# グローバル脅威調査レポート

エグゼクティブサマリー

## 忍耐強いステルス攻撃の時代は、高速の脅威の新時代に道を譲りつつあります。

当社の前年比分析では、明らかな戦略的転換が明らかになっています。敵対者はスピードを重視して再構築し、AIを武器にして新たな脅威を大規模に生み出し、長時間のステルスよりも即時実行を優先します。この加速により、防御側は数か月ではなく数分で測定される攻撃ライフサイクルに適応せざるを得なくなります。リアルタイムデータと履歴データの両方から導き出される、迅速で状況に応じた意思決定が効果的な防御の鍵となっています。

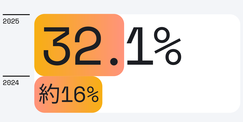
## Elastic Security Labsの2025年Elastic グローバル脅威レポートは、この新しい状況を詳しく分析しています。

グローバルな脅威テレメトリーの分析に基づき、敵の行動と防御のイノベーションを特定しました。以下の内容について論じます。

＃01

### Windowsにおける攻撃者の優先順位は逆転

**実行**の戦術カテゴリーが悪意のある動作の**32.1%**を占めるようになり（以前のシェア約16%から倍増）、**防御回避**を上回りトップの戦術となりました。これは3年間のトレンドを崩し、初期の隠密性から即時ペイロード導入への戦略的シフトを示しています。




**防御側への示唆**

→ 攻撃者はもはや隠れるのを待つことはなく、侵入後すぐに悪意のあるコードを実行することに集中しています。そのため、ランタイムメモリ保護と初期アクセス阻止がこれまで以上に重要になります。

＃02

### クラウドの攻撃対象領域は非常に集中


**すべてのクラウドセキュリティイベントの60%以上で、**攻撃者の目的は次の3点に集約されます。

攻撃者の目的

/初期アクセス
/永続化
/認証情報アクセス

**防御側への示唆**

→ すべての主要なクラウドプラットフォームにおいて、この**IDベースの攻撃**への注力は、認証フローを強化し、異常な特権アクセスを監視することが、クラウドワークロードを防御する最も効果的な方法であることを明確に示しています。

＃03

### AIの武器化が増加傾向

**+15.5%**

**「汎用型」脅威の15.5%の増加**を観測しました。これは、敵対者が大規模言語モデル（LLM）を使用して、シンプルながら効果的な悪意のあるローダーやツールを迅速に生成していることを示す傾向である可能性が高いです。

**防御側への示唆**

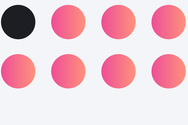
→ AI生成の脅威の増加により、直面するマルウェアの量と種類が劇的に増加します。これは、静的シグネチャに頼る割合が減少し、**行動分析とAI主導の検出**により、大規模な新たな脅威の洪水を自動的に特定し、阻止する必要があることを意味します。

＃04

### ブラウザーの認証情報盗難が一大ビジネスに

8件に1件以上

ブラウザーデータを盗むために設計



**15万件**を超えるマルウェアサンプルの分析により、**8件に1件以上がブラウザーデータを盗むように設計されている**ことが明らかになりました。これは単独で使用されるものではなく、これらの認証情報は、**アクセスブローカー**経済を支える原材料であり、他の攻撃者が企業のクラウドアカウントを侵害するための鍵を安定的に供給しています。

**防御側への示唆**

→ ブラウザーは組織の最も機密性の高いデータにとっての主戦場です。インフォスティーラーは搭載のブラウザー保護に適応しており、従来のID制御ではもはや十分ではありません。

## これらのトレンドは相互に深く関連しています。

攻撃者はAIが生成したマルウェアを使ってブラウザの認証情報を盗み、それを利用してクラウドアカウントへの初期アクセスを得ることができます。侵入後、攻撃者はすぐにランサムウェアのデプロイやデータの窃取に集中します。本レポートは、これらのTTPが現代の攻撃チェーンをどのように形成するのか、そしてさらに重要な点として、複数のポイントでそれをどのように破壊するのかを示しています。

脅威の状況は複雑ですが、マルウェアや脅威の振る舞いを理解し、高度な防御策を活用することで、組織のレジリエンスを大幅に向上させることができます。

### ステップ1
**実行を重視**

### ステップ2
**クラウドアカウントへの初期アクセスを取得**

### ステップ3
**AIが生成したマルウェアを使用**

### ステップ4
**ブラウザの認証情報を窃盗**

Elastic Securityは、今日の脅威に対処し、より安全な未来を築くために必要な共有インテリジェンス、高度な機能、洞察を提供します。