CROWDSTRIKE

攻撃者に逃げ場なし

問題なのはマルウェアではありません。問題は攻撃者です。

セキュリティチームは、脅威アクターがどう動くかを理解し、脅威アクターを阻止するために最適な位置にいることが重要です。

2023年版クラウドストライク脅威ハンティングレポートは、クラウドストライクのCounter Adversary Operationsチームによって作成されており、攻撃者の最新の手口を明らかにし、侵害阻止に役立つ知識とインサイトを提供しています。

驚異的な新しいインサイト

アイデンティティの脅威が主流に

攻撃者はアイデンティティベースの侵入を倍増させており、窃盗や侵害されたアイデンティティの悪用による影響が深刻化。

62%

侵害されたアイデンティティが関与した対話型侵入の割合

583% 増加

アイデンティティベースの攻撃手法であるKerberoasting件数

攻撃者の動きが速くなるにつれサイバー犯罪（ECRIME）が急増

攻撃者はこれまでにない速さで環境に出入りしています。

79 分

観察されたサイバー犯罪（eCrime）の平均ブレイクアウトタイム時間

7 分

観察されたサイバー犯罪（eCrime）のブレイクアウトタイムの最速記録

攻撃者はクラウドに精通してきている

脅威アクターはクラウドの専門家になりつつあります。よくみられる不適切な構成をエクスプロイトし、組み込みのクラウド管理ツールを悪用しています。

160% 増加

クラウドインスタンスメタデータAPIを介した認証情報の盗難件数

クロスプラットフォーム運用能力に注目が集まる

複数のオペレーティングシステムをカバーする運用能力が、2023年の対話型侵入の特徴です。

3倍 増加

Linuxでプラガブル認証モジュール（PAM）と悪意のあるモジュールを置き換える攻撃者数

金融、テクノロジー、サービス

最も深刻な影響のあった業界

貴社を標的にする攻撃者を発見

クラウドストライクは、その他200以上の攻撃者と合わせてこれらの攻撃者を積極的に追跡しています。2023年版脅威ハンティングレポートで詳細をご覧ください。

LABYRINTH CHOLLIMA

複数のオペレーティングシステム攻撃で先頭に立つ

VICE SPIDER

全Kerberoasting攻撃のうち27%を占有

INDRIK SPIDER

日和見的なサイバー犯罪（eCrime）からカスタマイズされた攻撃に移行

彼らを知る。彼らを見つけ出す。彼らを阻止する。

- → 当社の専門の脅威ハンターが顕著な侵入や手法について話す内容から優れたインサイトを取得
- → 実際の経験を身に付けて、セキュリティ戦略を強化し、動きの速い脅威を阻止
- → 世界的傾向と地域的傾向の両方を理解して攻撃者の一歩先を行く

レポートを入手する

CROWDSTRIKE