包囲されるエッジ：国家背景の攻撃者はいかに境界を悪用するか

2026-04-20

付録

付録 A：Ivanti Connect 悪用に関するケーススタディ

Ivanti Connect Secure は 2021 年以降繰り返し標的とされており、18 か月のあいだに 4 件の主要な攻撃キャンペーンが発生しています。世界で約 33,000 台が稼働し、企業および政府機関に集中していることに加え、LDAP/AD との直接統合を備えているため、1 台の侵害されたデバイスから即座にネットワークアクセスが可能となります。

CVE-2025-22457 は、X-Forwarded-For ヘッダー処理におけるスタックベースのバッファオーバーフロー脆弱性です。CVSS スコアは 9.0 で、22.7R2.6 より前のバージョンに影響し、認証なしの RCE を可能にします。2025 年 2 月 11 日にパッチが提供されました。UNC5221 は、パッチ提供から約 3〜4 週間後の 3 月中旬にエクスプロイトを開始しました。Mandiant は 4 月 3 日にアドバイザリを公表しています。

UNC5221 は Ivanti での持続化のために専用ツール群を展開しており、これは SPAWN マルウェアエコシステムとして知られています。下表に主要な構成要素を示します。

コンポーネント	機能	SHA-256
SpawnMole	SOCKS5 トンネラー、TLS 証明書のインジェクション、マジックバイトによる起動	`a3dbcc9d4e1dd523f2848689f7e0753465de6188cfac4d3a52389ab1ec3db83`
SpawnSnail	トロイの木馬化された SSH バックドア、root 権限	`4d7f4c330cdb4c16de4327b1b82f3cbe53d20c117fffc972a2d3a47e01e0a65f`
SpawnAnt	インストーラ／アップデーター、他のコンポーネントを再展開	`6f7e2148a5d20c17780a80e9bc9a1982f80820d5340a77e11beed940124eadd7`
SpawnSloth	選択的なログ消去、タイムスタンプの改ざん	`749cf36adc5513c92c7acc836d20935e3c433f3c2d5641293e7a9c57c5ce22c2`

表 1. Spawn ファミリーのコンポーネント

SpawnMole は Ivanti の web サーバプロセスにフックし、TLS ハンドシェイク関数にパッチを当てます。Client Hello 内に `0x17 0x03 0x03 0x48 0x4F 0x4F 0x4B`（`HOOK`）というマジックバイトを検知すると、接続を `localhost:447` 上の SpawnSnail へリダイレクトします。組み込まれた自己署名証明書 `CN=QcCpIAsFy6cEI` によって、攻撃者を認証します。

証明書の SHA-256：

```
761bedf645f2dfc7c06538194da8149985394419335694a73b4bd023d58bfd91
```

SpawnMole の証明書を用いた証明書ベースのピボッティングにより、CVE-2025-0282 が公表される 6 か月前の 2024 年 7 月に初めて観測された侵害済みホスト 2 台が特定されました。これは、それ以前から未知のゼロデイが存在していたか、もしくは攻撃者のテストインフラが存在していた可能性を示唆しています。侵入後、攻撃者はアクセス権を確保するために迅速に行動します。

- **資格情報の窃取：** UNC5330 は LDAP バインド資格情報を窃取し、ドメイン管理者へ権限昇格を行いました。
- **横展開：** FRP を展開し、外向き HTTPS を介して内部の RDP（`3389`）および SMB（`445`）を公開しました。
- **データの持ち出し：** 独自フレームワークが SSO クッキーを窃取し、MFA を回避して内部アプリケーションへアクセスしました。

以下の指標は、SPAWN エコシステムの活動を検知するために利用できます。

ファイルハッシュ

```
a3dbcc9d4e1dd523f2848689f7e0753465de6188cfac4d3a52389ab1ec3db836
4d7f4c330cdb4c16de4327b1b82f3cbe53d20c117fffc972a2d3a47e01e0a65f
6f7e2148a5d20c17780a80e9bc9a1982f80820d5340a77e11beed940124eadd7
749cf36adc5513c92c7acc836d20935e3c433f3c2d5641293e7a9c57c5ce22c2
c64f695e9e0855699d9e77790a56848b05b18390e8976815bcc1394a2aea6087
```

Webshell キー

```
ACcSPn2ZxBvmMapuTQJLezyFD3rbsqlO
```

関連コンポーネントおよび暗号関連情報

```
SpawnMole
SpawnSnail
SpawnArt
SpawnSloth
RC4
```

証明書フィンガープリント

```
SHA-256: 761bedf645f2dfc7c06538194da8149985394419335694a73b4bd023d58bfd91
SHA-1:   c91c787c0a9d81faf149d3aa53ceab9fcabb3c20
```

ネットワーク指標

```
TLS magic bytes: 0x17 0x03 0x03 0x48 0x4F 0x4F 0x4B
Non-standard SSH ports: 447, 8447
Fast Reverse Proxy (FRP) infrastructure
```

ファイルパス

```
/lib/libsecure.so.1                      # SpawnSnail
/lib/libdsproxy.so                       # SpawnMole variant
/lib/libdsplibs.so                       # SpawnMole variant
/lib/libupgrade.so                       # SpawnAnt
/data/runtime/scripts/checkintegrity.sh  # Modified script
```

付録 B：脆弱性ブローカーの価格設定

TrendAI の ZDI は、2005 年以来、世界最大のベンダー中立型バグバウンティプログラムを運営しており、独立系研究者から数千件の脆弱性を購入し、影響を受けるベンダーへの協調的脆弱性開示を主導してきました。20 年以上にわたり、ZDI はほぼすべてのソフトウェア・ハードウェアカテゴリにわたって数千万ドル規模の支払いを行ってきました。これにより TrendAI は、透明かつ合法的な市場において脆弱性が真にどの程度の価値を持つのかを直接かつ第一級の視点で把握できます。

市場データは、なぜエッジデバイスが国家背景のサイバースパイ活動において優先的な標的となったのかを示す重要なストーリーを語っています。ZDI が毎年開催する Pwn2Own コンペティションは、研究者が完全にパッチ適用されたデバイスを賞金をかけて攻撃する競技であり、カテゴリ別の脆弱性価値について最も透明性の高い公開ベンチマークを提供します。これらの数値を、並行して運営される攻撃用エクスプロイト調達市場の価格と並べると、構造的な異常が浮き彫りになります。すなわち、エッジデバイスの脆弱性は、それが提供する戦略的アクセスに対して著しく過小評価されています。

本付録では、その価格状況を以下の 4 つの市場セグメントにわたって整理します。

- 中国の国家主導の国内市場
- 西側の非防御目的のエクスプロイト購入ブローカー
- ロシアの国家系調達
- ZDI 自身の協調的脆弱性開示によるベンチマーク

これらを総合すると、コスト意識の高い国家アクターにとって、なぜエッジデバイスのエクスプロイトが第一選択のツールとなったのかが見えてきます。すなわち、使い捨てにできるほど手頃でありながら、勝利を収めるに足る価値を備えているからです。

Nvwa（女娲）

出典: `https://web.archive.org/web/20250227080447/https://nvwa.org/`

中国ではかつてオープンな脆弱性購入プログラムが運営されていましたが、近年の規制変更により、その多くは公の場から姿を消しました。Nvwa（女娲）プロジェクトのウェブサイト `nvwa.org` に残された過去のデータからは価格設定の状況を読み取ることができ、カテゴリ別の詳細価格が示されています。これにより、エッジデバイスの脆弱性がエンドポイント向けエクスプロイトに比べて大幅に安価であったことが裏付けられます。

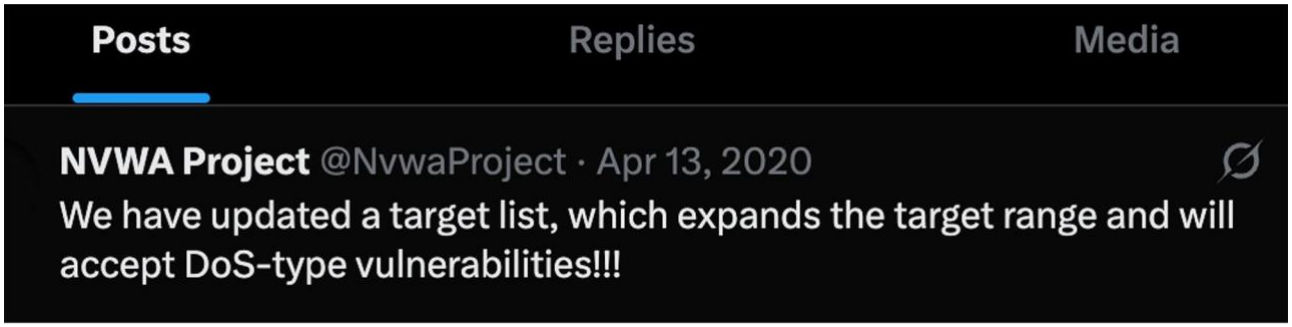

図 1. Nvwa プロジェクトが 2020 年に活動していたことを示すソーシャルメディア投稿

F5	-	RCE	Zero-Click	2020-09-04	∞	500,000
F5 BIG-IP	-	RCE	Zero-Click	2021-01-05	∞	500,000
Fastjson	-	RCE	Zero-Click	2021-01-05	∞	500,000
Firefox	-	RCE+LPE	Zero-Click	2019-11-01	∞	800,000
FortiGate	-	RCE	Zero-Click	2020-08-07	∞	350,000
Fortigate-Firewall	-	RCE	Zero-Click	2019-11-08	∞	800,000
FortiNet	-	RCE	Zero-Click	2020-09-04	∞	350,000
Fortinet(飞塔) Firewall	-	RCE	Zero-Click	2021-01-05	∞	50,000
Foxit	-	RCE+LPE	1-Click	2020-09-04	∞	500,000
FreeBSD	-	LPE	Zero-Click	2020-08-07	∞	500,000

図 2. 現在は閉鎖された Nvwa ウェブサイトのアーカイブ済みスクリーンショット

中国の価格設定を文脈に位置付けるため、本報告書ではグローバルな脆弱性市場を調査しました。以下の内訳は、2026 年初頭時点で公開されている複数プログラムの価格表から集計したものです。

Crowdfense Exploit Acquisition Program

Crowdfense は UAE を拠点とするハイエンドのエクスプロイトブローカーです。Crowdfense はゼロデイエクスプロイトを購入し、機関投資家グループに販売しています。その価格設定は、エッジデバイスの脆弱性が他のエクスプロイトに比べて大幅に低い価格で取引されていることを裏付けています。

モバイル

対象カテゴリ	価格帯
iOS ゼロクリック フルチェーン（iMessage）	5,000,000〜7,000,000 米ドル
Android ゼロクリック フルチェーン（WhatsApp、RCS）	5,000,000 米ドル
Chrome ワンクリック フルチェーン（RCE+SBX+LPE）	2,000,000〜3,000,000 米ドル
Safari ワンクリック フルチェーン（RCE+SBX+LPE）	2,500,000〜3,500,000 米ドル

表 2. モバイル、最大 700 万米ドル

デスクトップ

対象カテゴリ	価格帯
Windows ゼロクリック フルチェーン	1,000,000 米ドル
Chrome フルチェーン（デスクトップ）	1,500,000 米ドル
Firefox フルチェーン	300,000 米ドル

対象カテゴリ	価格帯
Word/Excel RCE	500,000 米ドル
Outlook RCE	300,000 米ドル
Windows LPE	100,000 米ドル
Linux LPE	100,000 米ドル

表 3. デスクトップ、最大 150 万米ドル

ルーター、ファイアウォール、エッジアプライアンス

対象カテゴリ	価格帯
Cisco RCE	100,000 米ドル
Fortinet RCE	100,000 米ドル
Citrix RCE	100,000 米ドル
SonicWall RCE	100,000 米ドル
MikroTik RCE	100,000 米ドル
Huawei RCE	100,000 米ドル
Sophos RCE	100,000 米ドル
Juniper RCE	75,000 米ドル
D-Link / TP-Link / Netgear RCE	50,000 米ドル
Ubiquiti RCE	50,000 米ドル

表 4. ルーター、ファイアウォール、エッジアプライアンス、最大 10 万米ドル

エンタープライズソフトウェア

対象カテゴリ	価格帯
Apache HTTP Server RCE	500,000 米ドル
Microsoft IIS RCE	500,000 米ドル
WordPress RCE	500,000 米ドル
Microsoft Exchange RCE	250,000 米ドル

対象カテゴリ	価格帯
Microsoft SharePoint RCE	250,000 米ドル
SAP RCE	250,000 米ドル
VMware ESXi / Hyper-V エスケープ	500,000 米ドル

表 5. エンタープライズソフトウェア

その他の注目すべき項目として、Ivanti、Zyxel VPN Firewall、WatchGuard、pfSense、F5 Big-IP、KerioControl が挙げられます。これらはリストに掲載されているものの、公開価格は示されていません。

Zerodium の過去の参考価格

Zerodium は、完全なゼロデイ価格表を初めて公開した企業です。最後に公開された価格設定でも、エッジデバイスのエクスプロイトがモバイル向けエクスプロイトに比べて大幅に安価であることが示されていました。

対象カテゴリ	価格帯
Android ゼロクリック フルチェーン＋持続化	2,500,000 米ドル
iOS ゼロクリック フルチェーン	2,000,000 米ドル
WhatsApp/iMessage RCE+LPE（ゼロクリック）	1,500,000 米ドル
Windows RCE（ゼロクリック）	1,000,000 米ドル
Chrome RCE（フルチェーン）	500,000 米ドル
Apache/IIS/Nginx RCE	200,000〜500,000 米ドル

表 6. Zerodium の過去の参考価格

Zero Day Initiative（ZDI）：TrendAI による協調的脆弱性開示プログラム

ZDI は世界最大のベンダー中立型バグバウンティプログラムであり、TrendAI が 2015 年から運営しています。Zerodium や Crowdfense とは異なり、ZDI は協調的脆弱性開示プログラムです。脆弱性は影響を受けるベンダーに報告され、公表前にパッチが適用されます。ZDI は他者へエクスプロイトを販売することはありません。

比較に際して重要な留意点として、ZDI の支払額は構造的に非防御目的のブローカーよりも低くなっています。これは、研究者が即時の支払額と引き換えに、ベンダーへの通知、パッチ調整、公的なクレジット付与といった協調的開示を選んでいるためです。Crowdfense のような非防御目的のブローカーがプレミアムを支払うのは、まさに脆弱性が秘匿され武器化可能な状態に保たれるからです。

ZDI は固定の価格表を公開していません。支払額は以下に基づいて個別に評価されます。

- 製品の導入規模と重要性。たとえばデータベース、ルーター、ファイアウォールは高価値とみなされます。
- 深刻度と悪用可能性。認証なしの RCE には最高額の支払いが設定されます。
- デフォルト構成での露出度。
- ソーシャルエンジニアリングが必要かどうか。

価格指標としての Pwn2Own

ZDI が毎年開催する Pwn2Own コンペティションは、ZDI が特定カテゴリをどのように評価しているかを示す、最も透明性の高い公開シグナルを提供します。これらは競技賞金であり、通常の購入価格ではありませんが、ZDI 内部の評価モデルを反映しています。

PWN2OWN IRELAND 2024：コンシューマー／SOHO 中心

対象カテゴリ	価格帯
SOHO Smashup（ルーター＋NAS の連鎖、9 件の脆弱性連鎖）	100,000 米ドル
SOHO Smashup（ルーター＋NAS の連鎖、単一チーム）	50,000 米ドル
SOHO Smashup カテゴリ賞	25,000 米ドル
個別の NAS デバイスエクスプロイト（QNAP、Synology、TrueNAS）	3,000～25,000 米ドル
個別のルーターエクスプロイト	3,000～25,000 米ドル
プリンターエクスプロイト（Canon、Lexmark）	3,000～10,000 米ドル
カメラエクスプロイト（Lorex）	3,000～5,000 米ドル

表 7. Pwn2Own Ireland 2024、コンシューマー／SOHO 中心、賞金総額 1,066,625 米ドル

PWN2OWN TORONTO 2023：コンシューマー／SOHO 中心

対象カテゴリ	価格帯
SOHO Smashup（30 分以内にルーター＋NAS）	100,000 米ドル
モバイル端末のフルチェーン（iPhone/Pixel、カーネルレベル）	250,000 米ドル
NAS デバイスエクスプロイト	5,000～40,000 米ドル
プリンターエクスプロイト	5,000～20,000 米ドル
スマートスピーカーエクスプロイト	5,000～20,000 米ドル

表 8. Pwn2Own Toronto 2023、コンシューマー／SOHO 中心、賞金総額約 1,000,000 米ドル

PWN2OWN VANCOUVER 2024：エンタープライズ／デスクトップ中心

対象カテゴリ	価格帯
ブラウザのフルチェーン（Chrome、Safari、Firefox）	85,000〜200,000 米ドル
Windows カーネルでの権限昇格	30,000〜90,000 米ドル
VMware ESXi/Workstation エスケープ	150,000〜250,000 米ドル
Tesla インフォテインメント	100,000〜200,000 米ドル

表 9. Pwn2Own Vancouver 2024、エンタープライズ／デスクトップ中心、賞金総額 1,132,500 米ドル

ZDI と非防御目的ブローカーの比較：本質的な違い

ZDI の価格は、協調的脆弱性開示の文脈においてエッジデバイスや SOHO 脆弱性が持つ倫理的な底値を反映しています。ZDI に脆弱性を売却することの大きな利点の一つは、売却した情報が厳格に倫理的な方法で利用されるという保証です。たとえば ZDI は、ベンダーによる緩和策の調整や協調的脆弱性開示の責任をしばしば自ら担います。

一方、Crowdfense のようなブローカーは同じ Cisco や Fortinet の RCE に対して最大 10 万米ドルを支払いますが、これは秘匿され武器化可能な状態のエクスプロイトを購入する価格です。これらのサービスを利用する顧客にとっての真の運用上の価値ははるかに高く、世界中で数百の被害組織に対して単一のエッジデバイスのエクスプロイトを使い回したキャンペーンが、それを実証しています。

下表の比較は、ZDI が Pwn2Own で SOHO およびエッジデバイスに付与する賞金（3,000〜100,000 米ドル）が、Crowdfense の購入価格（50,000〜100,000 米ドル）を下回ることを示しています。とはいえ、この結果は市場全体のパターンを裏付けるものです。

対象	ZDI Pwn2Own 賞金	Crowdfense 購入価格	差
エンタープライズ向けファイアウォール／ルーターの RCE（Cisco、Fortinet）	Pwn2Own 対象外	100,000 米ドル	比較不能
SOHO ルーターの RCE（D-Link、Netgear、QNAP）	3,000〜25,000 米ドル	50,000 米ドル	約 2〜5 倍
連鎖型 SOHO 攻撃（ルーター＋NAS）	25,000〜100,000 米ドル	個別記載なし	比較不能
モバイル OS のフルチェーン	150,000〜250,000 米ドル（競技）	5,000,000〜7,000,000 米ドル	約 20〜40 倍

表 10. ZDI Pwn2Own 賞金と Crowdfense 購入価格の比較

非防御目的のブローカーがモバイルに対して Pwn2Own を上回って支払う 20〜40 倍のプレミアムを、SOHO およびエッジデバイスにおける 2〜5 倍のプレミアムと対比すると、エッジデバイスがその戦略的価

値に対して過小評価されていることがさらに裏付けられます。これにより、エッジデバイスは国家背景の購入者にとって特に魅力的な対象となっています。

付録 C：漏洩したワークステーションの分析

2025 年 8 月、Phrack Magazine 第 72 号 第 7 記事において、侵害された攻撃者のワークステーションに関する分析が公表されました。同記事では、その攻撃者を北朝鮮系のグループ Kimsuky に帰属させていました。その後の Intel471、S2W、ならびに TrendAI 自身の調査では、同攻撃者はむしろ中国系であり、撹乱目的で DPRK の戦術・技術・手順（TTPs）を模倣している可能性が高いことが示されています。

中国系であることを示す証拠には、以下のようなものがあります。

- 翻訳ツールを介さずに簡体字中国語が広範に使用されていたこと。
- Baidu、CSDN、Freebuf、FOFA をはじめとする中国系サービスへの強い依存。
- 中国の祝日には活動がなく、北朝鮮の祝日には顕著な活動が見られたこと。
- Great Firewall 回避のため Apple の TLS プロキシを利用しており、出口ノードが台湾に存在していたこと。
- UNC5221 の活動と一致する Ivanti のエクスプロイトツールを保有していたこと。
- 中国系グループとの関連が知られている非公開ツールやエクスプロイトコードを使用していたこと。

対象マシン上では、以下のツールが見つかりました。

- **エクスプロイト開発：** IDA Pro 8.3、Ghidra、およびコード変換・解析向けの LLM／AI 搭載ツール。
- **カスタムマルウェア：** SpawnAnt、SpawnMole、SpawnSnail、SpawnSloth を含む SPAWN エコシステムの構成要素、Ivanti 特化の rootrot（Perl ベースの Webshell）、および Ivanti の `web` バイナリ向けホットパッチフレームワーク。
- **ルートキット：** 閲覧履歴の分析から、複数のオープンソースルートキットへの関心が確認されました。加えて、これまでどの攻撃者にも帰属が確認されていなかったカスタム `syslogk` ルートキットのソースコードも見つかりました。
- **C&C およびトンネリング：** Kharon および Velkor エージェントを含む Mythic フレームワーク、Havoc、SNIPROXY、FRP、ならびに独自の SOCKS 実装。
- **Anti-EDR：** 特定の EDR 製品向けのテストフレームワーク、およびカスタム Cobalt Strike モジュール。

標的には以下が含まれていました。

- **韓国：** 韓国国内の Ivanti デバイスに対する広範な FOFA 検索、韓国の標的に関連する複数のデータセット・ソースコード・データ、韓国の被害者向けに調整されたフィッシングツール、および通信セクターへの関心が証拠として確認されました。
- **台湾：** 台湾の IP およびドメインに対するログイン試行、ならびに台湾国内の FortiGate デバイスに対する FOFA 検索が証拠として確認されました。

漏洩したデータは、エッジデバイスが戦略的な侵入口であることを裏付けています。データに含まれていたツールキットは、エッジデバイスの侵害向けに明示的に設計されたものでした。オープンソースとカスタムツールが混在していることは、リソースに制約があることを示唆しており、エッジ向けエクスプロイトは初

期侵入のための使い捨て資産として扱われています。偵察活動は機会主義的ではなく体系的であり、標的の選定は中国系の戦略的諜報優先事項と整合しています。

ワークフローにおける AI ツールの早期導入

もう一つ注目すべき発見は、攻撃者の閲覧履歴の調査結果であり、攻撃者が AI および AI 搭載ツールを高水準で導入していることが明らかになりました。2025 年の時点ですでに、攻撃者はワークフロー全体を通じて多様な AI 搭載プラットフォームを利用していることが観測されています。

特筆すべき点として、攻撃者は `codeconvert.ai` や `syntha.ai` といったコード変換ツールを多用しており、Rust→C、Rust→C++、Golang→C、Golang→Python、Assembly→C といった言語ペアを集中的に対象としていました。これは、ツール群を複数の言語にわたって移植・変換しようとする能動的な取り組みを示唆しています。この手法は、マルウェアのリツール化や、言語固有の検知シグネチャを回避する目的と整合します。

これらに加えて、攻撃者は `blackbox.ai`、`code-mentor.ai`、`sourcery.ai` といった AI 支援型開発プラットフォームを、コードレビューや対話的なコーディング指南に利用していることが観測されました。これは、機械的な変換だけでなく、反復的な開発やデバッグ支援にも AI へ依存していることを示唆しています。

また攻撃者は、`deepseek.chat`、`deepai.org`、`yeschat.ai` をはじめとする複数のチャットボットサービスといった汎用 AI チャットプラットフォームに加え、`zhuanzhi.ai` や `toolify.ai` のようなリサーチ・発見ツールも利用していました。これは、初期調査、ツールの発見、コード開発から最終的なペイロード準備に至るまで、AI が攻撃者の運用ワークフロー全体に幅広く統合されつつあることをさらに示唆しています。

参考文献

1. Censys. (2026). *Censys | The Authority for Internet Intelligence and Insights*. 2026 年 4 月 4 日アクセス。
2. NUWA Project. (n.d.). *NUWA Project*. 2026 年 4 月 4 日アクセス。
3. NVWA Project [@NvwaProject]. (Apr. 13, 2020). *NVWA Project*. 2026 年 4 月 4 日アクセス。
4. Crowdfense. (n.d.). *Exploit Acquisition Program*. 2026 年 4 月 4 日アクセス。
5. Zerodium. (n.d.). *Zerodium*. 2026 年 4 月 4 日アクセス。
6. TrendAI Zero Day Initiative (ZDI). (n.d.). *Program Benefits*. 2026 年 4 月 4 日アクセス。
7. Intel 471. (Sep. 5, 2025). *The Phrack leak: Examining an APT's workstation*. 2026 年 4 月 4 日アクセス。
8. S2W Inc. (Aug. 22, 2025). *Detailed Analysis of Phrack's APT Down: The North Korea Files*. 2026 年 4 月 4 日アクセス。

TrendAI™

TrendAI™は、グローバルな AI セキュリティのリーダーであり、Trend Micro のエンタープライズ事業ユニットとして、AI に対する完全な可視性と、信頼を醸成し、イノベーションを推進し、リスクを排除する統合セキュリティを組織に提供します。

185 か国にわたる大手企業や政府機関から信頼を得ている TrendAI™は、アイデンティティからインフラ、データに至るまで、組織全体を保護します。

AI Fearlessly.

詳細はこちら: **https://trendaisecurity.com/ja/**