

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

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

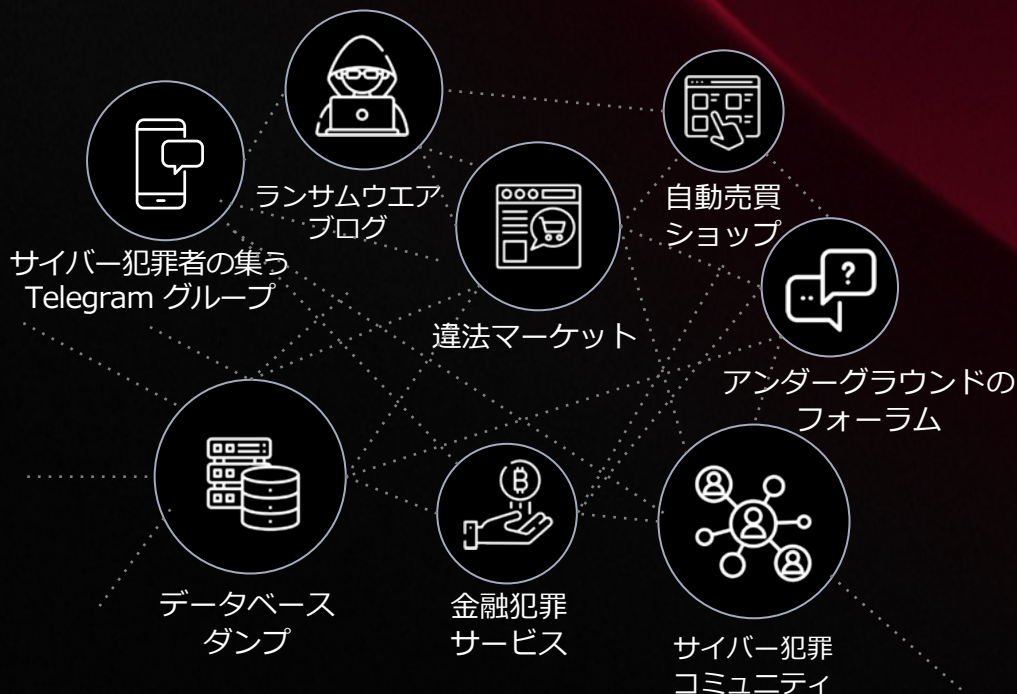
経歴

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 チャンネル開拓責任者
 APC（現在Schneider）：代理店営業責任者
 など

デジタル犯罪を阻止するインテリジェンス

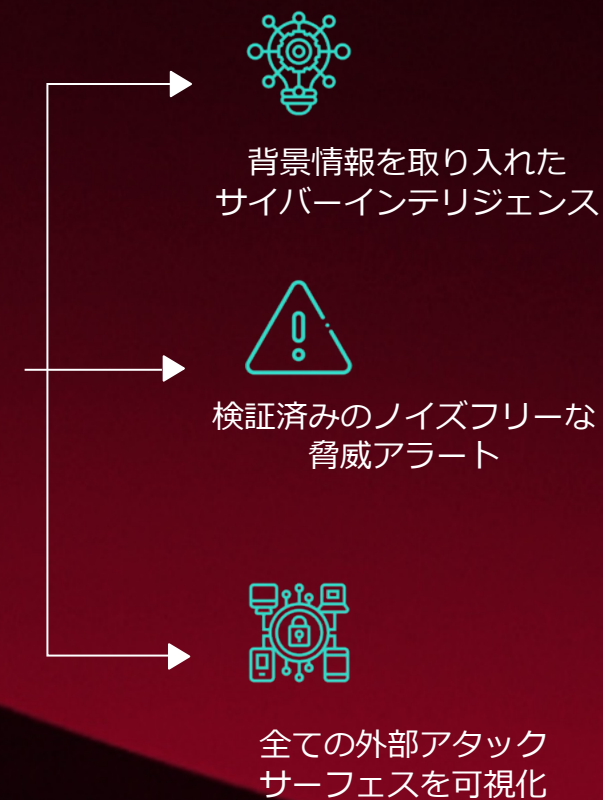
KELAは到達困難なアンダーグラウンド空間を詳細に把握、隠れた脅威を顕在化・抑制します。

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



本セッションの内容

前半パート

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

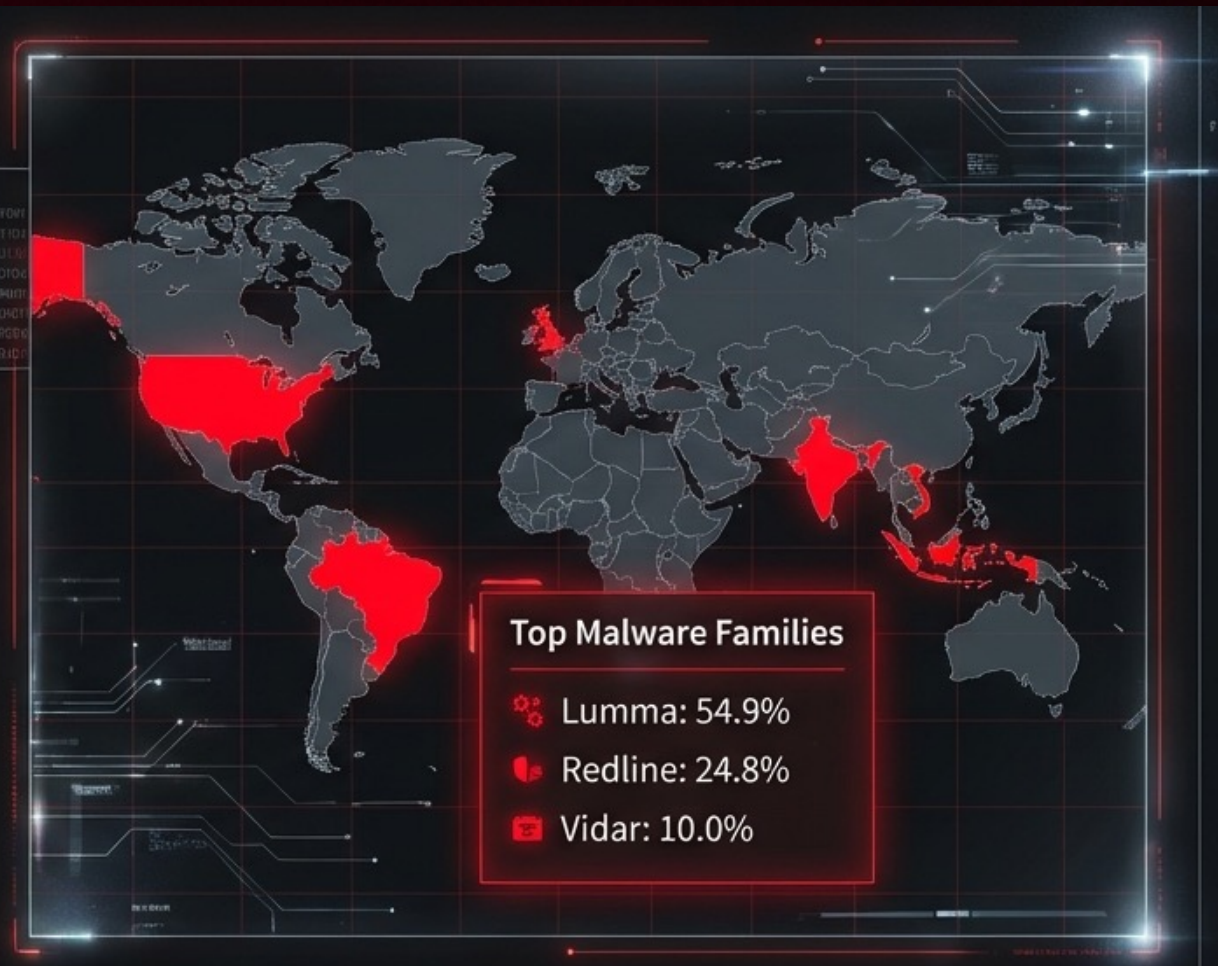
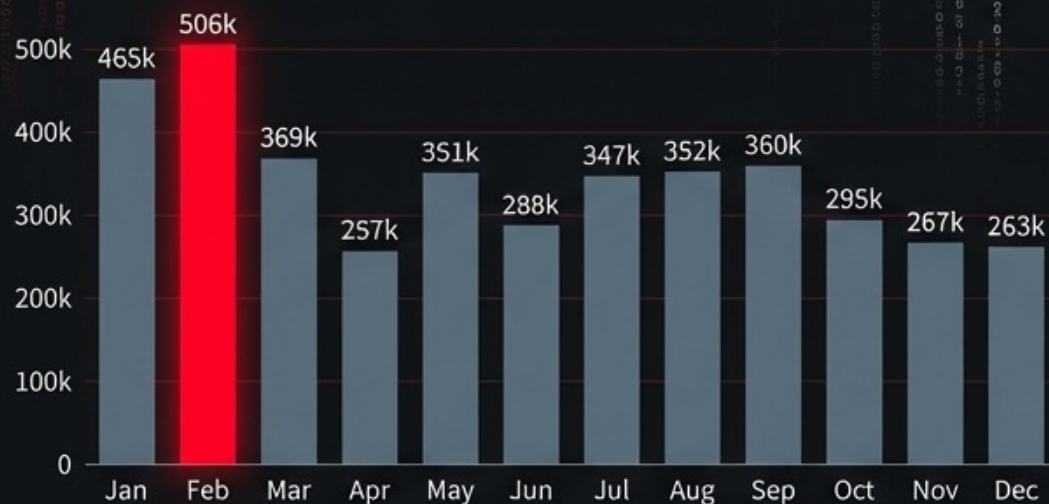
後半パート

- インフォステイ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

2025年のインフォステイラー感染状況

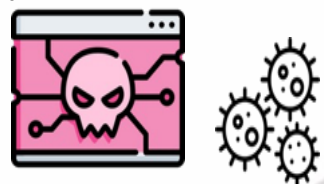
4,126,707

2025年 総感染端末数

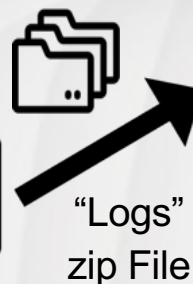


おさらい：インフォスティーラー（情報窃取マルウェア）

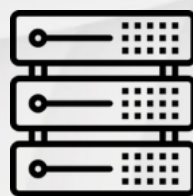
1. 攻撃者は、①スパイフィッシングで悪質な添付ファイルを送付、②チートツールを装うなどして不特定多数に配布、インストールさせ、PCをマルウェアに感染させる



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



4.1' ①のスパイ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。



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

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

Stealer: All System: All Country: Japan (21020) Links: Search by Links Search by Mask Search by Cookie Search by Email

State: All City: All Zip: accounts.google.com ONLY WITH COOKIES

ISP: ADSL Maroc telec Outlook: @domain.com Per page: 10 Vendor: All Price: 0 \$ 10 \$ Search

Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
Redline	Japan	workspace.google.com totalbattle.com epicgames.com	-	-	archive.zip	2023.09.17 sm####ez 0.13Mb	(platinum)	\$ 10.00	Buy
Vidar	Japan	workspace.google.com totalbattle.com epicgames.com	-	!	archive.zip	2023.09.17 Hy####ad 0.45Mb	(platinum)	\$ 10.00	Buy
Vidar	Tokyo	facebook.com facebook.com	-	!	archive.zip	2023.09.16 Hy####ad 0.26Mb	(platinum)	\$ 10.00	Buy
lumma	Saitama	auth0.openai.com auth0-id.com accounts.google.com connect.appen.com signup.live.com freelancer.com freelancer.com appleid.apple.com accounts.spotify.com	-	-	archive.zip	2023.09.14 Mo####yf 0.20Mb	(Diamond)	\$ 10.00	Buy

HUBHEAD LOGS



■ We have some private stealers | RedLine, Raccoon, M Aurora.. projects
■ Using separate sources | daily logs uploading
■ GEO - MIX | ES DE US IT FR EE LT GB NL BE ASIA
■ Logs amount enough for 10 people | 2000-5000/day
■ Private cloud logs only for 2022 | 4/02/23 ~2.000.000
■ If you need old logs - DM | logs sorted by dates of 20

4 2 2 11

Leave a comment

IceLogs

FAST LIFETIME - 250\$
MONTH - 150\$

If you want to buy fresh and premium logs
Everyday 3-5K logs upload in premium private

- ✓ Crypto, Wallets, Cards, Banks, Game Requ
- ✓ BR, AR, EU, USA, CA, Mixed country
- ✓ Uploading 1,000-5,000 Logs per day!
- ✓ Stillers: Redline, Meta Stealer, Raccoon

Admin cloud @RAZERTOP

PRICE LIST

FAST LIFETIME - 250\$
MONTH - 150\$

@REAPER - ULP FREE #20 (DATA 22.02.2026).txt
84.4 MB - Show in Finder

ULP - FREE

DING - DONG! NEW FREE ULP! "

DATA - 22.02.2026

REAPER OWNER : @ReaperOwner

3 84 14:17

Feb 22

DING - DONG!

DING - DONG! NEW ULP PRIVATE! "

DATA - 22.02.2026

REAPER OWNER : @ReaperOwner

86 14:18

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Telegram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。

KELA

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

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

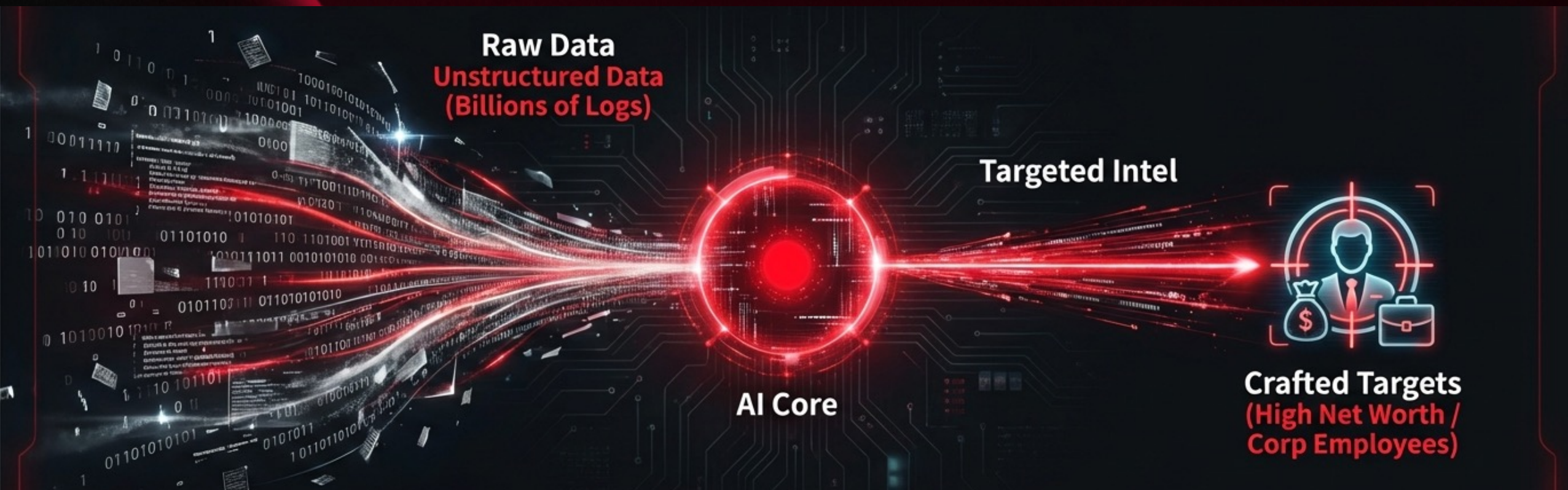
SEAMLESS INTEGRATION

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 — 高付加価値ターゲットの自動選別

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、総当たりの攻撃から、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

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）。

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

```
1 /Stealer_Log_Results\  
2 |- /Browsers  
3 |   |- /Chrome_Default  
4 |     |- Cookies.txt  
5 |     |- Passwords.txt  
6 |     |- Autofill.txt  
7 |- /System  
8   |- 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>



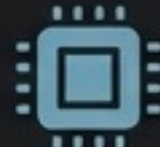
1. Credentials
(ID/PW)



2. Autofill Data
(氏名, 住所, 電話番号)

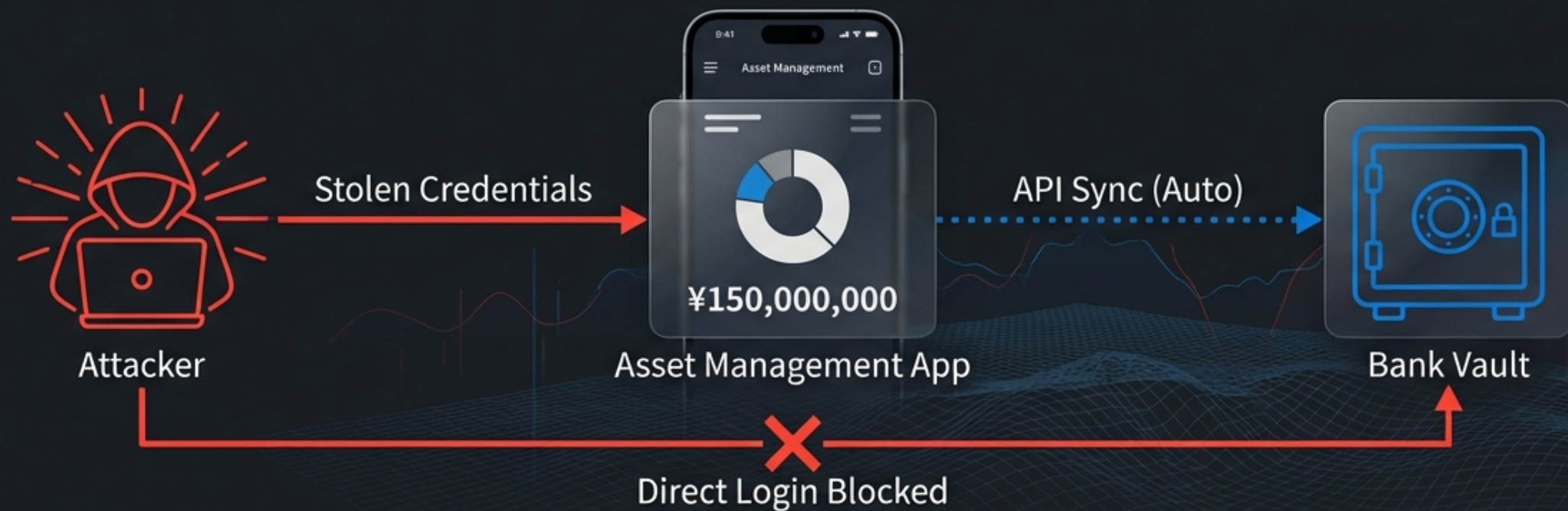


3. Cookies
(セッションハイジャック用)



4. System Info
(IP, Device ID)

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。

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

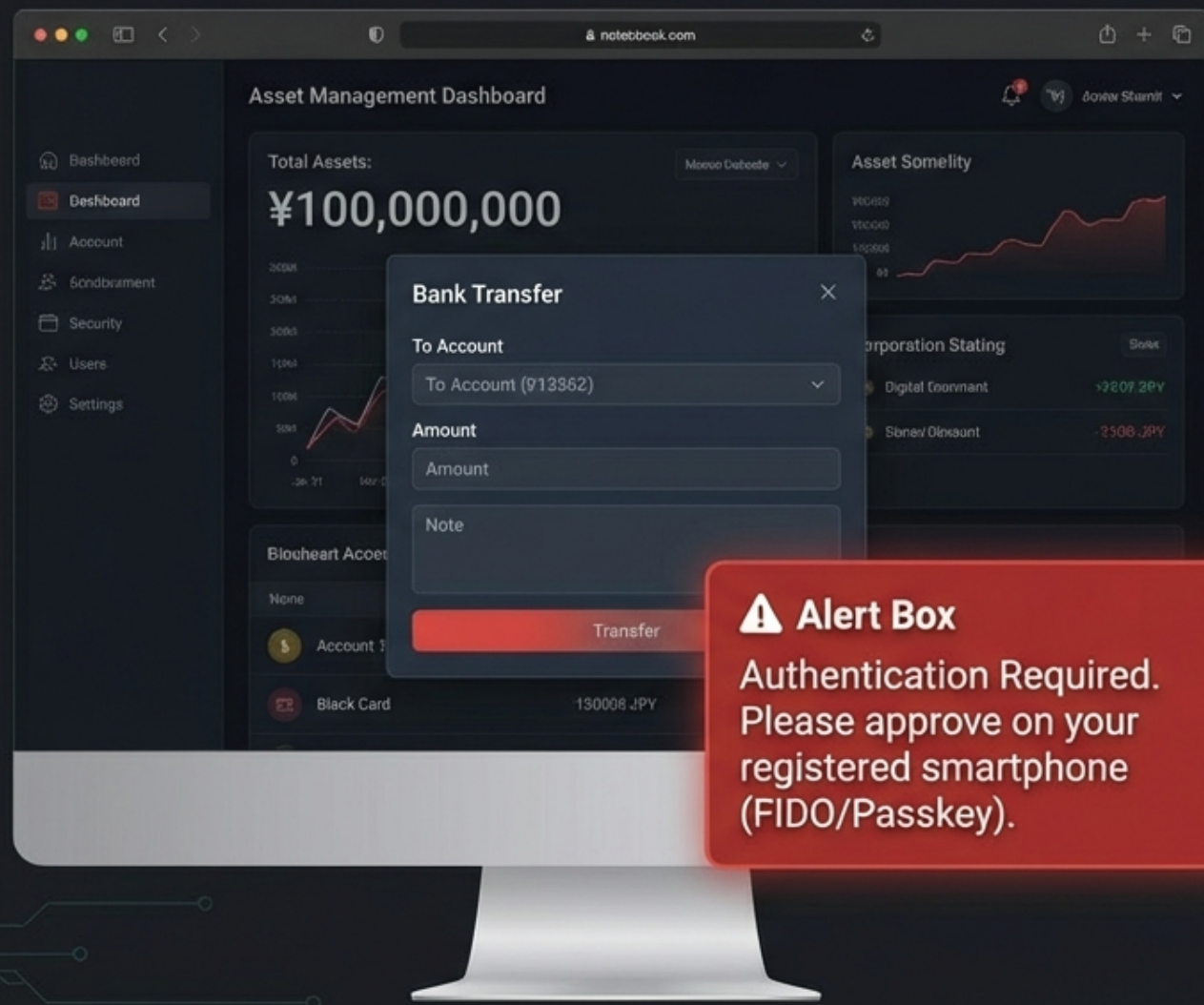


LLMの悪用: 攻撃者は生成AI（LLM）にログ（非構造化データ）を解析させることで、富裕層の抽出を自動化している。



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。

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。

突破口は「アナログ」にあり：コールセンターへの攻撃



Social
Engineering
Attack



- **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。

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

インフォステイラーに感染した
アクターをハッキングする

1. JLRを攻撃したReyの例

JLR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



JLR hack is costliest cyber attack in UK history, say analysts

Land Rover cyberattack shows how a single breach can halt modern manufacturing

Jaguar Land Rover Confirms Data Theft in Major Cyber Attack

Inside the Jaguar Land Rover hack: stalled smart factories, outsourced cybersecurity and supply chain woes

侵害されたアカウント

<https://jlr-int.com/arsys/shared/login.jsp>

ysong11

(Plaintext) JI*****

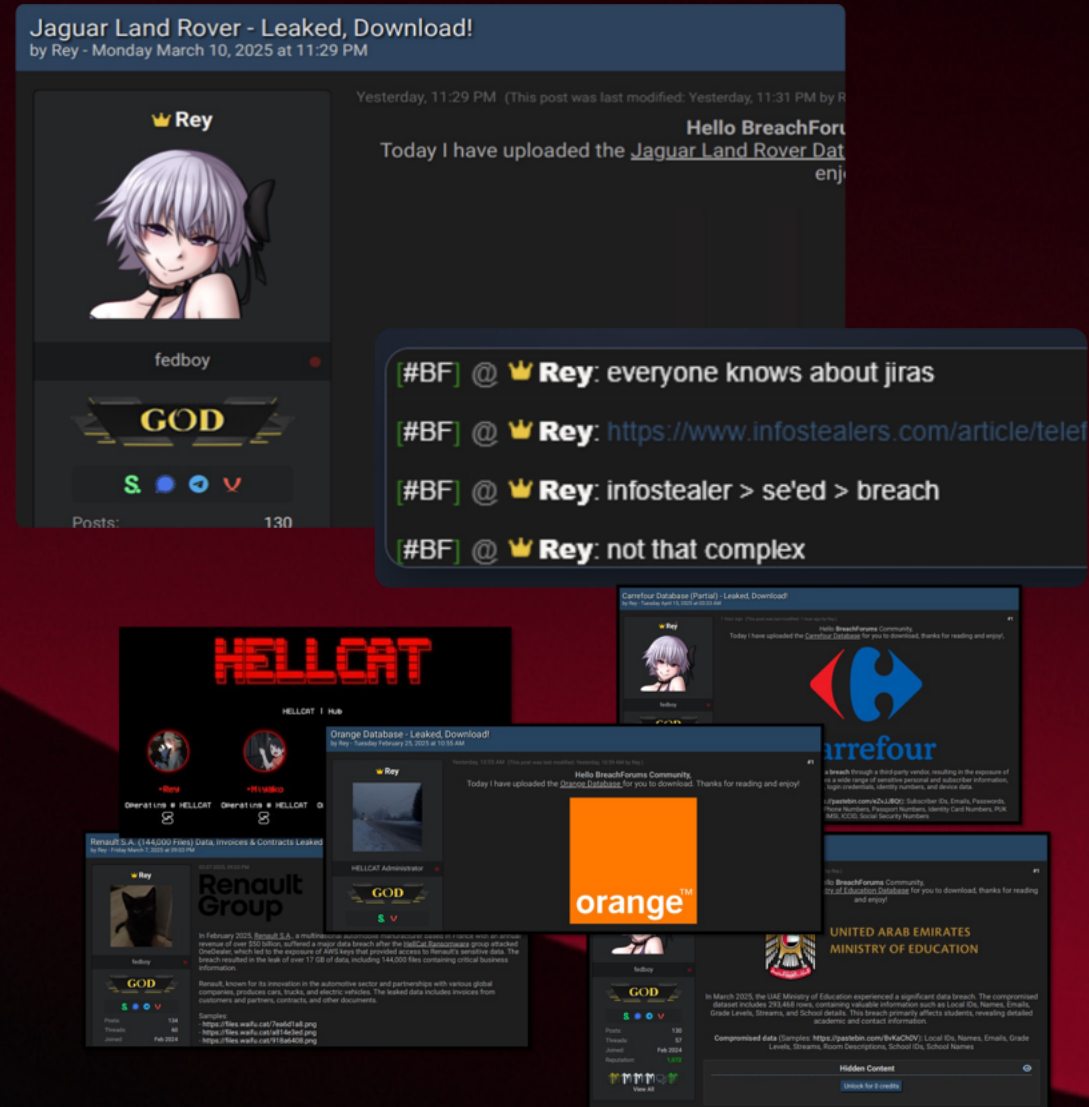
Infostealers Credentials Lists Source Date: Aug 18, 2025

(C) Recurring

Unresolved

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Scattered 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



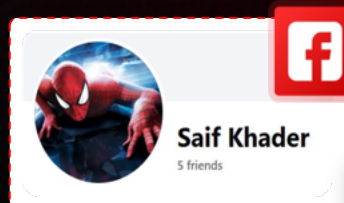
自身の感染によって暴かれた正体

- 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、Rayの正体はヨルダン在住のSaif Khaderと判明



KELA

Saif Khader



Showing 4 results

ID	Service	Username
c372357e-cfb8-11ee-bc68-...	https://escrow.breachforums.c...	hikki-chan
c372357e-cfb8-11ee-bc68-...	https://breachforums.cx/mem...	hikki-chan
c372357e-cfb8-11ee-bc68-...	LOGID-16559929 member	hikki-chan
c372357e-cfb8-11ee-bc68-...	member	hikki-chan

名前	変更日	サイズ
Autofill	今日 13:43	--
Brave_Default.txt	今日 13:43	3 KB
Google Chrome_Default.txt	今日 13:38	20 KB
Microsoft Edge_Autofill.txt	2024/03/16 19:57	20 KB
Microsoft Edge_Default.txt	2024/03/16 19:57	21 KB
Microsoft Edge_Payments.txt	2024/03/16 19:57	20 KB
blockchain.com	今日 13:35	--
Cookies	今日 13:35	--
Brave_Default.txt	2024/03/16 19:57	57 KB
Google Chrome_Default.txt	2024/03/16 19:57	796 KB
Microsoft Edge_Default.txt	2024/03/16 19:57	648 KB
domain detect.txt	2024/03/16 20:01	44 バイト
Downloads	今日 13:35	--
GoogleAccounts	今日 13:35	--
Google Chrome_Default.txt	2024/03/16 19:57	252...イト
information.txt	今日 14:43	6 KB
passwords.txt	2024/03/17 14:35	5 KB

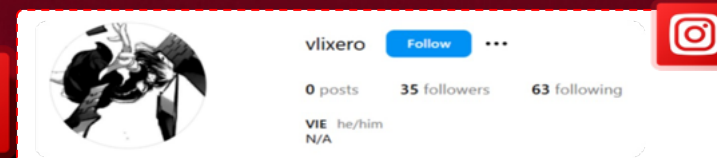
SKYPE

Registered : true

Id : live:.cid.f26bb24e76db1ad1

Name : Real Rey

Username : live:.cid.f26bb24e76db1ad1



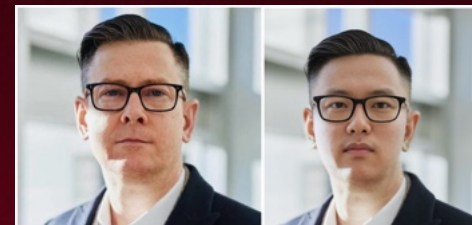
2. 北朝鮮IT労働者のケース

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）

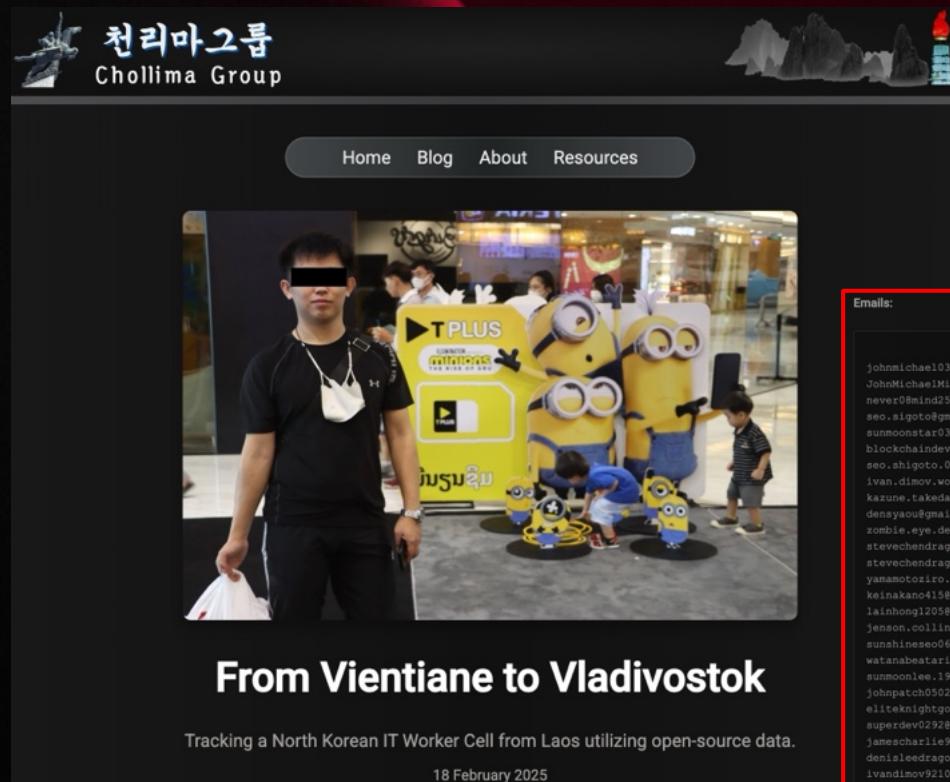
制裁をかいくぐるためにディープフェイクを用いて顔写真を偽造していた件は生成AIの悪用例として知られている



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

北朝鮮動向を追跡する研究者グループのブログ

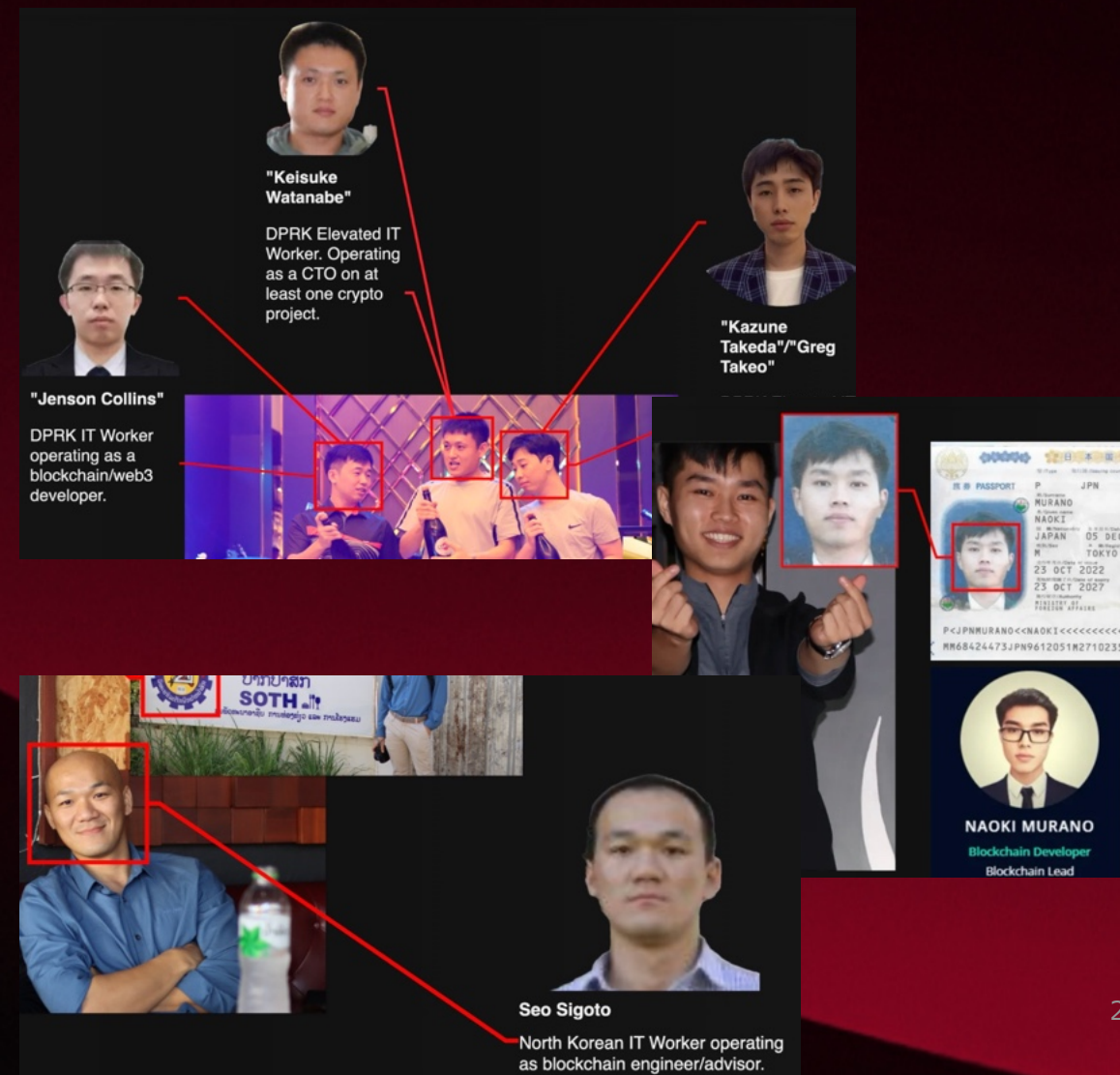


Chollima Group 2月発表のブログ
日本名を語る人物が複数登場

Emails:

- johnmichael10325@outlook.com
- JohnMichaelMillen0325@outlook.com
- never@mind25@gmail.com
- seo.sigoto@gmail.com
- sunmoonstar0319@outlook.com
- blockchaindeveloper777@gmail.com
- seo.shigoto.001@gmail.com
- ivan.dimov.work@gmail.com
- kazune.takeda@yahoo.com
- densyaou@gmail.com
- zombie.eye.dev@gmail.com
- stevechendragon@gmail.com
- stevechendragon@outlook.com
- yanamotosiro.0113@gmail.com
- keinakano415@gmail.com
- lainhong1205@gmail.com
- jenson.collins@hotmail.com
- sunshineseo0614@gmail.com
- watanabeari@gmail.com
- sunmoonlee.19900113@outlook.com
- johnpatch0502@outlook.com
- eliteknightgold@outlook.com
- superdev0292@gmail.com
- jamescharlie94@outlook.com
- denisleedragon@outlook.com
- ivandimov921016@outlook.com

ZachXNT Supplied:
0xm0neth@gmail.com



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

Search query: johnmichael0325@outlook.com OR JohnMichaelMillen0325@outlook.com OR neve 電子メール

Showing results for a 電子メール query, search instead as Free Text

Filters: ハッカーの話題, 漏洩した資格情報, インスタントメッセージ, **不正アクセスされたアカウント** (969), 侵害されたサーバー, インテリジェンス

Filter: すべてクリア, Type to search..., Fields, AssetsLens, Full Credentials

Filter: ANY TIME

Source Type: Bot Dumps, Credentials Lists, Instant Messaging

Source (3): Snatch Cloud Private ... (196), Loot Cloud Public Data (4), Fate Cloud Public Data (1)

Service (149): linkedin.com (6)

ID	Service	Username	Password	Source	Source Type	Posted Date
2GXUV23103VV6...	https://login.bitdefender.com/central/sig...	yamamotoziro.0113@...	Y@m@m0t0	Snatch Cloud Priv...	Bot Dumps	Oct 17, 2024
2GXUV23103VV6...	https://read-ebooks.club/sl-S1B8Q-D7256...	yamamotoziro.0113@...	YHT.bWEwQ99pZ5	Snatch Cloud Priv...	Bot Dumps	Oct 17, 2024
2GXUV23103VV6...	https://mynavi.agentsearch.jp/login/	seo.sigoto@gmail.com	FG@/M_ENwq/Ga-7	Snatch Cloud Priv...	Bot Dumps	Oct 17, 2024
2GXUV23103VV6...	https://twitter.com/login	seo.shigoto.001@gma...	sigotopw01@	Snatch Cloud Priv...	Bot Dumps	Oct 17, 2024
2GXUV23103VV6...	https://0xcocobets.com/register	yamamotoziro.0113@...	5nh7awZT6T@G@cu	Snatch Cloud Priv...	Bot Dumps	Oct 17, 2024
2GXUV23103VV6...	https://hashhub-research.com/	yamamotoziro.0113@...	Vv@ESde2wv7cn4q	Snatch Cloud Priv...	Bot Dumps	Oct 17, 2024
2GXUV23103VV6...	https://login.oracle.com/mysso/signon.jsp	yamamotoziro.0113@...	+nw\$mEy42/A8W=Q	Snatch Cloud Priv...	Bot Dumps	Oct 17, 2024
2GXUV23103VV6...	https://www.inflearn.com/user/signin	yamamotoziro.0113@...	P@ssw0rd	Snatch Cloud Priv...	Bot Dumps	Oct 17, 2024
2GXUV23103VV6...	https://app.clickup.com/signup	ivan.dimov.work@gm...	P@ssw0rd	Snatch Cloud Priv...	Bot Dumps	Oct 17, 2024
2GXUV23103VV6...	https://tenshoku.mynavi.jp/authenticate/	ivan.dimov.work@gm...	/*D8zJP4u2HfUA9	Snatch Cloud Priv...	Bot Dumps	Oct 17, 2024
2GXUV23103VV6...	https://www.wantedly.com/signin_or_sig...	stevechendragon@gm...	Security!2024	Snatch Cloud Priv...	Bot Dumps	Oct 17, 2024

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

フィルター条件に一致した 201 / 969 結果

Q ID	Service	Username	Password	Q Source	Source Type
2GXUV23103VV6...	https://login.bitdefender.com/central/sig...	yamamotoziro.0113@...	Y@m@m0t0	Snatch Cloud Priv...	Bot Dumps
2GXUV23103VV6...	https://read-ebooks.club/sl-S1B8Q-D7256...	yamamotoziro.0113@...	YHT.bWEwgQ99pZ5	Snatch Cloud Priv...	Bot Dumps
2GXUV23103VV6...	https://mynavi.agentsearch.jp/login/	seo.sigoto@gmail.com	FG@/M_ENwq/Ga-7	Snatch Cloud Priv...	Bot Dumps
2GXUV23103VV6...	https://twitter.com/login	seo.shigoto.001@gma...	sigotopw01@	Snatch Cloud Priv...	Bot Dumps
2GXUV23103VV6...	https://0xcocobets.com/register	yamamotoziro.0113@...	5nh7awZT6T@G@cu	Snatch Cloud Priv...	Bot Dumps
2GXUV23103VV6...	https://hashhub-research.com/	yamamotoziro.0113@...	Vv@ESde2wv7c	Snatch Cloud Priv...	Bot Dumps
2GXUV23103VV6...	https://login.oracle.com/mysso/signon.jsp	yamamotoziro.0113@...	+nw\$mEy42/A8	Snatch Cloud Priv...	Bot Dumps
2GXUV23103VV6...	https://www.inflearn.com/user/signin	yamamotoziro.0113@...	P@ssw0rd	Snatch Cloud Priv...	Bot Dumps
2GXUV23103VV6...	https://app.clickup.com/signup	ivan.dimov.work@gm...	P@ssw0rd	Snatch Cloud Priv...	Bot Dumps

ソースの詳細
◆ ソース名 Snatch Cloud Private Data
📎 Source File JP_50.7.159.34_2024-10-17 1...
Source fi

名前

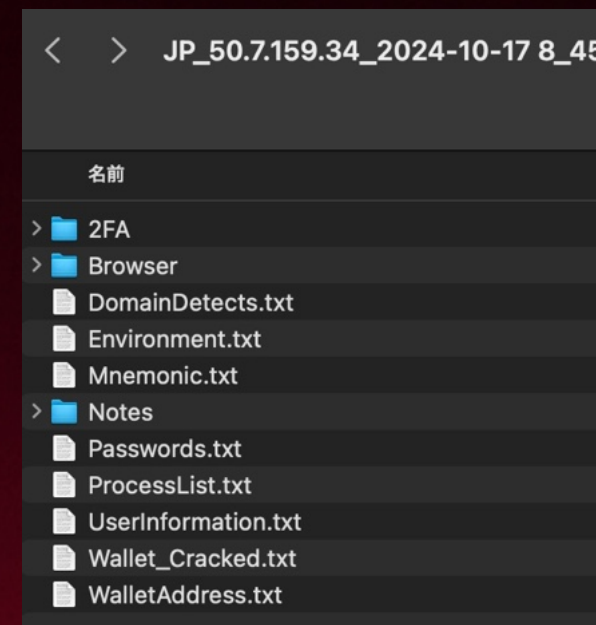
- > JP_50.7.159.34_2024-7-21 22_49_1_23OSKI6KKPWVZGQ61W8
- JP_50.7.159.34_2024-7-21 22_49_1_23OSKI6KKPWVZGQ61W8.zip
- > JP_50.7.159.34_2024-10-17 8_45_34_2GXUV23103VV628QQ55
- JP_50.7.159.34_2024-10-17 8_45_34_2GXUV23103VV628QQ55.zip
- > JP[FBA488FE01E172775BB73E7B9D9B9826] [2021-08-30T23_13_01.2637440]
- JP[FBA488FE01E172775BB73E7B9D9B9826] [2021-08-30T23_13_01.2637440].zip
- > US_23.106.169.120_2023_09_06_17_29_21
- US_23.106.169.120_2023_09_06_17_29_21.zip

- 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

Contact

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

Email
khorosuzuki0918@outlook.com

Address
Osaka, Japan

Education

Apr 2013 - Mar 2017
**Bachelor's degree,
Computer Science.**
Meiji University

Expertise

- Solidity

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.

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@...com
Password: password
```

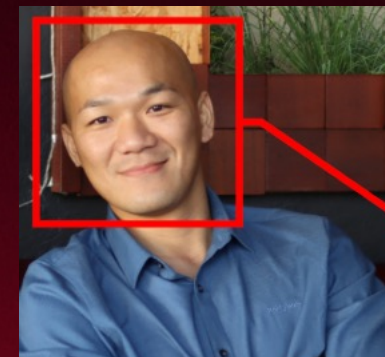
```
URL: http://52.69.70.108:8088/login
Username: a.saitoh119@...com
Password: password
```

```
URL: https://www.blockchain-sentry.com/
Username: seo.sigoto@gmail.com
Password: blockchainsentryP@ssw0rd
```

```
URL: https://br...com/login
Username: a.saitoh119@...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]_Profit
=====
URL: http://13.114.140.231:8088/reg
Username: a.saitoh11@...com
Password: password
```



開発業務従事者の
正体はSeo Sigoto

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、ライターをしています、
seo.sigotoと申します。
～出来る事・スキル～
[https://crowdworks.jp/public/employees/376\[REDACTED\]occupations](https://crowdworks.jp/public/employees/376[REDACTED]occupations)
ポートフォリオ・実績
[https://crowdworks.jp/public/employees/376\[REDACTED\]resumes](https://crowdworks.jp/public/employees/376[REDACTED]resumes)

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://hor[REDACTED].m/)
[https://www.\[REDACTED\]mecreamery.ca/](https://www.[REDACTED]mecreamery.ca/)
フロントはVue.jsのVuetyfyとBSVueを利用しバックエンドはPHPのLaravelを主に利用して
ブさせました。
【提供できるいくつかのメリット】

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て対応できま

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

ワーカープロフィール

Seo(徐)
個人 / 男性 / 30代後半 (千葉県)
最終アクセス: 18日前

♡ありがとう 119

本人確認済み
NDA締結済み
インボイス発行事業者確認済み

☆ 総合評価 4.5
評価件数 16件

☆ 総合評価 4.5
(16件の評価)

☆ 受注実績 30件

自己紹介
プロフィールを見てくださって本当にありがとうございます。
当社は20、30代ベンチャー開発チームとしてウェブ2、ウェブ3、ブロックチェーン業界で活躍しており、最近では生成AIのシステム開発を進めております。
クライアントのリクエストに責任を持って最後まで応えるのをモットとして、当社では、一般的なプログラム下請けの対応はもちろん、追加のアイデアも提供しております。あらゆるメンテナンスと更新をあらかじめ考え、最適なシステムを提案、開発することを肝に銘じ、一つ一つの案件に取り組んでいます。
世界一流のプロとして、迅速な対応と正確な納品、厳格な作業管理のスタイルを行っています。最新技術と迅速な対応で、お客様のニーズに最適にお応えできるので、案件やお見積もりのご相談を承れることを楽しみにしております。

評価

スキル	評価
スキル	4.5 ★★★★★
クオリティ	4.5 ★★★★★
スケジュール	4.5 ★★★★★
コミュニケーション	4.5 ★★★★★
パートナーシップ	4.5 ★★★★★

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、そのうち一つのは、アダルトグッズ販売・エンターテイン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）

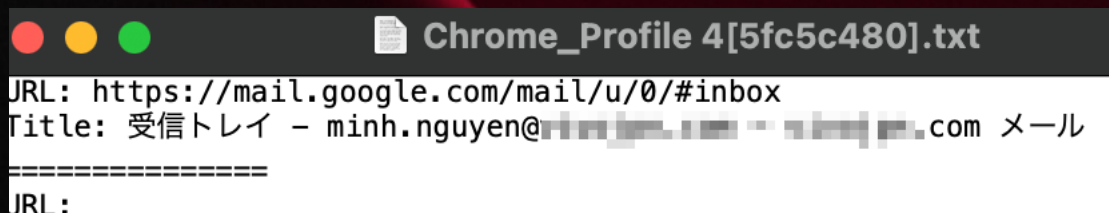
```
Chrome_Profile 3[cc638061].txt - 編集
URL: https://mail.google.com/mail/u/0/#inbox
Title: 受信トレイ - pham@fun - メール
=====
URL: https://app.slack.com/client/T016CRWKMJC/D06SBEN56L
Title: pham (DM) - Slack
=====
URL: https://www.notion.so/withny/04b908b93fec4bd6aba145
v=9a28050d81ce46d7b94617cec1fd75f4
Title: (1) withny wiki | Home
=====
URL: https://translate.google.com/
Title: Google 翻訳
=====
URL: https://github.com/
Title: GitHub
=====
URL: https://github.com/withny/fun
Title: withny
=====
URL: https://github.com/withny/un/next -frontend
Title: withny/un/next -frontend
=====
URL: https://ap-northeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1
Title: Clusters | Elastic Container Service | ap-northeast-1
=====
URL: https://chat.openai.com/
Title: ChatGPT
=====
URL: https://f.ieyasu.com/login
Title: HRMOS勤怠 by IEYASU | 勤怠管理システム
=====
URL: https://staging.api.fun/api-docs/
Title: Swagger UI
```



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



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上の企業プロフィール管理ツール）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）の企業プロフィー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）



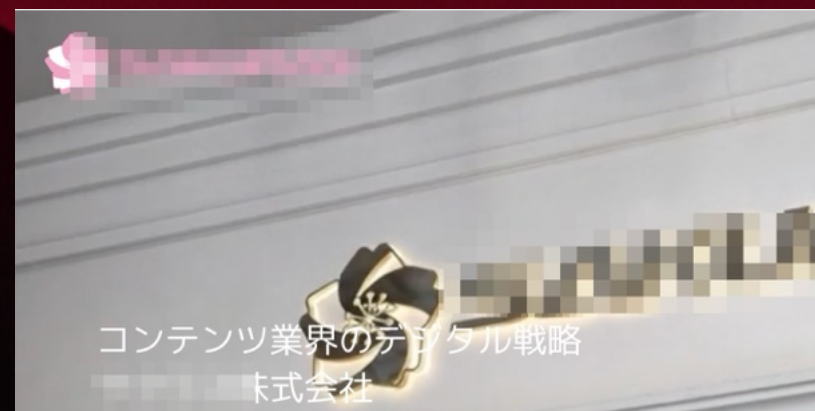
ブックマークにのこされていた痕跡(3)

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@  メール
=====
URL: https://app.slack.com/client/T014C4K625B/C014S4MDCBT
Title: general (Channel) -  Slack
=====
URL: https://github.com/
Title:
=====
URL: https://www.notion.so/ /00ce2518a9a94c0983ea5e3
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) - hp73c 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_0bnTmG5WRaITlu5hrvN069-yEAK
Title: マス_スタートアップマニュアル - Google ドキュメント
```



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イ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、さまざまな業種・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