年 11 月 30 日まで Dropbox の IP に接続していました。さらに、同じパターンが 1 月の攻撃中に再び確認され、Dropbox IP への接続が 2025 年 1 月 17 日から 2025 年 1 月 24 日の間に発生していました。

11 月の攻撃

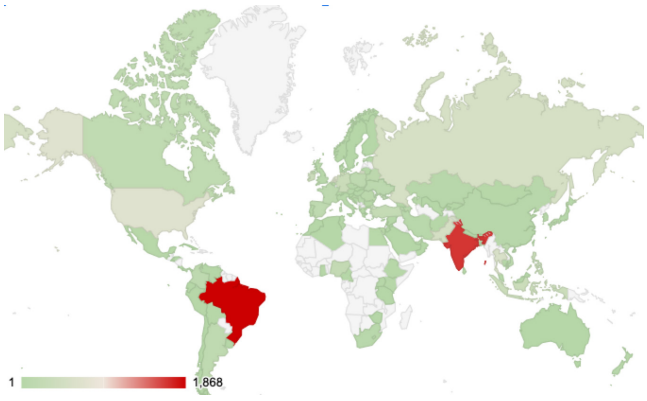
11 月の攻撃では、全世界で C2（86.104.74.51）を使用した 181 件の被害が発生しました。上記の分析と中間プロキシの役割を踏まえると、攻撃者はポート 1245 と 3389 経由でプロキシ 83.234.227.53 と 83.234.227.49 を通じてサーバーを管理していたことになります。



2024 年 11 月の攻撃による被害数（C2 への接続が行われた）

12 月の攻撃

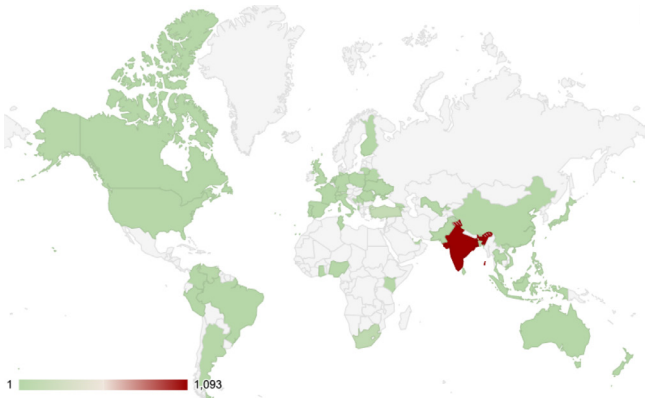
2024 年 12 月の攻撃では、3 台の C2 サーバー（185.153.182.241、45.128.52.14、86.104.74.51）で 1,225 件の被害が確認されました。ブラジル（32 件の固有 IP）とインド（284 件の固有 IP）に集中しており、C2 サーバーへのトラフィックが最も多い国となっています。



2024 年 12 月の攻撃による被害数（C2 への接続が行われた）

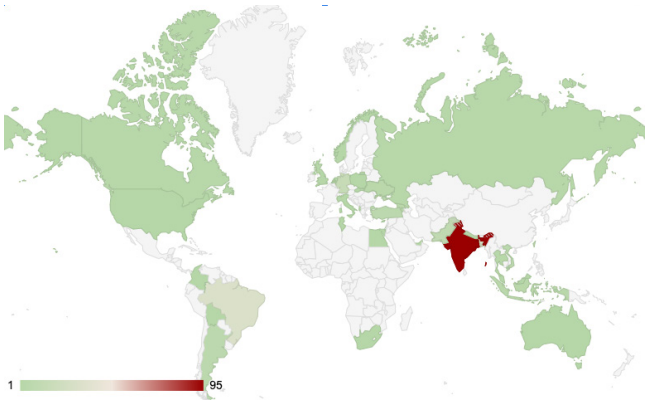
1月の攻撃の分析

最近確立されたC2サーバー（94.131.9.32）は、複数の難読化層を経由して、175.45.178.11および175.45.178.10を発信元とするトラフィックを受信しています。特に、175.45.178.11からのトラフィックは、2025年1月を通じて常にルーティングされ、Astrill VPNの出口ポイント（70.39.70.196、70.39.70.197）およびプロキシ（83.234.227.53）を経由して宛先に到達していました。94.131.9.32の関与する活動は、2025年1月21日から23日にかけてピークを迎え、これらのプロキシ経由でサーバーに大量のトラフィックが流入しました。ポート1224経由で通信を行っているこの直近の攻撃の一環として、233件の被害が発生しています。インドが最も影響を受けた国であり、この攻撃期間中に110件の被害が確認されています。



2025年1月の攻撃による被害数（C2への接続が行われた）

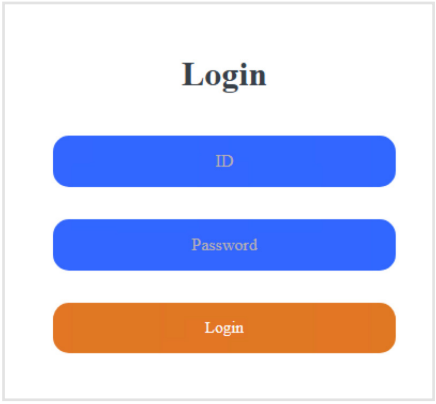
攻撃者は、同じくStark Industriesでホストされている別のサーバー（94.232.247.192）を設定し、プロキシ83.234.227.53が2025年1月23日に接続しました。本稿執筆時点で、このサーバーはもうオンラインではありません。別のプロキシ83.234.227.52は、2025年1月21日から2025年1月22日の間に、ポート1224と3389で接続を確立しました。この攻撃は短期間で終了し、インドで最も被害の大きかった87件の事例でこのサーバーと通信していました。



2025年1月の攻撃による被害数（C2への接続が行われた）

C2攻撃インフラ

分析の多くは、攻撃者の工作インフラと平壌へのアトリビューションを中心に行われてきました。しかし、これらの攻撃におけるポート1245の役割は、未解明のままとなっています。プロキシサーバーがポート1245から接続していることは明らかであり、特定の攻撃を管理している可能性を示唆しています。今回の調査で、ペイロードやダウンローダーの他に、C2サーバーは「隠蔽された」Web管理パネルもホストしていることが判明しました。調査したところ、このウェブ管理ポータルはポート1245で動作し、バックエンドへのアクセスには認証が必要なログインページが表示されていました。C2サーバーでホストされているこのパネルは、被害者から窃取したデータの表示を容易化するとともに、攻撃者に情報の検索とフィルタリング機能を提供しているものと見られます。



Reactベースの Web 管理画面ログイン

パネルはカスタムメイドで、C2 サーバーに特別に配置されていると考えられます。トラフィックパターンの分析から、攻撃者は Astrill VPN を使用し、プロキシ接続を経由して情報にアクセスしていることが示唆されています。

さらにサーバーを調査した結果、その機能と攻撃者のインターフェースについて有益な情報が得られました。今回の調査結果から、このアプリケーションは Node.js で構築され、複数の API エンドポイントを公開しており、さらに重要な情報が得られる可能性があることが判明しました。Config.js ファイルを分析することで、利用可能な API エンドポイントと、攻撃者がアクセス可能な特定のページについての詳細が得られました。

```
const api = {
    api_url : "http://94.131.9.32:1224/",
    // api_url : "http://localhost:1224/",
    login_path : "login",
    get_info : "info",
    get_allinfo: "allinfo",
    restart_server : "rSvr",
    dmup_db : "dumpsql",
    get_userInfo: "getUser",
    edit_userInfo: "editUser",
    add_user: "addUser",
    remove_user: "removeUser",
    expiredTime: 3600,
};
export default api;
```

Config.js

別のファイル App.js では、攻撃者がアクセスできる特定のページについて、さらに詳細な情報が明らかになりました。このファイルから抽出したデータは、ログインウォールに隠蔽された特定のページパスを示しています。

```
/* Layout CSS */
import "./assets/css/layout.css"
import "./assets/css/font-awesome.min.css"
/* Components PC Pages ------------------------------------------------*/
import Login from "./pages/Login/login";
import Info from "./pages/Info/info";
import AllInfo from "./pages/AllInfo/allinfo";
import UserInfo from "./pages/User/userInfo";
import EditUser from "./pages/User/edit";
import AddUser from "./pages/User/add";
import { AppContext } from './AppContext';
```

App.js

情報

情報ページには被害者に関する詳細が掲載されていますが、実際のバックエンドデータは表示できませんでした。ファイルを調査することで、その実際の機能を判断できます。JavaScript ファイルを静的に分析すると、被害者がアップロードしたデータをサーバーがバックエンドから取得していることが判明しました。これには、PC 名、URL、パスワードなど、窃取された情報が含まれます。さらに、/keys API エンドポイントと相互作用するインプラントから抽出されたデータが表示されています。

```
class info extends Component {
    constructor(props) {
        super(props);
        this.state = {
            keyDataHeader : [
                { name : 'Name', field : 'name', sortable : true },
                { name : 'Type', field : 'type', sortable : true },
                { name : 'Time', field : 'time', sortable : true }
            ],
            keyData : [],
            uploadDataHeader : [
                { name : 'PC_name', field : 'pc_name', sortable : false },
                { name : 'URL', field : 'url', sortable : true },
                { name : 'Username', field : 'username', sortable : true },
                { name : 'Password', field : 'userpwd', sortable : false },
                { name : 'Browser', field : 'browser', sortable : true },
                { name : 'created', field : 'created_time', sortable : true },
                { name : 'last', field : 'last_time', sortable : true }
            ],
            uploadData : [],
            OkeyData : [],
            OuploadData : [],
            currentPane : 'keys',
            keysnum : 5,
            uploadsnum:100,
            is_loaded:false,
        }
```

Info.js

ペイロードから送信されたデータは、バックエンドのキーテーブル内に表示されます。

```
{
    'ts': str(B),          # A timestamp in milliseconds.
    'type': sType,         # An identifier (hardcoded as "99").
    'hid': hn,             # Hostname of the system, potentially modified.
    'ss': 'sys_info',      # A label indicating system information.
    'cc': str(A.sys_info) # Serialized system and network info.
}
```

競合仮説分析（ACH）

競合仮説分析（ACH）は、所与の問題や状況について、複数の説明の可能性を評価することを目的として考案された、体系的な方法論です。元来 CIA によって開発された ACH は、アナリストがエビデンスを整理し、バイアスを特定し、競合する仮説を体系的に比較して最も可能性の高い結論を決定するうえで役立ちます。

仮説

- **H1：**この攻撃は Lazarus グループ（北朝鮮 APT）が主導しており、北朝鮮が直接関与している。
- **H2：**この攻撃は、Lazarus になりすましてアトリビューションを隠蔽しようとする非国家的アクターまたは犯罪グループによって実行されている。
- **H3：**この攻撃には、複数の国家的アクターまたは非国家的アクターが連携しており、Lazarus も一部または間接的に関与している。
- **H4：**この攻撃は Lazarus とは一切無関係で、TTP（戦術、技術、手順）が類似しているために誤認されている。

分析

- **H1（Lazarus グループの関与）：**北朝鮮の IP との直接的な関連、Lazarus の既知の TTP、インフラの使用状況、標的のパターンなど、ほとんどのエビデンスがこの仮説を強く裏付けている。STRIKE の調査は、このアトリビューションと密接に一致している。
- **H2（非国家的アクターのなりすまし）：**可能性はあるが、この攻撃の練度、規模、Lazarus の過去の活動との整合性から、このシナリオの信憑性は低い。平壌由来の IP との関連性や Astrill VPN の利用といったエビデンスは、この仮説をさらに否定するものである。
- **H3（共謀）：**この仮説は攻撃の複雑性を説明するものではあるが、Lazarus 以外の共謀者を示唆する説得力のあるエビデンスは存在しない。確認されたインフラと技術は、グループの能力と一致する一元的な活動であることを示している。
- **H4（アトリビューションの誤り）：**エビデンスの大半は Lazarus の関与を直接示しており、アトリビューションの誤りである可能性は極めて低い。一部の手法（サプライチェーン攻撃など）は理論的には模倣可能だが、平壌由来 IP と Astrill VPN の利用との明確な関連性は、この仮説に強く反している。

まとめ

- **最も可能性の高い仮説：**H1 - この攻撃は Lazarus グループ（北朝鮮 APT）が組織している。
- **信頼度：**高

まとめ

Operation Phantom Circuit によって、サプライチェーン攻撃を通じて暗号通貨業界とソフトウェア開発者を標的にした、Lazarus による極めて巧妙な世界規模の攻撃が明らかになりました。正規のソフトウェアパッケージに難読化されたバックドアを埋め込むことで、Lazarus はユーザーを騙して侵害されたアプリケーションを実行させ、1224 ポートのコマンド・アンド・コントロール（C2）サーバーを通じて機密データの窃取や感染端末の管理を可能にしました。この攻撃のインフラは、窃取されたデータを一元管理するために、隠蔽された React ベースの Web 管理パネルと Node.js API を悪用しており、世界全体で 233 件以上の被害が発生していました。この窃取されたデータは、Astrill VPN と中間プロキシによる多層化されたネットワークを通じて、北朝鮮の平壌まで遡って追跡されました。

今回の攻撃は、組織や開発者に対し、厳格なコード検証プロセスやネットワークトラフィックの監視を実施し、サプライチェーンのセキュリティを強化するよう緊急に求めるものです。セキュリティチームは、グローバルに連携して脅威インテリジェンスを共有し、最新の Web 技術と高度な難読化手法を駆使する Lazarus の進化する手口に先手を打って対応する必要があります。特に暗号通貨業界のようなリスクの高い業界は、高度な脅威アクターからの将来的な攻撃を回避するために、堅牢な監視ツールの採用、パッチ管理の徹底、予防的防御の導入を優先する必要があり、直ちに対応しなければなりません。こうした脆弱性への対処を怠ると、重要なシステムやデータが同様の攻撃を受けることになります。

インシデント対応に関する STRIKE への問い合わせ

自社が Operation Phantom Circuit、Operation 99、または類似の Lazarus の攻撃による影響を受けていると思われる場合は、直ちに STRIKE 戦略情報チーム（investigations@securityscorecard.io）までご連絡ください。STRIKE の専門家が次のように対応します。

- **迅速な封じ込め：**被害を最小限に抑え、進行中の侵害を阻止します。
- **フォレンジック分析：**攻撃者のアクセス経路と影響を受けたデータを把握します。
- **戦略的インテリジェンス：**進化し続ける脅威に対するセキュリティ体制を強化します。

サプライチェーンのリスクを未然に軽減

将来のサプライチェーン攻撃から組織を守るため、SecurityScorecard のサプライチェーン検出・対応（SCDR）ソリューションには、次のようなツールが用意されています。

- ソフトウェアサプライチェーンの脆弱性を監視し、評価する。
- 開発パイプライン全体の不審な活動を検出する。
- 「Phantom Circuit」のような高度な脅威を防ぐための実用的な知見を得る。

今すぐサプライチェーンのセキュリティを管理しましょう。SCDR およびインシデント対応サービスの詳細については、弊社までお問い合わせください。

STRIKE に関する取材・報道関係のお問い合わせはこちらから受け付けております。