KELA INTELLIGENCE BRIEFING

インフォスティーラーによるアカウント侵害の実態とスティーラーログ解析によるサイバー犯罪者の活動の可視化

KELA株式会社
Principal Security Engineer, CISSP
川崎　真

TLP: Amber

Date: February 2026

自己紹介

KELA株式会社
Principal Security Engineer, CISSP
川崎　真

2020年11月入社：イスラエル脅威インテリジェンスベンダー**KELA**における国内のお客様の脅威インテリジェンスサービスの利活用を支援

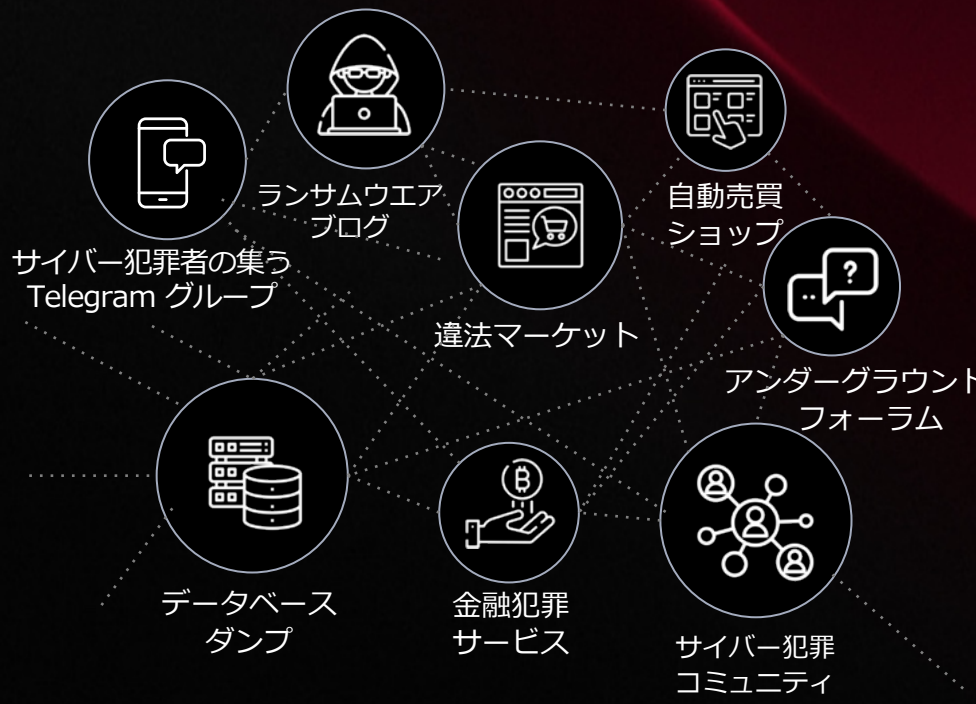
経歴
英CTIベンダー Digital Shadows: カントリーマネージャ
Websense / Forcepoint：日本地域責任者
Symantec: DLP/暗号化製品営業マネージャ
VMware：日本法人立上げ時期 チャネル開拓責任者
APC（現在Schnider）：代理店営業責任者
など

KELA

デジタル犯罪を阻止するインテリジェンス

KELAは到達困難なアンダーグラウンド空間を詳細に把握、隠れた脅威を顕在化・抑制します。

アンダーグラウンドに広がる
サイバー犯罪のエコシステム



KELAサイバーインテリジェンス
プラットフォーム

**ノイズの少ない
インテリジェンス**

背景情報を取り入れた
サイバーインテリジェンス

検証済みのノイズフリーな
脅威アラート

全ての外部アタック
サーフェスを可視化

KELA

本セッションの内容

前半パート

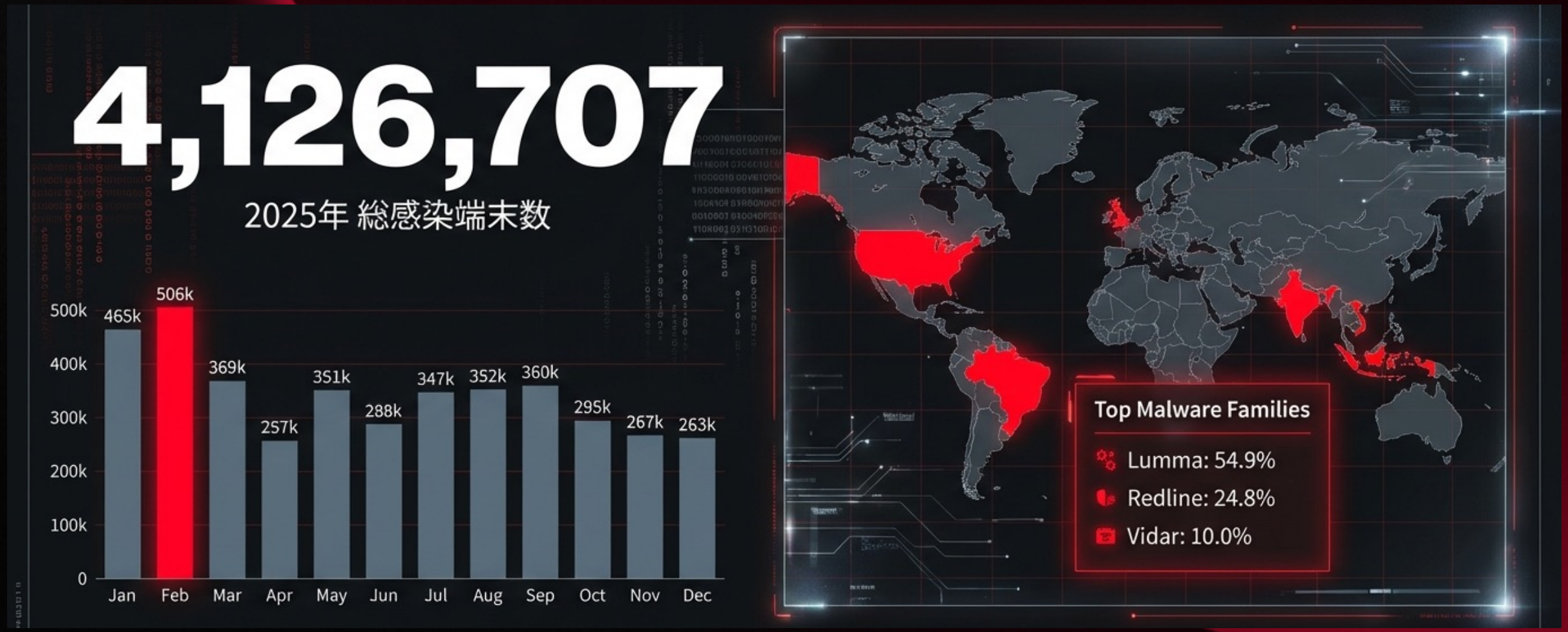
- 2025年のインフォスティーラー被害状況概況
- 生成AIの活用による新たな脅威動向

後半パート

- インフォスティーラーに感染した脅威アクターをハッキングしてみた
  1. JLR社を侵害したアクターReyの素性を暴く
  2. 北朝鮮IT労働者の日本国内での活動の痕跡を探る

KELA

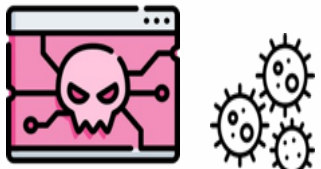
2025年のインフォスティーラー感染状況



KELAデータレイク収集数をベースにカウント：
最も趨勢をほこるLummaのオペレーションが3月に当局によりテイクダウンにされ一時的に減少したが、その後再度増加した。

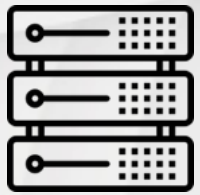
おさらい：インフォスティーラー（情報窃取マルウェア）

1. 攻撃者は、①スピアフィッシングで悪質な添付ファイルを送付、②チートツールを装うなどして不特定多数に配布、インストールさせ、PCをマルウェアに感染させる



4.1′ ①のスピアフィッシングでの攻撃では攻撃者が窃取した情報を自身で悪用。

“Logs”
zip File



C2 Server

3. マルウェアは収集した情報(Logs)をZipファイルにまとめて、攻撃者は用意したC2サーバでZipファイルを回収する。

Forums
& IM Platforms

4.2′ ②のばらまき型の場合は、窃取した情報を闇マーケットやテレグラムチャネルで販売し収益化する

マーケットを利用する
サイバー犯罪者たち

5. 闇マーケットやテレグラムで入手された情報(Logs)は、

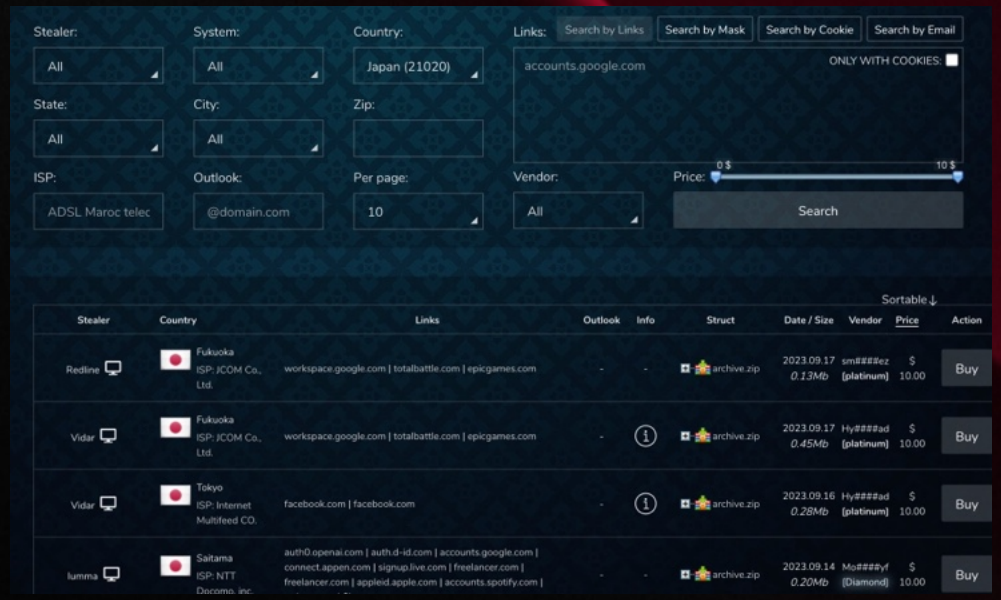
- 金融口座での不正な送金、売買
- 各種ポイント、サービスの不正売買
- ランサムウェアの初期アクセス
- サイバースパイ活動

などに悪用される

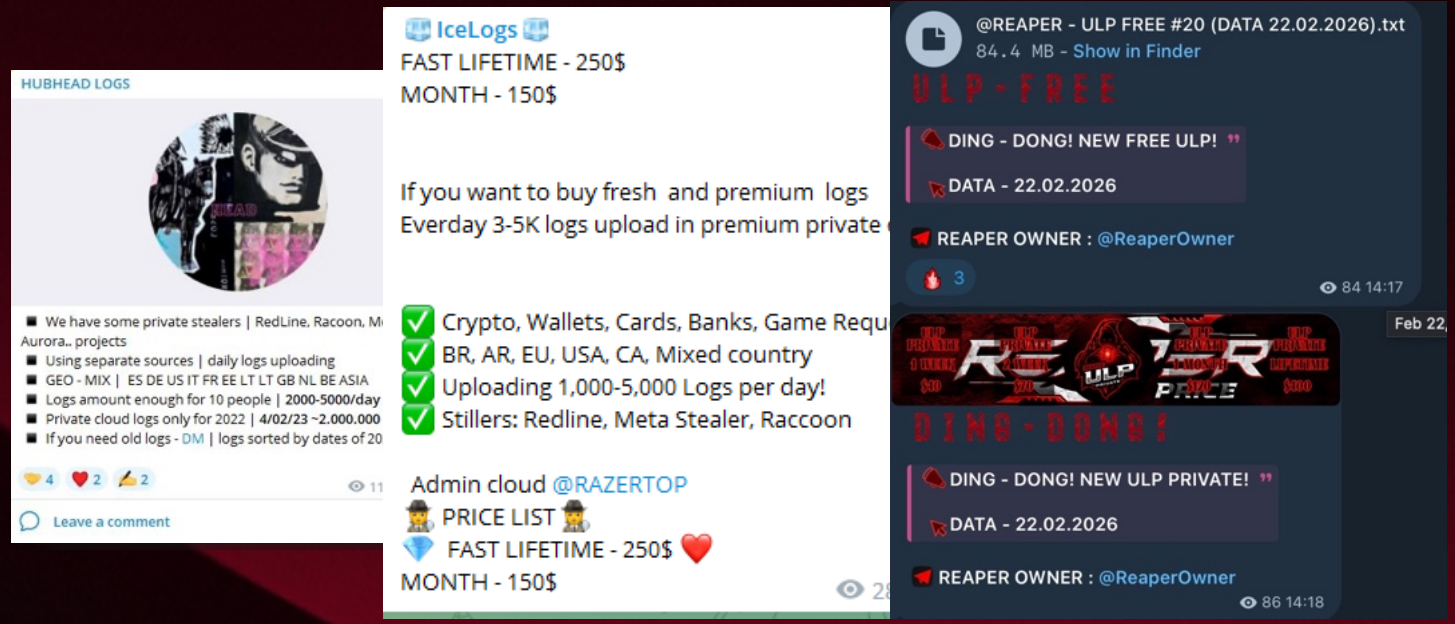
2. 感染したPCのブラウザに保存されたログイン情報、Cookie、その他カード番号やWallet情報などがマルウェアに収集される

KELA

闇マーケットやTelegramグループで販売されるスティーラーからの認証情報



ダークウェブで展開される違法なマーケットサイト。購入者は、窃取されたPCの国や、アクセス先ドメインなど様々なフィルタで目的の情報を選べる。価格は１台あたり１０米ドルが相場。



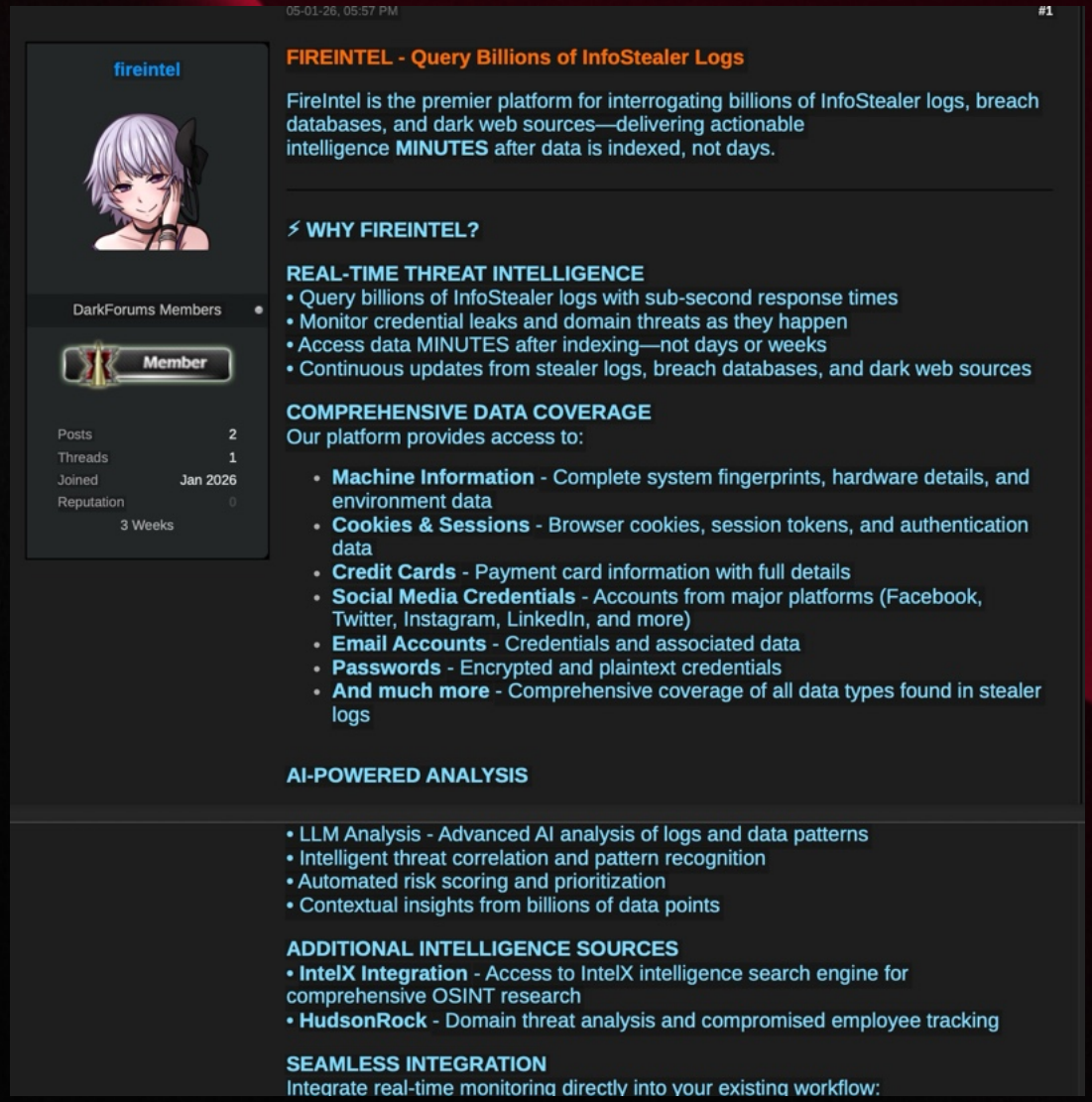
脅威アクターは、より手軽な販売チャネルとしてテレグラムを利用、2022年頃から多数のスティーラーログ販売チャネルやULPファイル共有チャネルが出現している。

月150ドルで、３万～10万の被害PCのログをバルクで入手できる。

多くの金融系サイトではMFA、パスキーの導入が進み、不正ログイン対策は進みつつある

KELA

生成AI・LLMによる解析サービスの登場



05-01-26, 05:57 PM #1

fireintel

DarkForums Members

Member

Posts 2
Threads 1
Joined Jan 2026
Reputation 0
3 Weeks

FIREINTEL - Query Billions of InfoStealer Logs

FireIntel is the premier platform for interrogating billions of InfoStealer logs, breach databases, and dark web sources—delivering actionable intelligence **MINUTES** after data is indexed, not days.

⚡ WHY FIREINTEL?

REAL-TIME THREAT INTELLIGENCE
- Query billions of InfoStealer logs with sub-second response times
- Monitor credential leaks and domain threats as they happen
- Access data MINUTES after indexing—not days or weeks
- Continuous updates from stealer logs, breach databases, and dark web sources

COMPREHENSIVE DATA COVERAGE
Our platform provides access to:

- **Machine Information** - Complete system fingerprints, hardware details, and environment data
- **Cookies & Sessions** - Browser cookies, session tokens, and authentication data
- **Credit Cards** - Payment card information with full details
- **Social Media Credentials** - Accounts from major platforms (Facebook, Twitter, Instagram, LinkedIn, and more)
- **Email Accounts** - Credentials and associated data
- **Passwords** - Encrypted and plaintext credentials
- **And much more** - Comprehensive coverage of all data types found in stealer logs

AI-POWERED ANALYSIS
- LLM Analysis - Advanced AI analysis of logs and data patterns
- Intelligent threat correlation and pattern recognition
- Automated risk scoring and prioritization
- Contextual insights from billions of data points

ADDITIONAL INTELLIGENCE SOURCES
- **IntelX Integration** - Access to IntelX intelligence search engine for comprehensive OSINT research
- **HudsonRock** - Domain threat analysis and compromised employee tracking

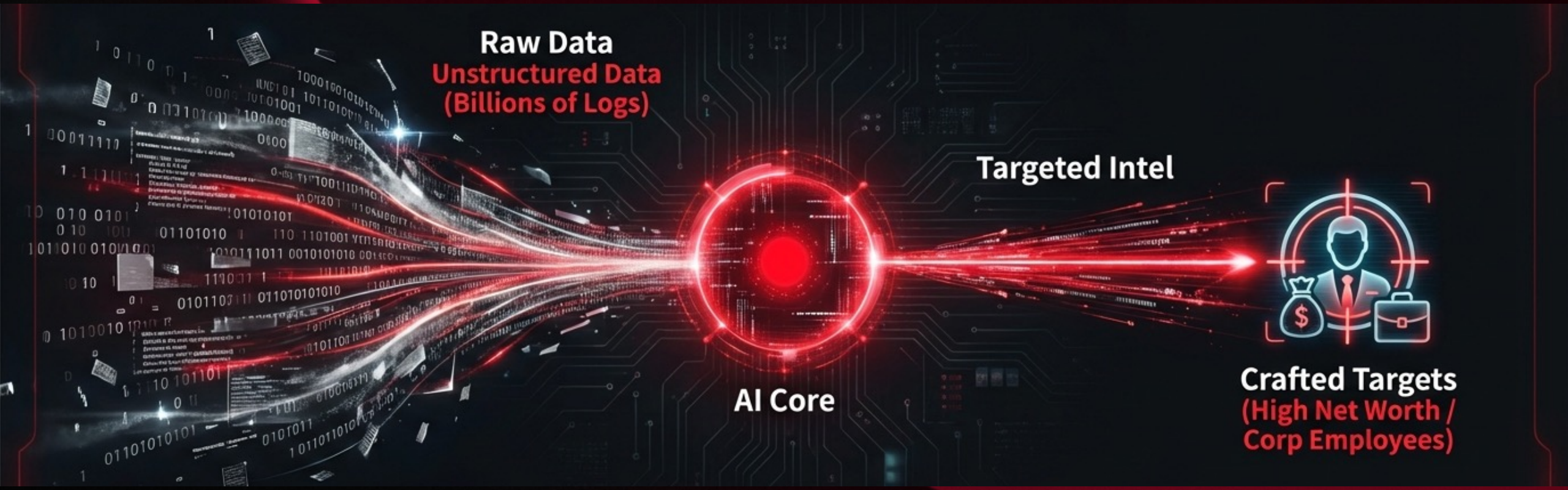
SEAMLESS INTEGRATION
Integrate real-time monitoring directly into your existing workflow:

アンダーグラウンド系サイトDarkForumの投稿

- Fireintelを名乗るサービスを宣伝
- 実態は攻撃者向けスティーラーログ検索基盤
  - 数十億のスティーラーログを検索
  - スティーラーログへのフルアクセス
  - 認証情報だけでなく、カード情報、ソーシャルメディア、メールアドレスその他
- AI-Powered分析　ー 高付加価値ターゲットの自動選別

KELA

生成AI・LLMによる悪用の高度化



脅威アクターは、膨大なスティーラーログを効率的に解析するために生成AIやLLMを活用し始めている。これにより、総当たり的な攻撃から、資産家や特定企業の従業員を狙う手の込んだ攻撃へのシフトを可能にしている

KELA

パスキー導入の成果と、攻撃者の戦術シフト

現状の成果 (Direct Defense)

防御の進化：生体認証（Touch ID/Face ID）とFIDOの連携により、kabu.com等への**直接的ななりすましログイン**はほぼ防御可能となった。

攻撃者のシフト (Infostealer Strategy)

攻撃の進化 (Infostealer)：攻撃者はID/PWを盗むのではなく、ブラウザに保存された「**Cookie（セッション情報）**」そのものを窃取する。
脅威の本質：これにより、攻撃者は「ログイン行為」をすることなく、**正規ユーザーのセッションを乗っ取る**ことが可能になる（Session Hijacking）。

KELA

窃取されるのは「ID/PW」だけではない：デジタルライフの全容流出

```
/Stealer_Log_Results\
|- /Browsers
|   |- /Chrome_Default
|   |   |- Cookies.txt
|   |   |- Passwords.txt
|   |   |- Autofill.txt
|- /System
    |- Information.txt
```

```
URL: https://id.moneyforward.com/sign_in
Username: ya[redacted]ta@gmail.com
Password: [REDACTED]
...
URL: https://global.americanexpress.com
URL: https://coin-trade.cc
URL: https://snkrdunk.com
URL: https://www.amazon.co.jp
```

1. Credentials
(ID/PW)

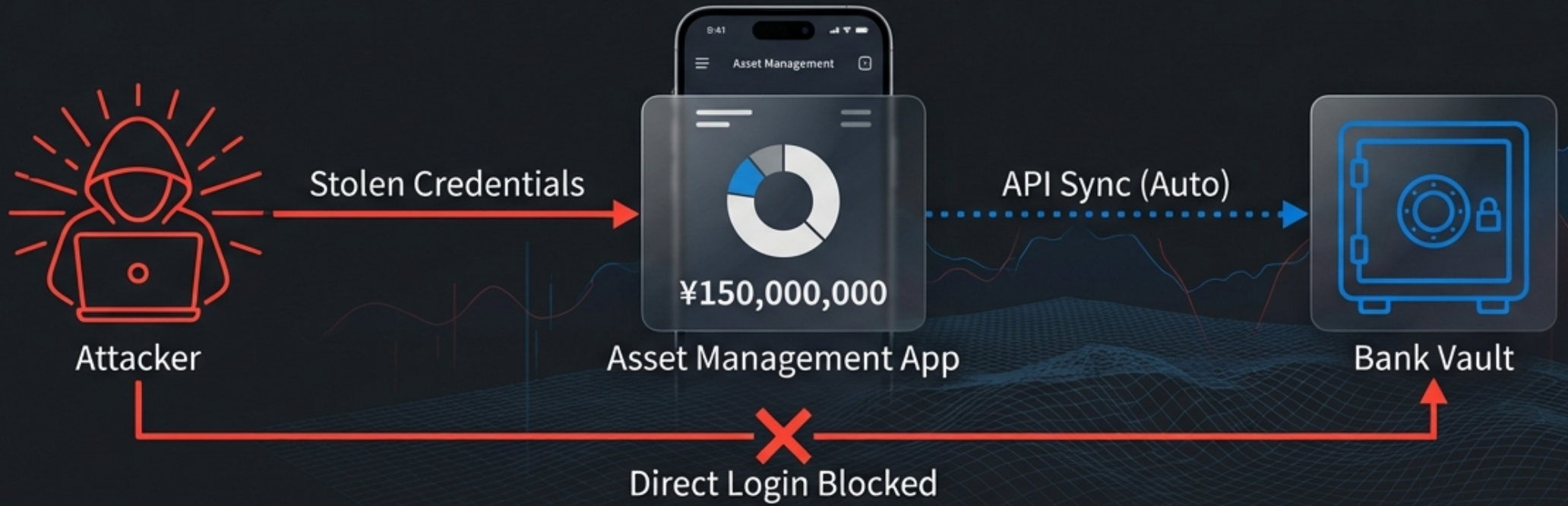
2. Autofill Data
(氏名, 住所, 電話番号)

3. Cookies
(セッションハイジャック用)

4. System Info
(IP, Device ID)

KELA

盲点となる「資産の可視化」リスク



資産のぞき窓: 攻撃者は銀行口座に直接ログインせずとも、API連携された資産管理アプリ経由で総資産額を把握できます。

標的型攻撃へ: 「資産を持っている」と特定された顧客は、ランダムな攻撃ではなく、コストをかけた巧妙な標的型フィッシングや恐喝のターゲットとなります。

攻撃者の課題：膨大なログの海と「選別のコスト」

Daily Uploads:

5,000+ Logs

Total Database:

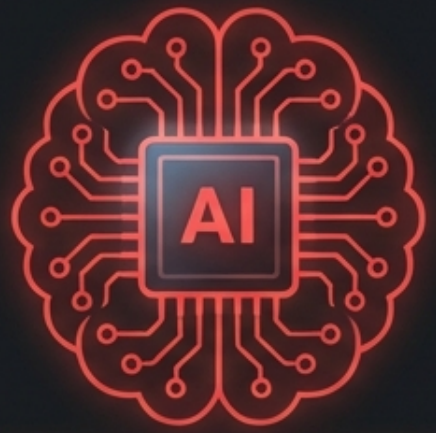
Millions of Records

データの洪水：ダークウェブ（Hubhead Logs, IceLogs等）では、毎日数千〜数万件の新規ログがアップロードされている。

- **従来の手法：**手作業でログを開き、富裕層を探すのは時間と労力がかかる非効率な作業だった。
- **ノイズ：**大半のログは、資産価値のない一般ユーザーや学生、あるいは死んだセッション情報である。
- **攻撃者のニーズ：**「確実に利益が出せる富裕層」だけを、この山の中から瞬時に抜き出したい。

KELA

生成AIによる「スナイパー型」標的選定の自動化



Prompt Console

```
> PROMPT: Analyze logs. Find users with URL
  contains 'moneyforward' OR 'wealthnavi'.
> FILTER: Look for keywords 'Platinum',
  'Black Card', 'Asset Overview'.
> OUTPUT: List Japan residents with >100M
  JPY implied assets.
```

High Value Targets

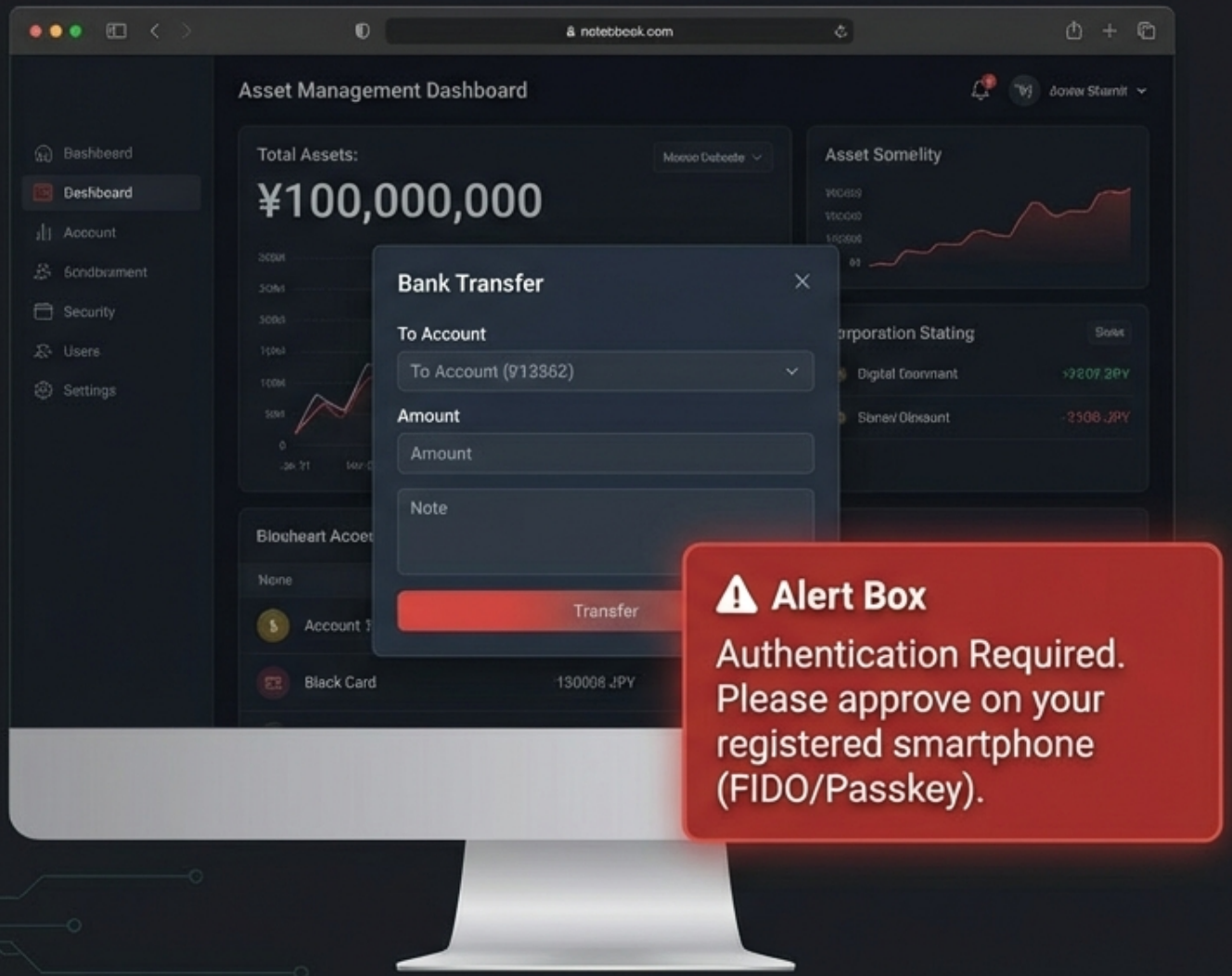
- Target 1: Japan Resident, Implied Assets > 100M JPY, Platinum
- Target 2: Japan Resident, WealthNavi, Asset Overview, Black Card
- Target 3: Japan Resident, Money Forward, 150M JPY, Asset Overview
- Target 4: Japan Resident, Money Forward, 150M JPY, Asset Overview
- Target 5: Japan Resident, Money Forward, 100M JPY, Asset Overview

LLMの悪用: 攻撃者は生成AI（LLM）にログ（非構造化データ）を解析させることで、富裕層の抽出を自動化している。

劇的な効率化: これにより、攻撃者は数秒で「資産1億円以上の日本人ターゲットリスト」を作成可能にする。

KELA

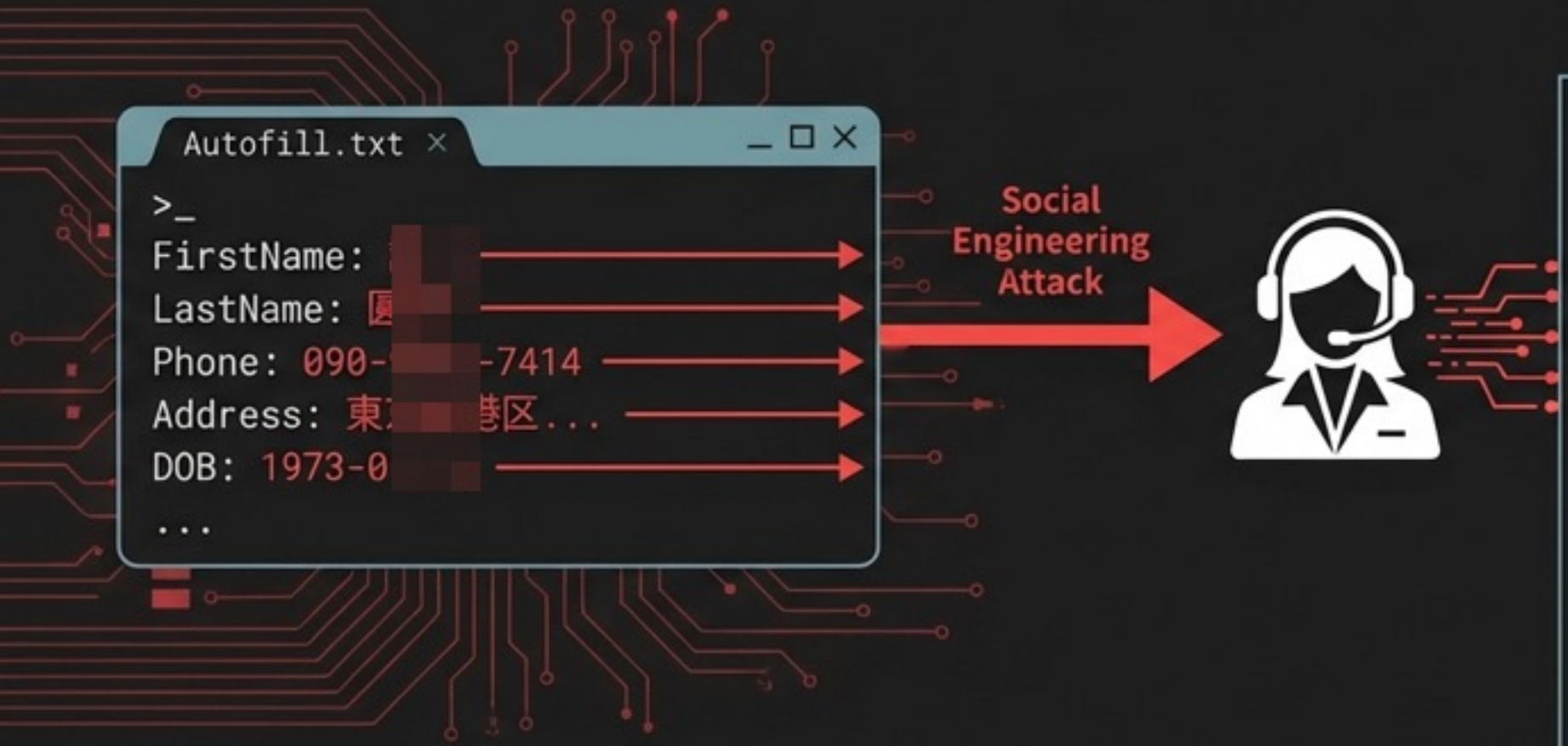
攻撃の壁：資産は見えても「動かせない」



- **閲覧と操作の分離:** 資産管理ツールで残高は確認できるが、実際の送金や出金には、金融機関サイト側での「強固な認証（2FA/パスキー）」が求められる。
- **攻撃者の心理:** 「金はそこにある。あとは『承認』さえ突破できればいい。」
- **Next Step:** デジタルでの突破を諦め、アナログ（ソーシャルエンジニアリング）へ舵を切る。

KELA

突破口は「アナログ」にあり：コールセンターへの攻撃



- **本人確認情報の形骸化:** コールセンターが本人確認のために尋ねる「氏名・住所・生年月日・電話番号」は、インフォスティーラーによって既に「完全な形（Fullz）」で盗まれている。
- **攻撃の非対称性:** オペレーターは「お客様」と話しているつもりだが、相手は「お客様以上の情報」を持った攻撃者である。

KELA

なりすましシナリオ：「スマホ紛失」という緊急事態の悪用

スマホを紛失してしまい、パスキーが使えません。
急ぎで振込が必要なのですが...

ご本人様確認のため、生年月日とご住所をお願いします。

1973年1月1[redacted]日、東京都港区...

確認とれました。一時的に制限を解除します。

- **なりすましシナリオの巧妙化:** 「スマホ紛失」という、パスキー利用者が最も陥りやすい状況を装う。
- **リアリティ:** 攻撃者はMoney Forward等で「どの支店にいくらあるか」を知っているため、会話に矛盾が生じず、オペレーターを信用させる。

前半パートまとめ

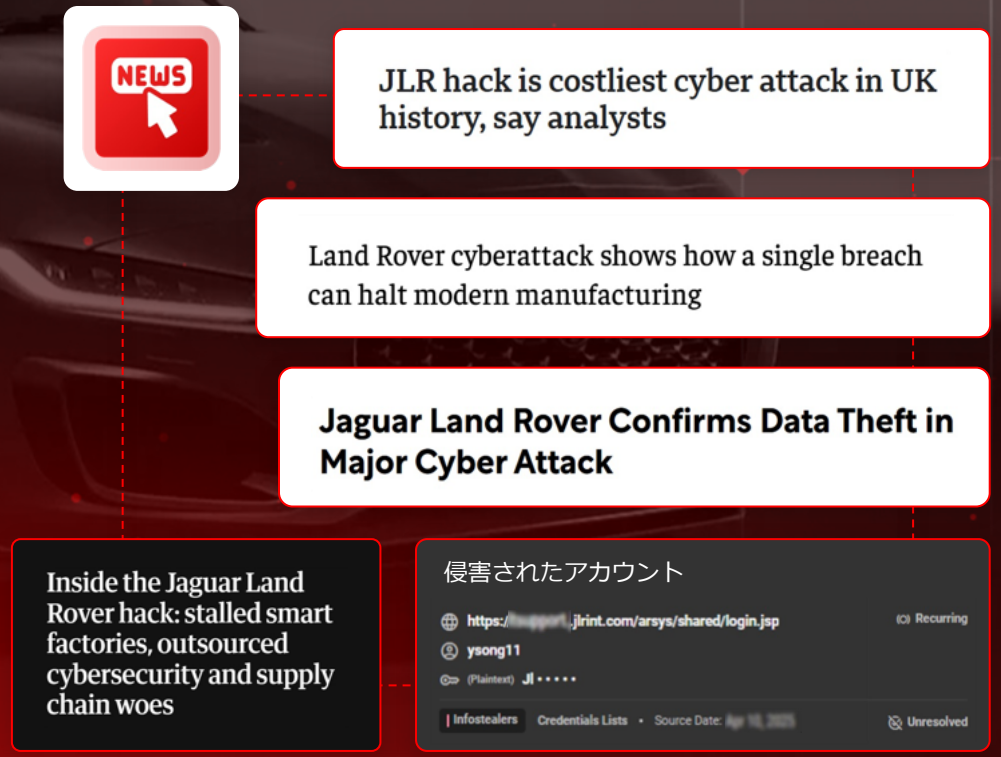
- 2025年は2024年から引き続き、インフォスティーラー感染は減少せず多くの被害をもたらしている
  - 金融口座への不正アクセス、ランサムウェアの初期アクセスなど
- 金融機関（特に証券会社）などではパスキーログインを必須化するなど、盗用認証情報によるログインは困難になりつつある。
- スティーラーログは端末利用者の個人情報を豊富に含むため、使い方次第ではなりすましの材料になる
- 生成AI/LLMの活用によりスティーラーログの悪用の手口は進化。ソーシャルエンジニアリング攻撃への備えを

インフォスティーラーに感染したアクターをハッキングする

1. JLRを攻撃したReyの例

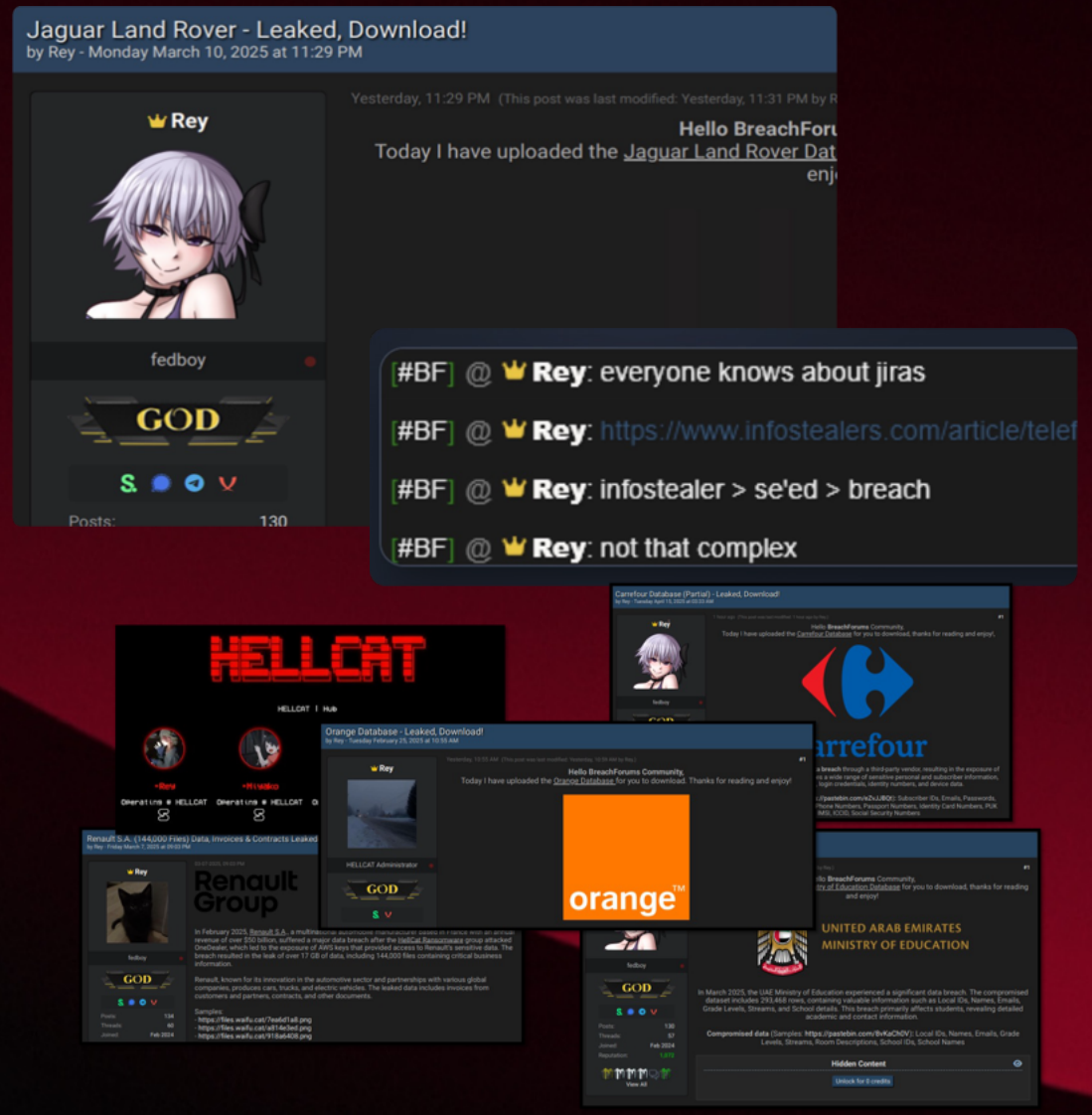
JRLのサイバー攻撃事案：何があったのか？

- 2025年8月31日、JLR大規模な「デジタル包囲攻撃（digital siege）」が開始され、Jaguar Land Rover は全世界のITシステムを予防的に停止し、すべての車両製造を中断する事態に追い込まれた
- 管理系ITシステムからOT環境まで広範囲にラテラルムーブメントが展開された
- 初期アクセスに使われたJIRAアカウントは、2021年にインフォスティーラーによって窃取されたものだった（ゼロデイ攻撃ではなく、正規アカウントによる不正アクセス）
- 本事件は、英国経済に19億ポンドの損失をもたらし、GDPの下振れを招いた



Rey – 地下フォーラムのアクター

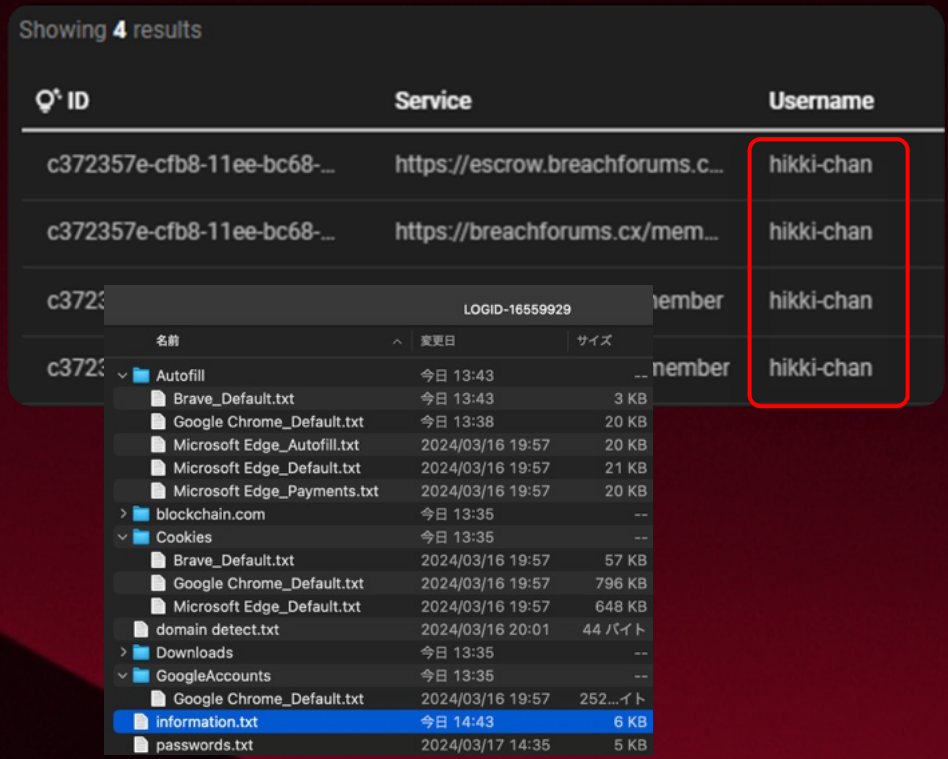
- 2025年3月10日にBreachForumでJLRのデータを公開
- Attlanssian JIRAアカウントへの侵入を認める投稿
- Hellcatグループの管理者、のちにScarttered Lapsus$ Huntersの管理者にも
- Breachforumのアーカイブ分析から、元のハンドルネームは”Hikki-Chan”
- インフォスティーラーからの認証情報を悪用し、多数の侵害に関与



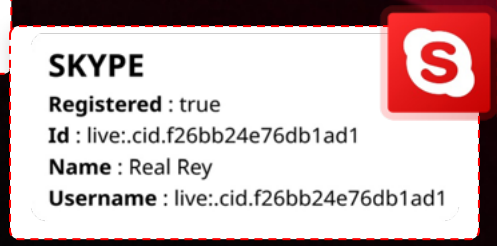
KELA

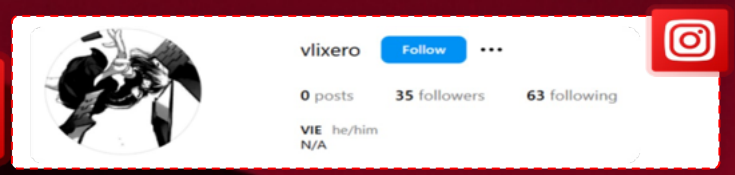
自身の感染によって暴かれた正体

- Ray自身の端末が2024年2月にRedline、3月にVidarスティーラーに感染
- KELAで収集したデータレイクからインフォスティーラーログを解析
- 複数のメールアドレス、多くのソーシャルメディアアカウント情報、Autofill情報から、Reyの正体はヨルダン在住のSaif Khaderと判明



Saif Khader





2. 北朝鮮IT労働者のケース

北朝鮮IT労働者とは？

北朝鮮政府による外貨獲得手段のひとつ

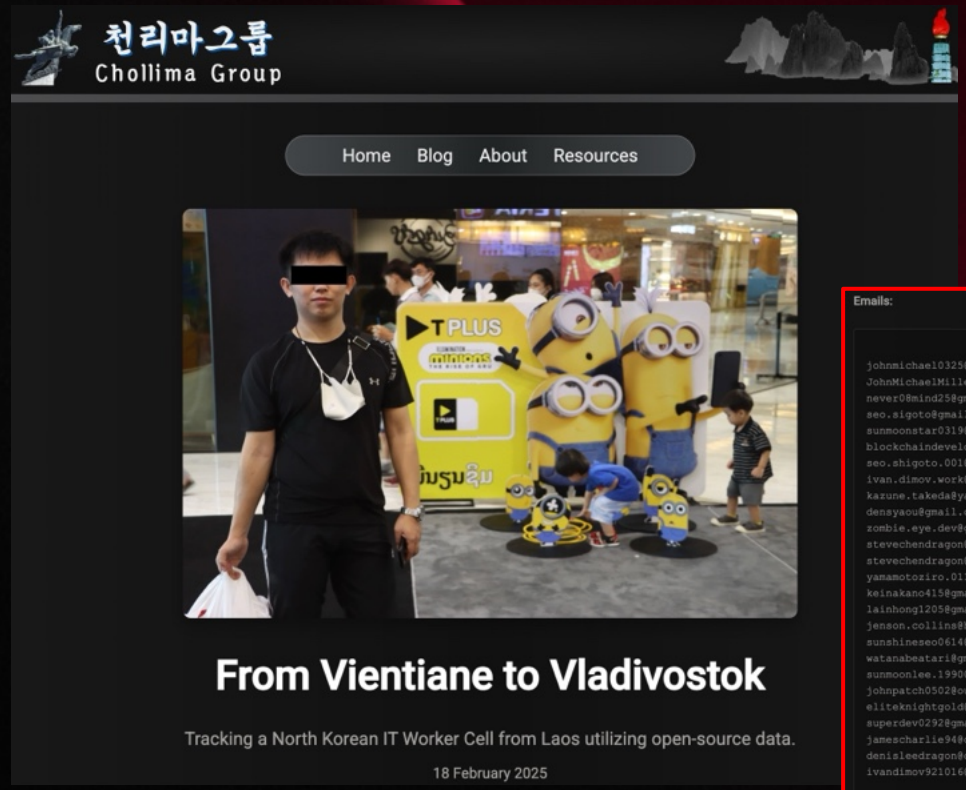
国連安保理決議第2397号（2017年12月）に基づく経済制裁をかいくぐり、数千～数万の北朝鮮IT労働者が国外での業務に従事、年間数億ドルの収益を得ているとも（ 多国間制裁監視チームMSMTの第２回報告書、2025年10月）

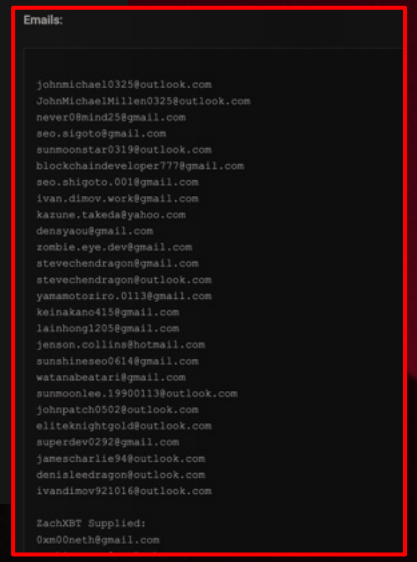
制裁をかいくぐるためにディープフェイクを用いて顔写真を偽造していた件は生成AIの悪用例として知られている

Knowbe4社サイトより

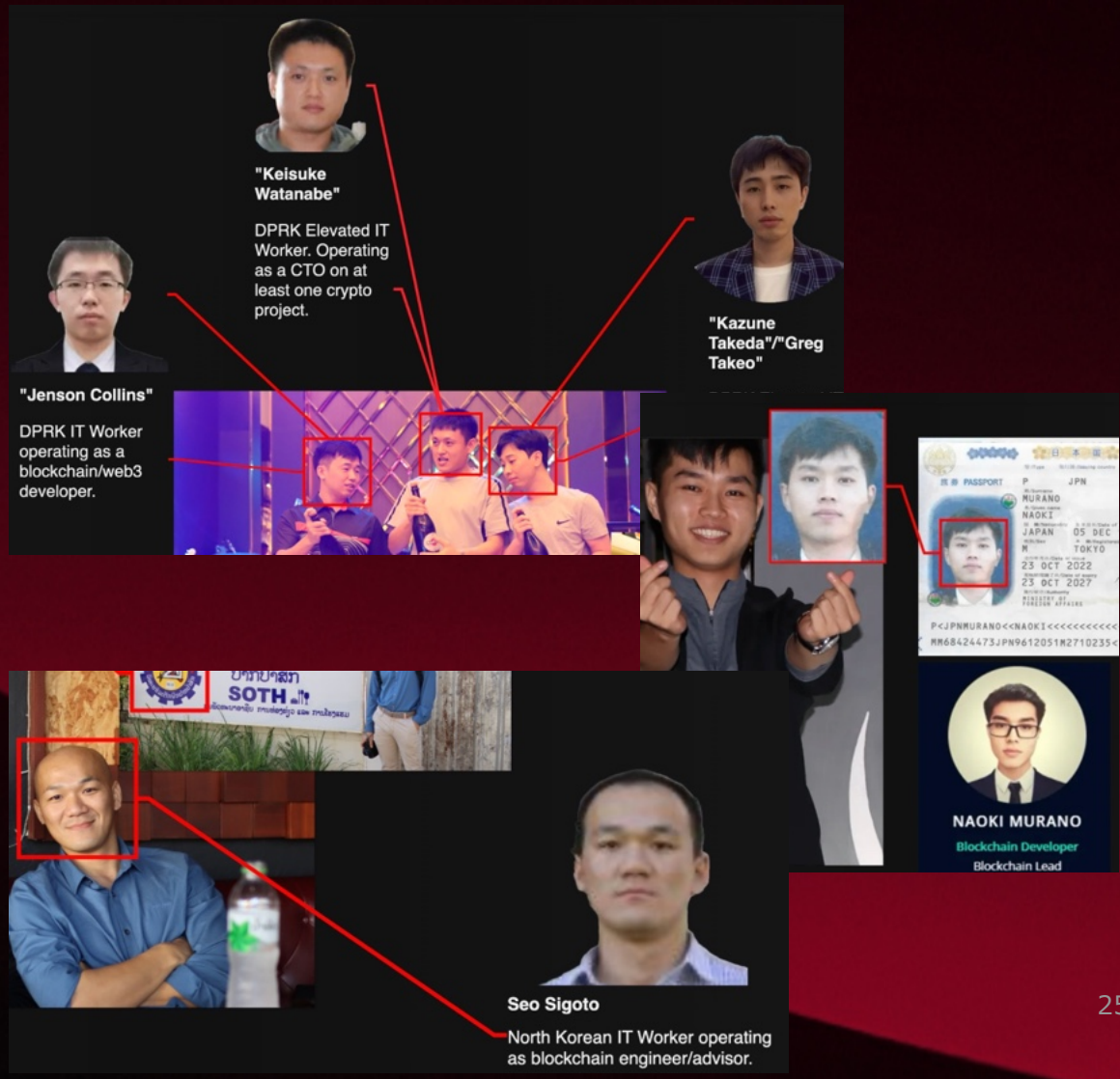
米司法省ウェブサイトより引用：
北朝鮮IT労働者にラップトップファーム環境を提供し、1700万米ドルの収益に寄与したかどで摘発された在アリゾナの女性クリスティーナ・チャプマン(50)の自宅写真
2025年7月、チャプマンには禁錮8年６ヶ月、罰金17万ドルの刑が確定

i北朝鮮動向を追跡する研究者グループのブログ



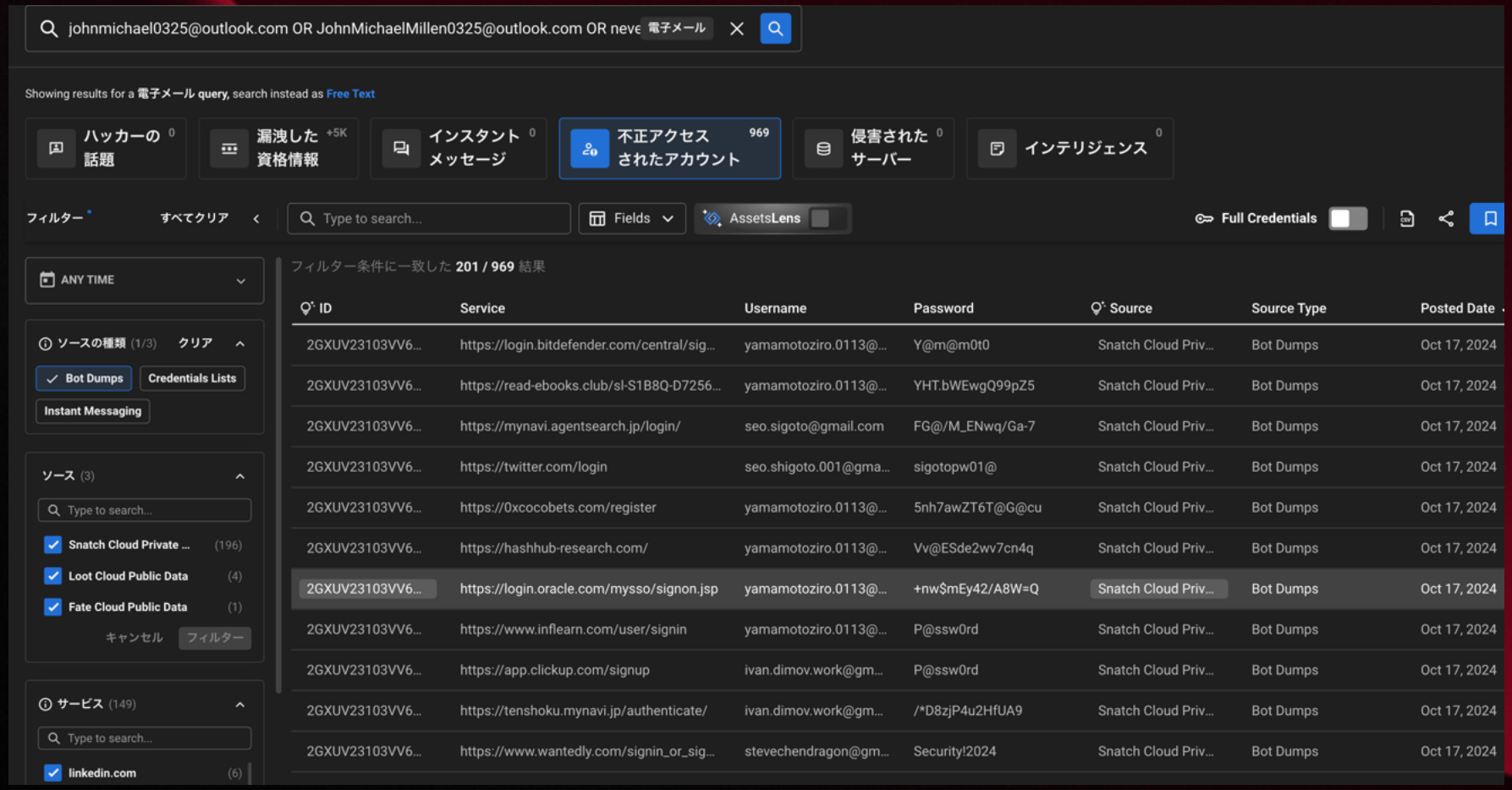


Chollima Group 2月発表のブログ
日本名を語る人物が複数登場



KELAプラットフォームによる探索

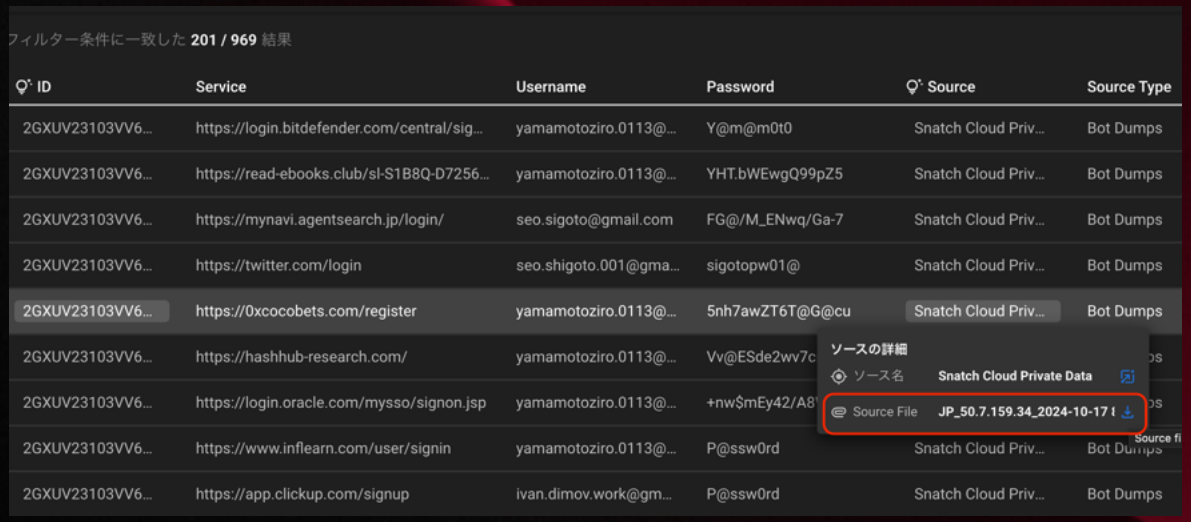
記載されていた30のメールアドレスをKELAデータレイクにクエリ



Compromised Accountsの結果のうち、スティーラーログダウンロード可能なBot Dumpsでフィルタ

KELAプラットフォームによる探索の結果

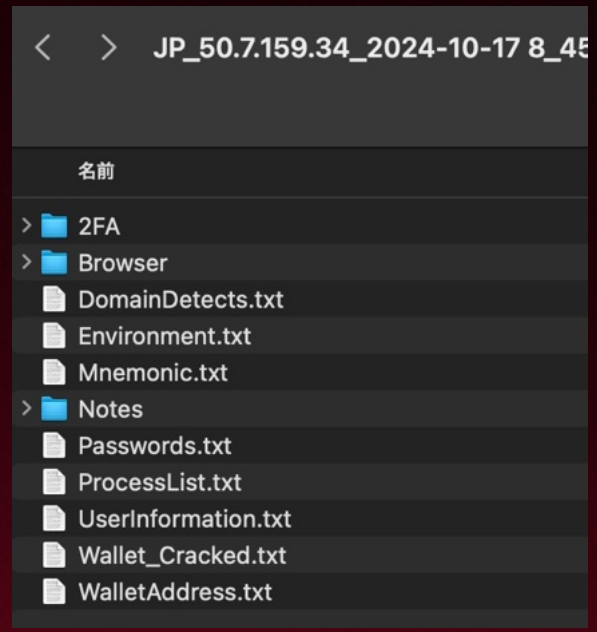
関連するスティーラーログ４つを特定、うち３つは日本のIPアドレスを利用する端末で感染したものだった



- 2024年の7月、10月に感染したそれぞれの端末はいずれもIPアドレス 50.7.159.34 を使用。
  - このIPはAstrill社レンジのものであり、実際にはVPNを利用して国外から接続していたと思われる
- 2021年8月に感染した端末はIPアドレス 89.187.161.220を使用。
  - こちらはDataCamp社が用いているIPで、これもVPNを使用した国外からの接続と思われる
- USのIPアドレスの端末には日本国内関連では特筆すべきものがなかったため上記３つのスティーラーログに絞って調査を開始した。

スティーラーログの中身

- ブラウザのパスワードマネージャーに保存された認証情報
- 2FA情報：Chrome拡張機能のAuthenticator, GithubログインのMFAシード
- 端末情報：Hardware ID他HW情報, OS version, IP, Time Zone, Keyboard等
- Cookie：ブラウザで保存されているセッション情報等
- Autofill：HTMLフォームに入力した内容。氏名、メールアドレス、電話番号等
- History：ブラウザ閲覧履歴
- ブラウザのブックマーク
- Wallet：仮想通貨Wallet情報、復元用シード情報
- Sticky Note :デスクトップの付箋メモ



- ✓ 同一端末内で多数のプロファイル（別ログインアカウント）が作成されている。
- ✓ 異なる受託先のGmailアカウント等SaaSアプリの切り替えを手早く行うためかと思われるが、同一端末を複数人で使い回している可能性も

ブラウザの閲覧履歴から見えたこと

- 国内のありとあらゆる求人、フリーランス求人サイトへのアクセス
- Google翻訳を相当駆使してメールやチャットツールでの日本語コミュニケーションを図っていた
- 時には敬語サイトも利用して質の高い日本語表現を目指していた

パスワードファイルに保存されていた認証情報

- Seo Sigoto, Jiro Yamamoto名のログインID多数
- 国内求人サイト、フリーランサー募集サイト
  - Indeed、Wantedly、レバテック、Lancers、Crowdworks他多数
- 履歴書（Resume)作成支援サイト
- スキル向上関連サービス各種
- 各種SaaSアカウント
- 多数のGmail, live.com,
- IT製品、サービスアカウント
- Autodesk, VMware, HPE
- 国内企業メールアドレスがログインIDに用いられた開発環境・テストサイトのアカウント
- 多数のGithubアカウント

Daniel Suzuki

BlockChain Engineer

A skilled blockchain engineer with 6 years of professional experience looking to contribute knowledge in web and blockchain technology . Especially focus on Defi. Proficient at performing well as working in a group or independently in a fast-paced setting. Deep understanding of distributed ledger, blockchain safety, blockchain design principles, and various blockchain protocols and environments.

Contact

linkedin

https://www.linkedin.com/in/daniel-suzuki

Email

ichirosuzuki0918@outlook.com

Address

Osaka, Japan

Education

Apr 2013 - Mar 2017

Bachelor's degree, Computer Science.

Meiji University

Expertise

- Solidity

Experience

Feb 2023 - Sep 2023

Goose Finance

Blockchain developer

Goose Finance is a decentralized exchange running on Binance Smart Chain and Pancake swap exchange, with lots of other features that let you earn and win tokens .

- Developed the smart contracts of staking and farming using Solidity, Hardhat.
- Used the Sushi's masterchef staking and Pancake protocol to develop the contracts with Golden Egg tokens.
- Realized the auto-compounding in this finance.
- Developed the subgraph for frontend data fetching.

Mar 2022 - Jan 2023

Fringe Finance

Blockchain developer

Fringe Finance is a decentralized money market designed to unlock the capital spread in crypto assets regardless of their capitalization and supported network.

- Developed the smart contracts using Solidity, Typescript, Hardhat.
- Focus on lending and borrowing with interest rate model such as Aave protocol.
- Developed the price oracle contract using Chainlink price provider, Uniswap V2 price provider.
- Collaborated with frontend developers for interaction to smart contract.

Apr 2021 -Feb 2022

FutureSwap

現在でも公開状態となっている、ダニエルスズキ（明大卒）を称する北朝鮮IT労働者の洗練された英文履歴書

国内企業の業務に従事したと思われるアカウント

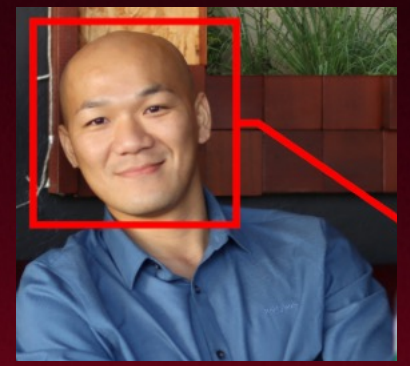
流出パスワードリストのなかに、ペット保険（動物の治療費を補填する保険）の大手であるA社のアカウントがいくつも含まれており、a.saitoh119というアカウント名で複数のテスト環境への認証情報が保存されていることからも同社のシステム開発に携わっていた様子がうかがえる。

```
URL: https://sokudan.work/login
Username: seo.sigoto@gmail.com
Password: sigotopw01
Application: Google_[Chrome]_Default
===============
URL: http://35.72.171.239:8088/login
Username: a.saitoh119@[redacted]
Password: password
```

```
URL: http://52.69.70.108:8088/login
Username: a.saitoh119[redacted].com
Password: password
===============
URL: https://www.blockchain-sentry.com/
Username: seo.sigoto@gmail.com
Password: blockchainsentryP@ssw0rd
```

```
URL: https://br[redacted].com/login
Username: a.saitoh119@[redacted].com
Password: password
Application: Google_[Chrome]_Default
```

```
URL: https://signin.aws.amazon.com/
Username: keisuke.yokoyama@ponypart
Password: E=)VZyq4=n!m6V5
Application: Google_[Chrome]_Profil
===============
URL: http://13.114.140.231:8088/reg
Username: a.saitoh11[redacted].com
Password: password
```

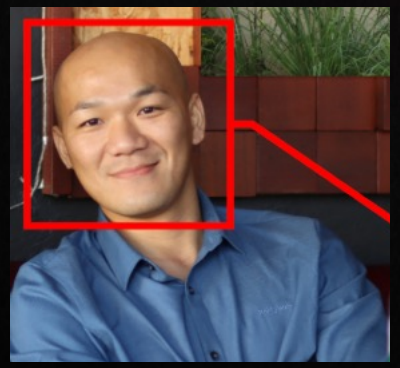


開発業務従事者の
正体はSeo Sigoto

KELA

Seoが使っていたデスクトップ付箋（Sticky Note）

- よく利用するメールアドレス、パスワード群、
- 日本の電話番号２つ
- 応募時に利用するメールのテンプレート
- テンプレートには実績紹介としてクラウドワークスの公開プロフィールへのリンクが含まれており現在も閲覧可能



seo.sigoto@gmail.com/amazon.jp/sigotopw01@@@@
yamamotoziro.0113@gmail.com
moon1357Lee
seo-san: +81 070 417[redacted]
my phone +81 070 144[redacted]

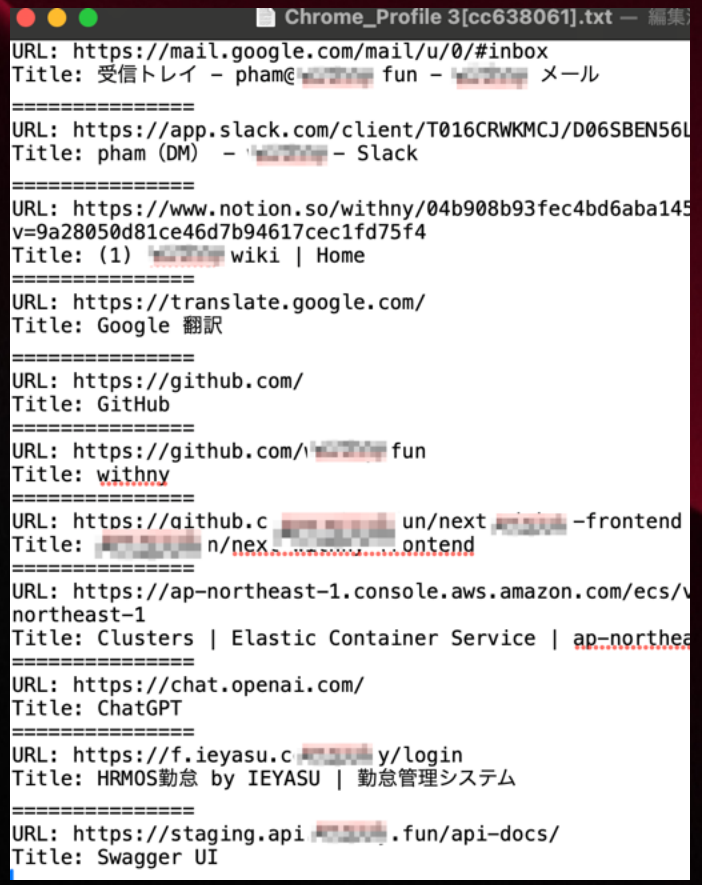
初めまして。提案文をご覧いただき誠にありがとうございます。
フリーランスでディレクター、エンジニア、ライターをしております、
seosigotoと申します。
～出来る事・スキル～
https://crowdworks.jp/public/employees/376[redacted]ccupations
ポートフォリオ・実績→
https://crowdworks.jp/public/employees/376[redacted]esumes
――
募集内容を拝見し、弊社で担当可能な案件と思いました。
参考として、以前弊社で開発成果物をご覧になれる、URLを添付させていただきます。
https://hor[redacted]m/
https://www.[redacted]mecreamery.ca/
フロントはVue.jsのVuetifyとBSVueを利用しバックエンドはPHPのLaravelを主に利用して
プさせました。
【提供できるいくつのメリット】
――
1.１０年の長年の経験であらゆる分野で活動し、WEBシステム開発に関しては幅広い経験とノウ
――
2. 納期よりも早く納品することが可能です。
今までのコードの所有権をもっており、経験したコードをモジュール化し組み立てで対応できま
――
3. 予算より安い価格でお受けすることも可能です。
モジュール化したコードの組み合わせで時間を最小限に短縮し、精度をあげながらも予算を抑え

現在でもクラウドワークスのサイトで公開状態となっている、Seo Sigotoのワーカープロフィール。
2021年をピークに2024年まで計30件の業務受託実績

ブックマークにのこされていた痕跡(1)

- ブラウザのブックマーク情報がプロファイル別に窃取されており、そのうち一つのものは、アダルトグッズ販売・エンターテイメントサイトの開発業務の従事に用いられていた

- メール
- Slack
- 勤怠管理
- ナレッジ（社内Wiki)
- 翻訳ツール
- 開発環境
  - フロントエンド
  - API環境
  - インフラ（AWS)



当社の開発業務に従事した人物の正体もおそらくSeo（確信度・中）。ここではPhamというベトナム人を詐称していた。

ブックマークにのこされていた痕跡(2)

別のプロファイルでは保存されていたのは僅かだったが、とある企業のメールアカウントらしきものが確認できた

Chrome_Profile 4[5fc5c480].txt

```
URL: https://mail.google.com/mail/u/0/#inbox
Title: 受信トレイ - minh.nguyen@[redacted].com メール
==========
URL:
```

このメールアカウントはとある都内にあるデジタルマーケティングに強みをもつコンサル・開発企業のものだが、このプロファイルに紐づくパスワードファイル・Autofillファイルから、この企業がソリューションを提供しているYext（Web上の企業プロファイル管理ツール）プラットフォームで化粧品ブランドや外食チェーン（回転寿司運営）の企業プロファイル管理にも従事していたことが判明した
この人物minh.nguyenは、Withnyの業務に従事したPhamと同一人物（おそらくSeo）

ブックマークにのこされていた痕跡(3)

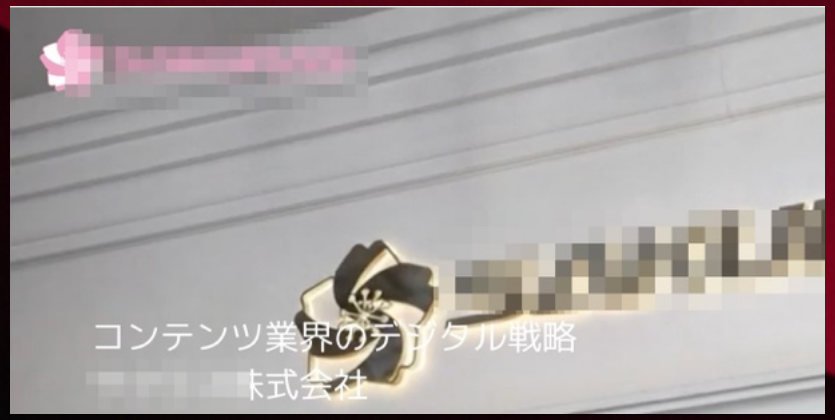
そのほかのプロファイルのブックマークでも、ITコンサル・開発関連企業のメールアカウントやSlackアカウントのものがあり、IT開発系の業務に従事していたことがうかがえる

Chrome_Profile 5[19fea3e5].txt — 編集済み

```
URL: https://mail.google.com/mail/u/0/#inbox
Title: 受信トレイ - h.nguyen@[redacted] メール
==========
URL: https://app.slack.com/client/T014C4K625B/C014S4MDCBT
Title: general (Channel) - [redacted]
==========
URL: https://github.com/[redacted]
Title: [redacted]
==========
URL: https://www.notion.so/[redacted]/00ce2518a9a94c0983ea5e3[redacted]
Title: ヒューさん オンボーディング資料
```

Chrome_Profile 6[d3b30a4a].txt

```
URL: https://mail.google.com/mail/u/0/#inbox
Title: 受信トレイ (4) - hp73@[redacted]株式会社 メール
==========
URL: https://app.slack.com/client/T01GF023FUY/C01FRASAJGK
Title: 00_公式発表 (Channel) - SAK1st - Slack
==========
URL: https://docs.google.com/document/d/1vpxm4R_8m_ObnTmG5WRalTlu5hrvNO69-yEAK[redacted]
Title: マス_スタートアップマニュアル - Google ドキュメント
```



KELA

後半パートまとめ

- JLRサイバー攻撃の一味であるReyのように、アクターは複数のハンドルネームを使い分け、身元の隠匿を図っている。しかしうっかりスティーラーマルウェアを踏んでしまうとハッカーでも全てが丸裸にされてしまうこともある

- 北朝鮮IT労働者の実態
  - ほぼ全ての大手求人サイト・フリーランサー向けプラットフォームを駆使し、さまざまの業種・幅広いスキルの業務に従事。
  - 信頼あるプラットフォーム上で、正規の認証にくわえて”レピュテーション・高い評価”を獲得しており、発注側で北朝鮮IT労働者への発注リスクを判断するのは極めて困難
  - Astrill 等のVPNを駆使し、日本国内からのアクセスを偽装

Thank you!

www.kelacyber.com

KELAGROUP