「先読み」の鍵：
アジア最前線・台湾から読み解くサイバー脅威動向

2026.05.15 CyCraft Day

PK Tsung | CISO 兼共同創業者

CYCRAFT

本日のアジェンダ

01 直近の攻撃手法動向

台湾で観測された 5 つの主要な攻撃パターン

02 Silver Fox 事例

中国発 APT 攻撃の日本への波及

03 台湾政府機関の事例

実際の侵入事例とランサムウェアの比較

01

直近の攻撃手法動向

台湾で観測された５つの主要な攻撃パターン。

Overview

最近観測される主要な攻撃手法

01 Living off the Land

正規ツールを悪用し、悪意のあるコマンド実行および C2 通信。

02 Initial Access Broker

窃取したデジタル資産をダークウェブで販売し、地下経済の形成を助長。

03 Supply Chain Attack

PyPI、npm、Chrome 拡張機能が侵害され、正規コンポーネントを置き換える攻撃の急増。

04 AI Abuse

権限悪用、ツール利用、またはプロンプトインジェクション等の AI 機能悪用、および攻撃の自動化。

Living off the Land × Infrastructure-Less 攻撃

自前インフラの構築から、正規サービスの悪用へと変化

自前インフラに依存せず、正規クラウドサービスやCDN、侵害済みサイトを C2 として悪用。攻撃通信を正常トラフィックに混在させることで、既存防御策による検知を回避。

Type 1
Cloud Service
Microsoft Graph API → GRAPHBROTLI / GRAPHRELOOK

Type 2
C2 behind Cloudflare
RCREMARK を用い、Cloudflare 経由で攻撃者の C2 を隠蔽

Type 3
Compromised Website
侵害済みの正規サイトへ setup.py をアップロードし、マルウェアを配布

ケーススタディ：中国系 APT による政府・製造業への攻撃

観測された攻撃トレンド

- 中国系 APT による政府・製造業を標的としたスパイ活動。
- 正規のパブリックサービスを C2 として悪用。
- ESC の脆弱性を突き、AD 管理者の権限へ昇格。
- ログオンスクリプトを介したマルウェア配布。
- BYOVD（Bring Your Own Vulnerable Driver）手法の一般化 （例：Silver Fox による攻撃活動）。

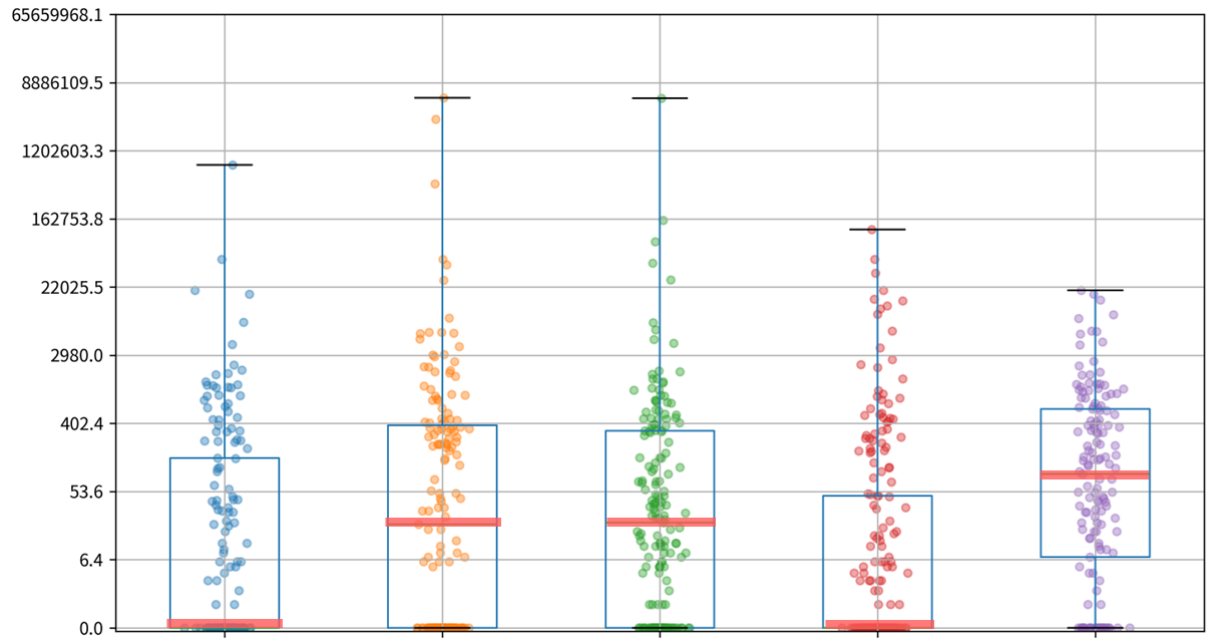
認証情報の流出が攻撃者にとって有利な足がかりに

849
分析対象ドメイン数

67%
認証情報の流出を確認

5 個
東アジアの国を対象

3 ヶ月
調査期間



KEY INSIGHTS

台湾
政府ドメインでの突出した流出量を観測。
地政学的な影響による標的化を反映。

日本・韓国
特定企業における大規模な情報流出を確認。
特にコンシューマー電子機器産業に集中。

シンガポール
調査地域で最も低い流出率。
ガバナンスによる成果を反映。

調査対象地域における認証情報流出の分布 (HK / JP / KR / SG / TW)

APT サプライチェーン：ツールとインフラの共有 (Medusa Malware Supplier)

攻撃側サプライチェーンの成熟と高度化。専門のサプライヤーがマルウェアの販売に加え、カスタマーサービスも提供。
複数の APT による同一ツール・インフラの共有により、追跡とアトリビューションは一層困難に。

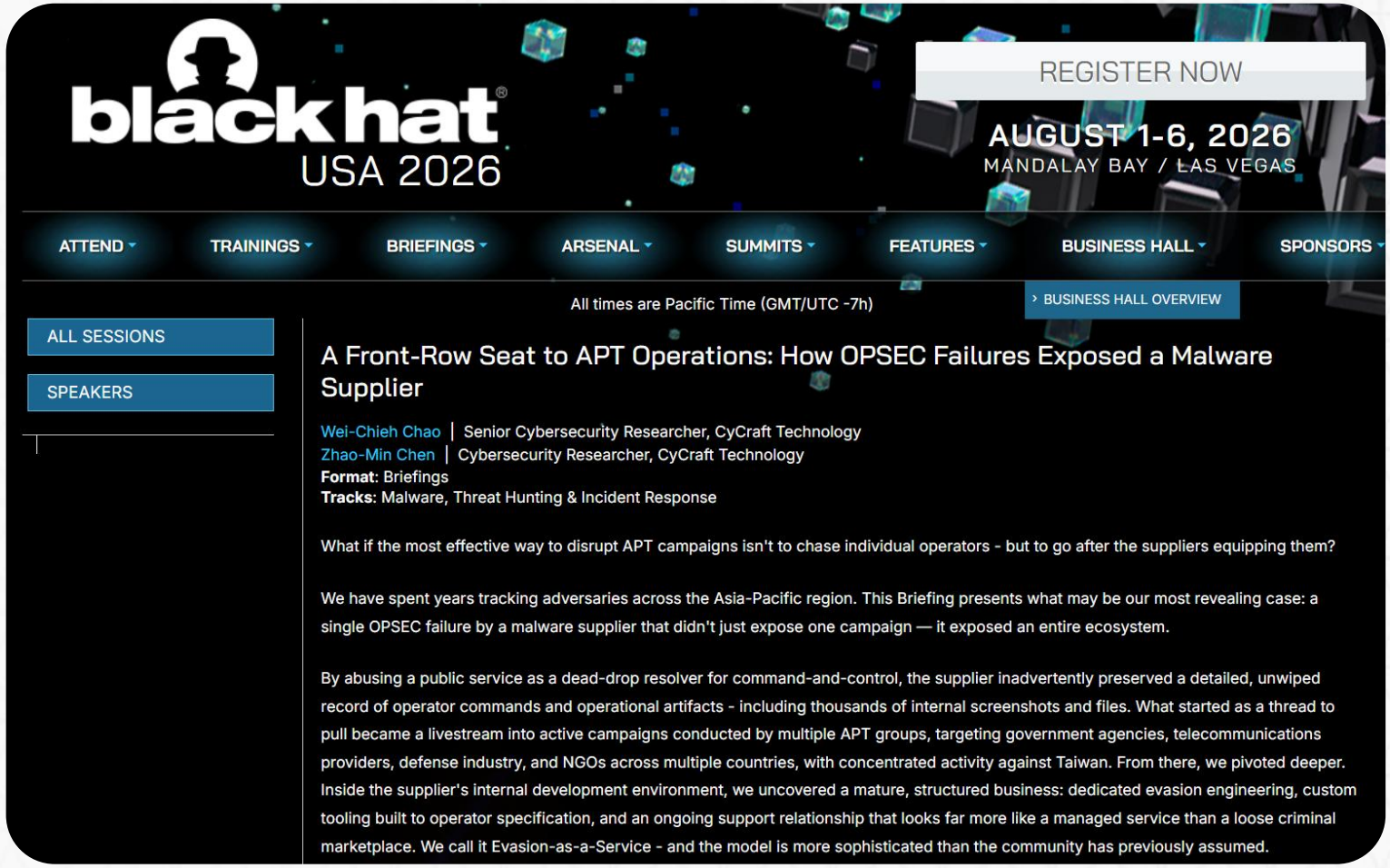
マルウェア サプライヤー →

PT-01	PT-02	PT-03	PT-04
ダウンストリーム APT 東南アジア	**ダウンストリーム APT** 台湾	**ダウンストリーム APT** グローバル	**ダウンストリーム APT** 中東

ダウンストリーム APT による、共通サプライヤーからのマルウェアとツール購入。

46	77	409	1,711	2,006
GitHub リポジトリ	ドメイン	エンドポイント	漏えいしたファイル	スクリーンショット

Medusa Malware Supplier に関する詳細は、
今年の Black Hat USA に採択され、8 月頃に米国にて発表予定。



https://blackhat.com/us-26/briefings/schedule/index.html#a-front-row-seat-to-apt-operations-how-opsec-failures-exposed-a-malware-supplier-51877

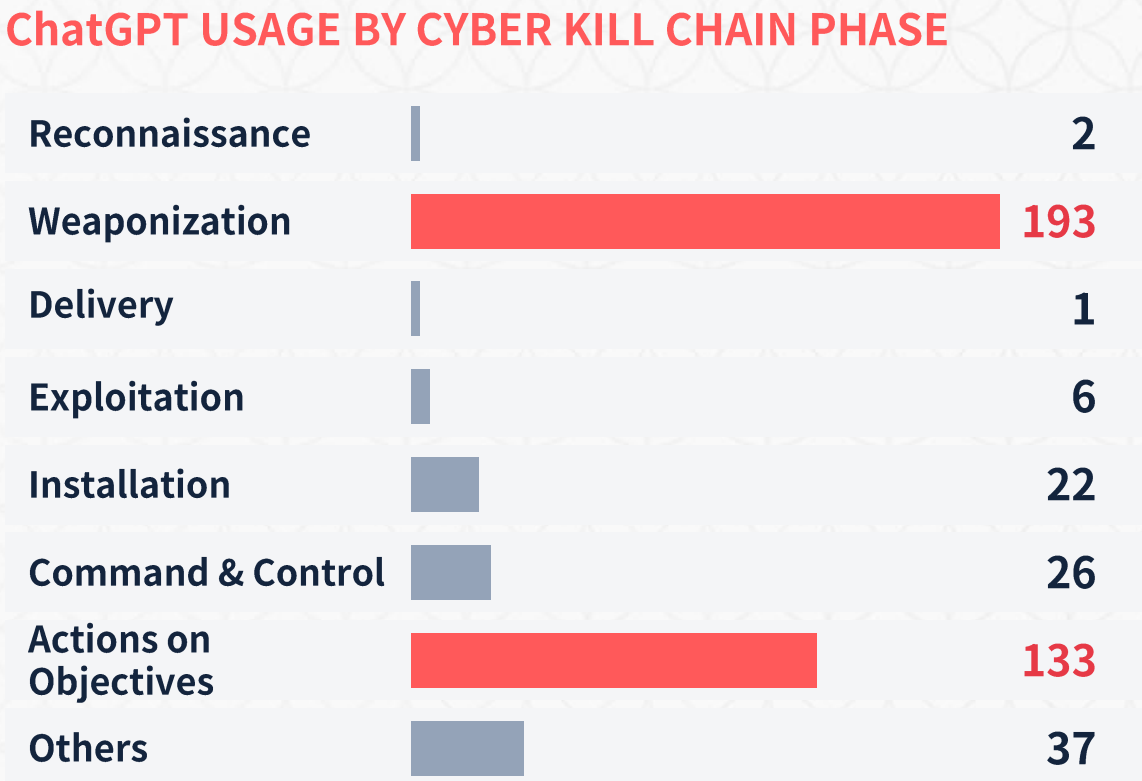
APT 攻撃における AI 応用の現状

AI 開発支援による
マルウェア・イテレーションの加速

悪意のある AI エージェントや LLM による直接的な攻撃のみならず、無料版 ChatGPT を日常的な「開発支援ツール」として大量利用している実態を観測。

攻撃者が最も AI を活用するフェーズ：「武器化（Weaponization）」

マルウェア開発における AI 支援の主流化。
高度な自動化技術はもはや一部のレッドチームに限られたものではなく、攻撃者全体の能力を底上げしている。



AI 時代の攻防加速

AI による攻撃側・防御側の進化

AI は攻撃側のスピードを加速させるだけでなく、防御側にも同等の速度での対応が求められる。

攻撃側：Malware から Promptware への変化

「Promptware」の台頭

- **AI as Infrastructure**：AI サービスを攻撃プロセスに不可欠なコンポーネントとして組み込み。
- **Just-in-Time Malice**：悪意ある指示を実行段階で動的に生成。従来の YARA ルール等による検知を無効化。
- **Evasion of AI Analysis**：対抗的プロンプトを用い、次世代 AI セキュリティ分析を突破。

防御側：AI による自動化と対応の加速

AI 駆動による防御の進化

- **Breach Attack Simulation**：デフォルトスクリプトから自律型エージェントへ。
- **AI Agent**：ネットワーク環境内の高価値資産への攻撃パスと脆弱性の自動探索。
- **インテリジェンスと分析の自動化**：脅威情報の収集から相関分析までを自動化し、防御のスピードを攻撃側の進化に同調。

Breach Attack Simulation (BAS)

防御側の進化：スクリプトから自律型エージェントへ

Breach Attack Simulation は、「デフォルトスクリプトの反復実行」から「AI エージェントによる自律探索」へと進化しており、防御側は高価値な攻撃パスを事前に発見することが可能となる。

従来の方式

デフォルトスクリプトの反復実行

- 人手による固定的な攻撃スクリプトに依存。
- 網羅性はプレイブックの範囲に依存。
- 想定外の組み合わせによる攻撃パスの発見困難。
- 検証頻度は人的リソースに依存。

→

AI 駆動

AI 駆動の自律型 BAS エージェント

- AI エージェントによる攻撃チェーンと条件の自動推論。
- 高価値な攻撃パスの継続的かつ自動的な発見。
- 組み合わせ型・想定外の攻撃設定の探索。
- 人的リソースに依存しない検証頻度。

AI 攻撃の高速化に対し、AI 防御も加速しなければならない。鍵となるのは「迅速な対応」。

PIVOT

台湾で観測されたこれらのトレンドは、日本にとっての「早期警戒」となる。

ここからは、Silver Fox と台湾政府への攻撃事例を具体的に掘り下げ、
ケーススタディとして紹介する。

02

ケーススタディ：Silver Fox

中国系 APT の拡張軌跡：中国国内 → 台湾 → 日本。
中国国内の財務型詐欺から、アジア各地における
国家支援型のサイバースパイ活動へ。

ケーススタディ

Silver Fox とは？

脅威アクター

Silver Fox

別名

Void Arachne・Monarch Spider
SwimSnake・Valley Thief
UTG-Q-1000

主要な TTP

SEO ポイズニング・フィッシングメール・ソーシャルエンジニアリング

BYOVD・ValleyRAT・WinOS 4.0

攻撃ターゲットの変遷

- **早期：収益獲得期**
  中国国内のユーザーおよび企業を標的とした
  情報の窃取・詐欺活動。
- **中後期：サイバースパイ活動への転換**
  国家級のサイバースパイ活動へと変貌。
  ターゲットを台湾および他のアジア地域へシフト。
- **2025 年：日本への拡張**
  日本企業を標的としたフィッシングメール。
  税務機関や人事部門を装った巧妙なテーマで誘引。

ケーススタディ

Silver Fox の進化タイムライン

2008 年の Gh0st RAT ソースコード流出から、2025 年の日本企業への拡張まで。

2023
初登場
中国国内での窃取・詐欺活動

2024
大規模活動
SEO ポイズニング・フィッシング

2025
アジアへ進出・スパイ活動
台湾、日本企業が標的に

2008
Gh0st RAT
ソースコード公開

2023/02
Qi-Anxin
「谷堕大盗」を発見

2023/09
Proofpoint
ValleyRAT と命名

2024/06
Valley RAT
ソースコード流出

2024/06
トレンドマイクロ
大規模な
SEO ポイズニング

2025/01
Fortinet
台湾企業への
フィッシング攻撃

2025/10
日本拡張
日本企業への
フィッシング攻撃

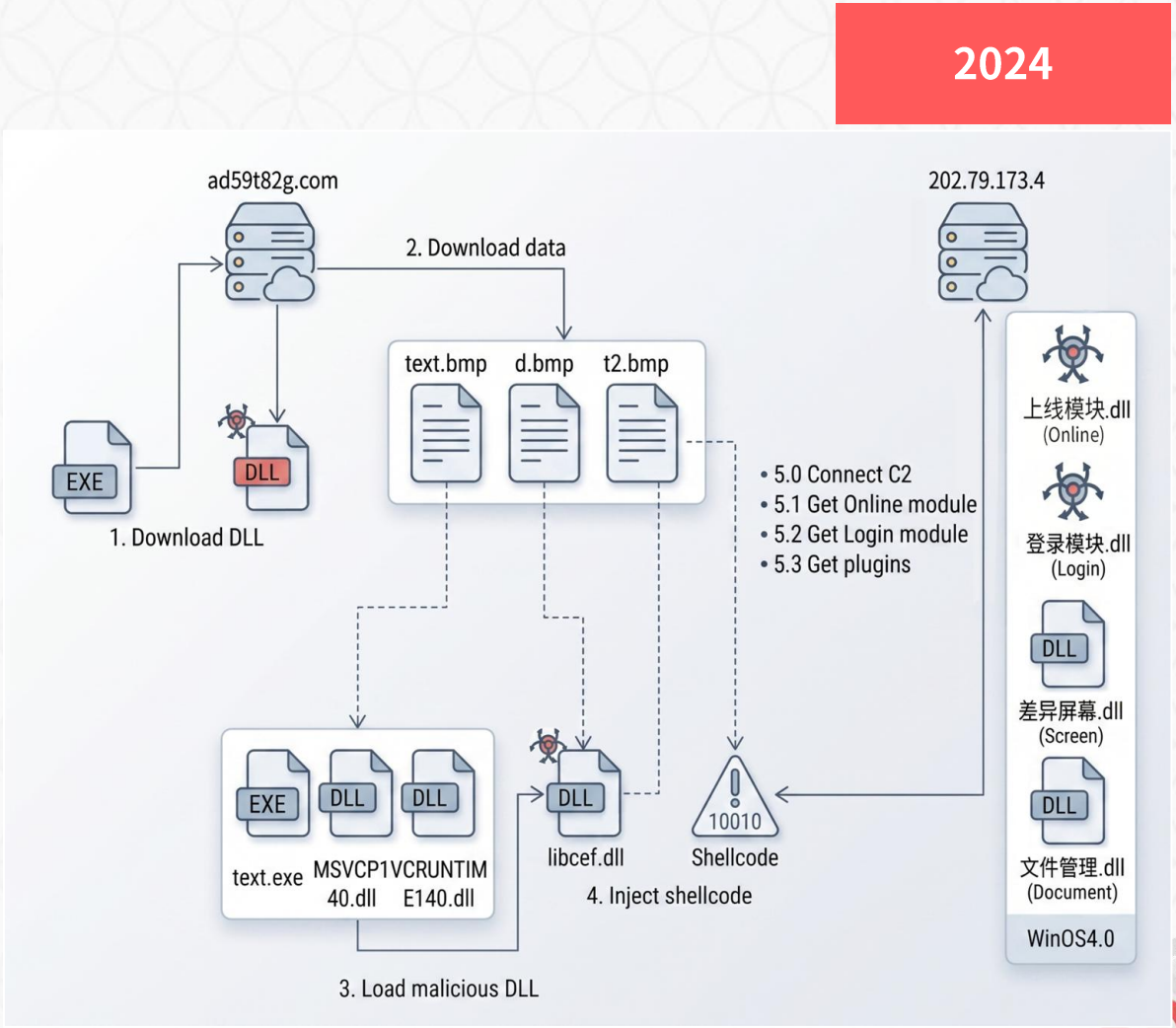
攻撃手法 01 / 04

SEO ポイズニング

2024

OBSERVATIONS

1. 主に海賊版ゲームやソフトを通じて拡散。
2. 主に中国語を使うユーザー（基本は中国国内）を攻撃。
3. VPN や AI 画像処理アプリが一般的な偽装対象



攻撃手法 02 / 04

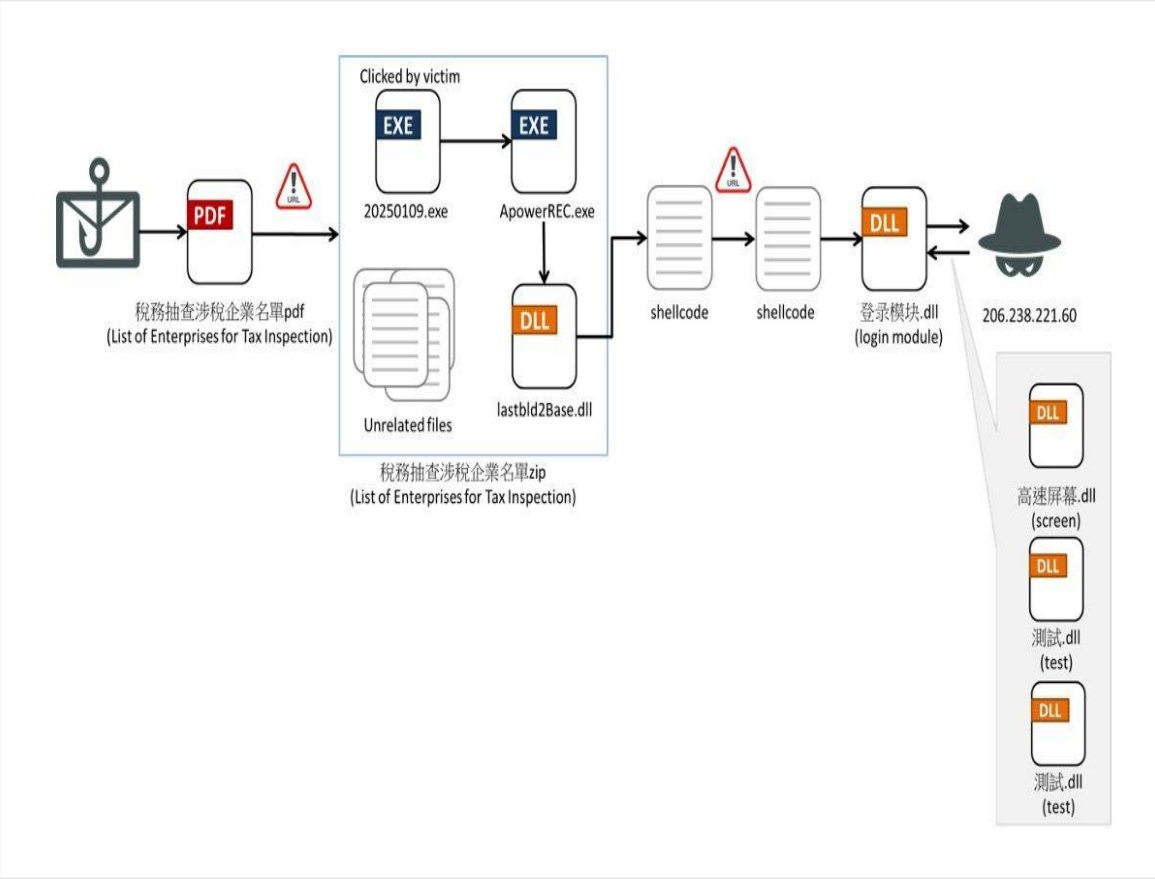
台湾の国税局を装った偽メール

2025 / 01

2025/01

OBSERVATIONS

1. 台湾企業の財務担当者を標的に。
2. 国税局を装った「税務監査通知」のフィッシングメールを送信。
3. 添付ファイルのダウンロードを誘い、ValleyRAT（バックドア）をインストールさせる。



CYCRAFT

攻撃手法 03 / 04

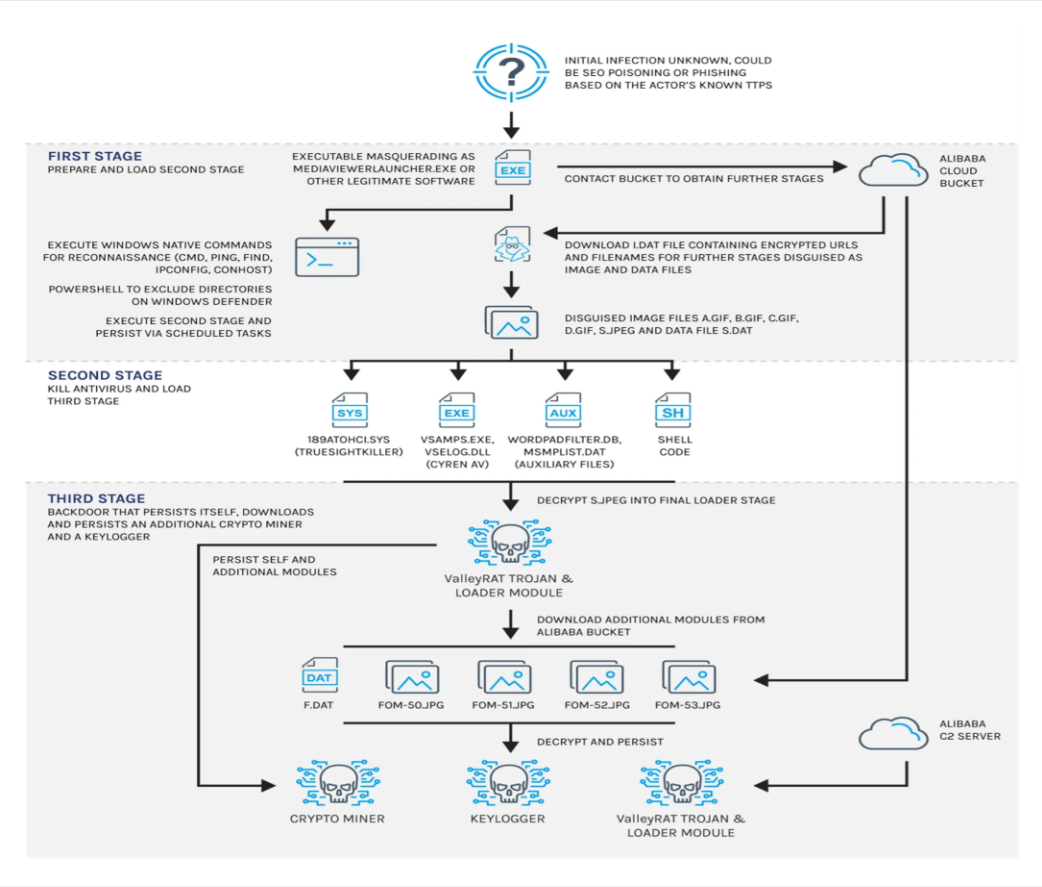
医療ソフトウェアへの攻撃

2025 / 02

2025/02

OBSERVATIONS

1. バックドアが仕込まれた Philips DICOM Viewer（医療用画像ツール）。
2. 初期アクセスは SEO ポイズニングまたはフィッシングと推測。
3. 被害範囲の拡大開始：アメリカ、カナダ、台湾、日本に及ぶ。



攻撃手法 04 / 04

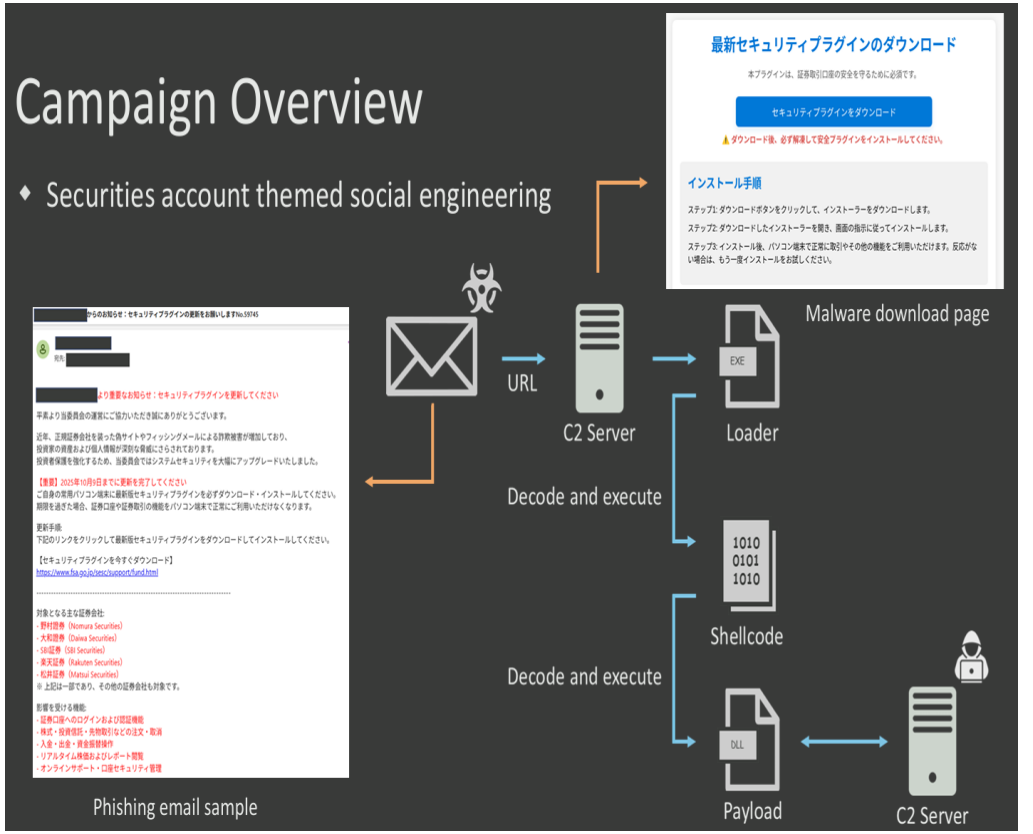
日本企業を標的としたフィッシングメール

2025 / 10

2025/10

OBSERVATIONS

1. 日本企業の従業員を対象とした税務・人事関連のフィッシングメールを送信。
2. 社内通知や財務書類を偽装。
3. 主なテーマは税務違反通知、給与改定、人事異動等。
4. 添付ファイルにより ValleyRAT をダウンロードさせる。



03

ケーススタディ：
台湾政府機関への APT 攻撃事例

システム侵害とデータ窃取の実際事例。

ケーススタディ

内部システムの把握による、正規活動への偽装

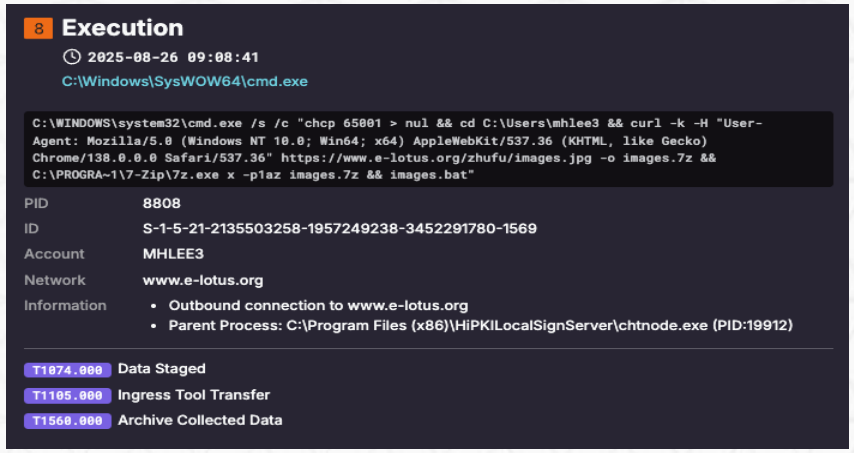
本ケースにおける攻撃者の特徴は、標的組織の内部システムの運用構造を深く把握。7-Zip を用いたデータアーカイブにより、正規のシステム活動の中へ巧妙に隠す。

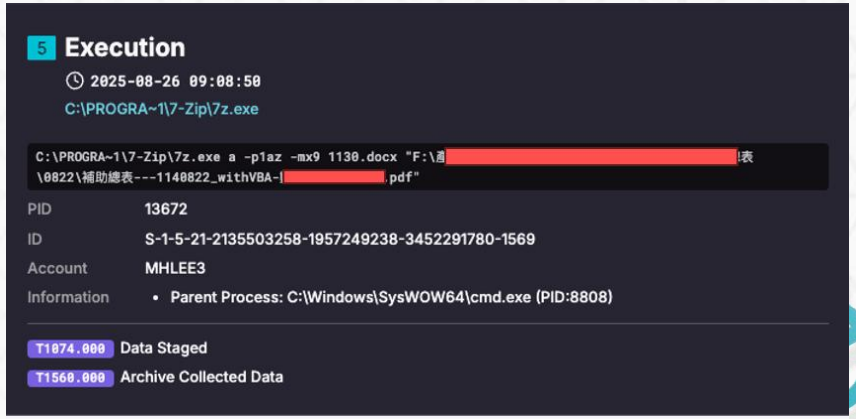
主な発見事項

- 攻撃者による組織内のソフトウェア運用の高度な把握。
- 7-Zip を用いたデータのアーカイブ。
- 悪意ある挙動を、アンチウイルスの正規プロセス（DSAgent.exe）への擬装。
- 環境内における大量の正規 7z 実行ログの存在。

悪意あるコマンドの例

```
C:\PROGRA~1\7-Zip\7z.exe a -p1az -mx9 1130.docx
"F:\XXXXX\XXXXX組\2025\資料\XXXXXX総表\0822\
補助金総表---1140822_withXXX-XXXX分析.pdf"
```





ケーススタディ・攻撃チェイン

侵入および感染手法

01 コマンドの置き換え

攻撃者による
gpupdate force.bat の
アップロード

02 悪意あるファイル
のダウンロード

5 つの正規サイトから
モジュールをダウンロード

03 AD による配布

AD サーバから
被害端末へ配布

04 最終感染

Chksrv / Chtnode /
HIPKIServer.js の実行

攻撃手法の特徴

侵害済みのサイトを悪意あるプログラムのホスティングプラットフォームとして利用。ネットワークセキュリティ製品の検知やブロックを巧妙に回避。

C2 ドメイン

www.e-lotus.org
www.meco-labor.org.tw
www.new123.com.tw
www.ie7.com.tw・cec.usc.edu.tw

感染コンポーネント

Chksrv.exe・Chtnode.exe・HIPKIServer.js など、複数の悪意あるモジュールが協調動作し、完全な攻撃チェーンを構築。

ケーススタディ・集団防衛と N-ISAC

官民連携 = 集団防衛

600,000+
リアルタイム監視エンドポイント

+10
後続の被害確認機関

1
国家 ISAC 共有ノード

事件の経緯

01 CyCraft による検知
エンドポイントから隠蔽された攻撃を観測。

02 N-ISAC への共有
昨年、情報を国家 ISAC へ提供。

03 横断的な一斉調査
政府がネットワークゲートウェイを通じて大規模調査を実施

04 追加で 10 機関を発見
さらに 10 の機関で同様の攻撃痕跡を確認。

民間企業
技術的広範性・即時可視性

＋

政府機関
ガバナンス権限・実行能力

＝

早期警戒 ＋
能動的防御

ランサムウェアランキング・台湾 × 日本

過去 3 年のランサムウェア Top 10

出典：ransomlook.io

台湾

1	**LockBit3**	OVERLAP
2	Crazyhunter Team	
3	**Ransomhub**	OVERLAP
4	**Qilin**	OVERLAP
5	Devman	
6	Nightspire	
7	Babuk-Bjorka	
8	**Space Bears**	OVERLAP
9	Fsociety	
10	Sarcoma	

日本

1	**LockBit3**	OVERLAP
2	**Qilin**	OVERLAP
3	**Ransomhub**	OVERLAP
4	8base	
5	Alphv	
6	Lynx	
7	**Space Bears**	OVERLAP
8	The Gentlemen	
9	Safepay	
10	Bianlian	

高い類似性

4

つのランサムウェアが重複

LockBit3
Qilin
Ransomhub
Space Bears

台湾・日本両国間における高い重複性：APT およびランサムウェア攻撃の類似した時系列傾向。

Key Takeaways

Key Takeaways

3 つのキーインサイト

01

「ファイルレス」および「正規ツール」への攻撃転換

攻撃者は正規のツールやサービスを悪用。認証情報を窃取し、正規ユーザーとしてシステムへログイン。従来の IoC のみでは検知困難な状況。

02

AI による攻撃の加速と、インフラ共有によるアトリビューションの困難化

AI の活用が進むことで、マルウェアのイテレーションがかつてない速さで進行。APT グループ間でのツールやインフラ共有により、追跡や攻撃主体のアトリビューションが困難に。

03

日本に対する早期警戒としての台湾

台湾はアジアにおける APT 攻撃の最前線。台湾で観測された攻撃は、数ヶ月後に日本で発生する傾向。台湾での観測事例を教訓として活用すべき。

日本企業にとって、これらの脅威の進展を継続的に注視し、
先んじて防御能力を構築することが、サイバーレジリエンス強化の鍵。

ご清聴ありがとうございました。

2026.05.15 CyCraft Day
PK Tsung | CISO 兼共同創業者
peikan.tsung@cycraft.com