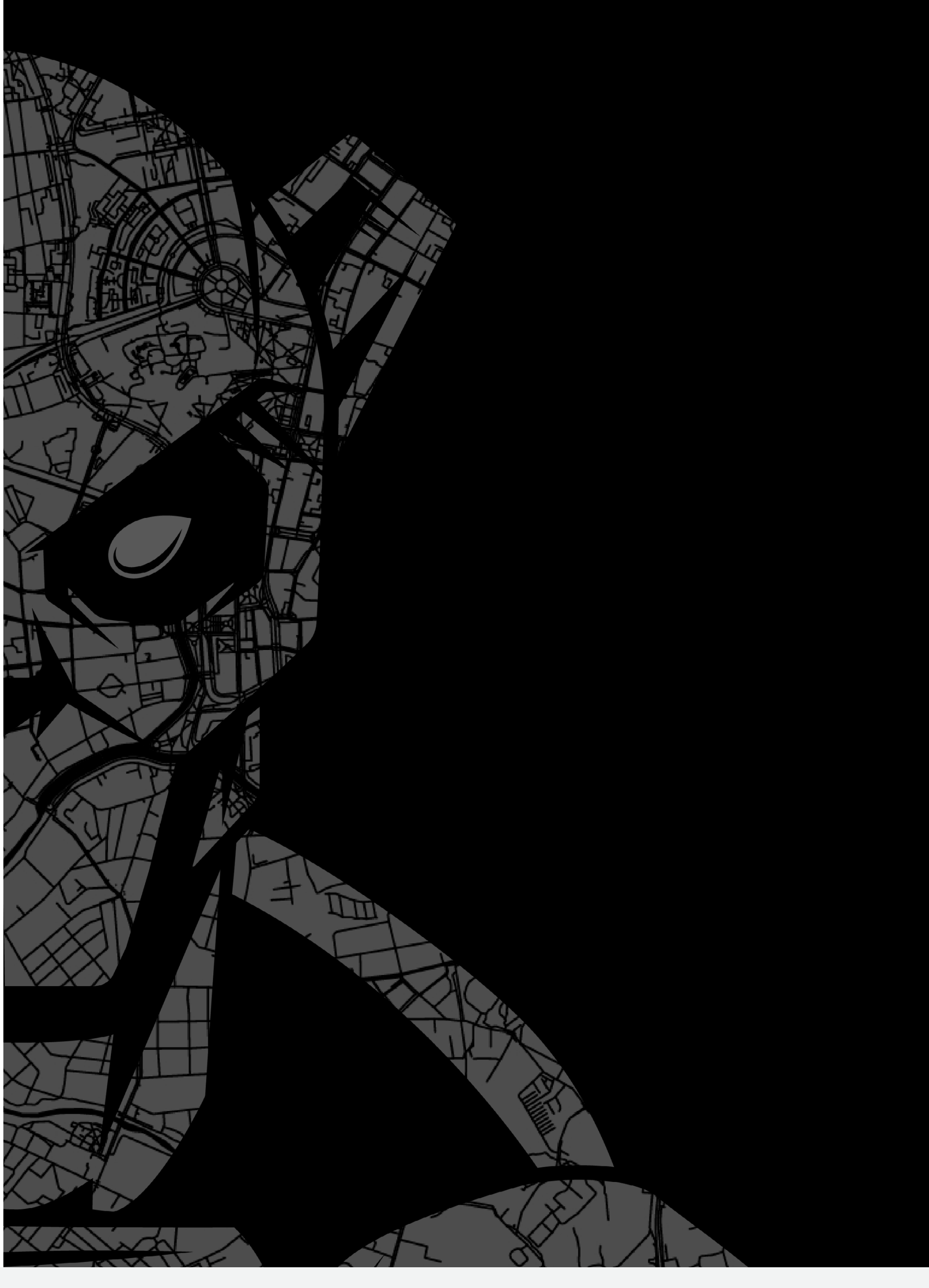
CROWDSTRIKE

2023
年版
グローバル
脅威レポート

執拗な攻撃の増加
2022 年の攻撃スピードと巧妙さ：
知っておくべきこと



クラウドストライク 2023 年版グローバル脅威レポートは、
最新の脅威の状況と進化し続ける攻撃者グループの攻撃の手口、
ならびに 2022 年における最も重要な攻撃の傾向と
その背後に潜む攻撃組織に関する包括的な分析を提供する、
業界で最も信頼されるレポートの 1 つです。

攻撃者を知る

サイバー犯罪 (ECRIME) | 国家主導型 | ハクティビスト

33 の攻撃組織が 2022 年に新たに特定

200+ の攻撃者を追跡

どこで活発な攻撃を繰り広げているのか

- テクノロジー
- 金融サービス
- ヘルスケア
- 電気通信
- 製造
- 学術
- 政府組織

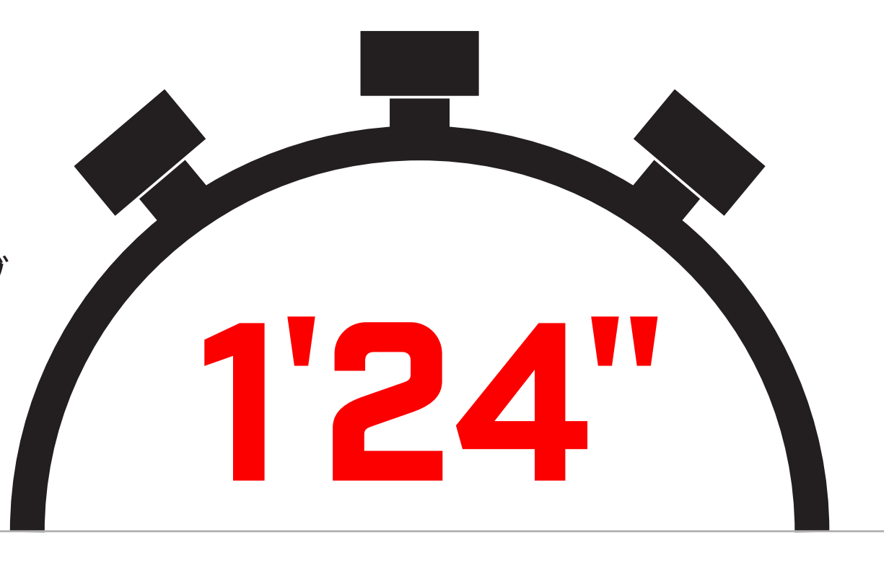
サイバー攻撃の内容

脅威の状況は 2022 年も進化し続け、攻撃者の活動により、
組織の安全確保がますます困難になっています。

98'
84'

ブレイクアウトタイムは 2 時間未満

サイバー犯罪 (eCrime) を行う攻撃者がラテラルムーブメントを開始するまでに要する時間は、1 時間 24 分で 2021 年に比べ 14 分短縮しています。



71%

の攻撃はマルウェアフリー

攻撃者の攻撃手法はマルウェアから「ハンズオンキーボード攻撃」へと移行し続けています。この傾向は、アクセスと永続化を可能にするために正規のクレデンシャルを大量に乱用することや、脆弱性を迅速に悪用する能力に関連しています。

50%

対話型攻撃キャンペーンの急増

クラウドストライクは、対話型攻撃が大幅に増加し、2022 年の第 4 四半期に急増したことを観測しました。

アクセスブローカー広告が 112% 急増

2022 年には、アクセスブローカーサービスの人気が高まり、広告も 2,500 件以上掲載され、2021 年と比較して急増しています。これはアクセスブローカーサービスに対する需要が高まっていることを裏付けています。

サイバー攻撃者の狙い

攻撃者は、2022 年、被害者のデータとインフラストラクチャを
執拗に狙っていました。

クラウドエクスプロイトインシデントの増加

95%

2022 年には、クラウド環境を狙う脅威アクターが関与する事案は 2021 年からほぼ 3 倍に増加し、サイバー犯罪 (eCrime) および国家主導型攻撃者が知識と手法を獲得して、クラウド環境を標的にする傾向が高まっていることを示しています。

データの盗難と恐喝はランサムウェアなしで継続

CrowdStrike Intelligence は、ランサムウェアを展開せずにデータの盗難や恐喝を行う攻撃者の数が 20% 増加したことを確認しました。この「二重脅迫」モデルは、ビッグゲームハンティング (BGH) を行う攻撃者の間で最も広く使われいている戦術です。

脆弱性の再利用が、公開された状態のコンポーネントを危険にさらします

2022 年に観察されたゼロデイおよび N デイの脆弱性は、攻撃者が専門知識を使用して以前のパッチが提供したリスク緩和策を回避し、同じ脆弱なコンポーネントを複数回標的にすることが可能であることを示しています。

最も活発な標的型攻撃を繰り広げるのは中国由来の攻撃者グループ

中国由来の攻撃者と、彼らと同じ戦術、技術、手順 (TTP) を使用するアクターらは、2022 年に、CrowdStrike Intelligence が追跡する 39 のグローバル産業セクターと 20 の地理的地域のほぼすべてを標的にしたと見られています。

ロシア由来の攻撃者は、ウクライナに対し軍事、心理、ハクティビスト攻撃を継続的に展開

2022 年全般を通じて、インテリジェンスの収集、インフラストラクチャの破壊、または分裂の扇動、ヨーロッパに流出する国民の感情に影響を与えることを目的としたサイバー攻撃が、これまでにないレベルで展開されたことが分かりました。

次にすべきことは？

必要なことはすべて行い、準備を整えましょう。つまり、

- > 攻撃者を知る
- > アイデンティティ保護とクラウド保護を優先する
- > 脆弱なコンポーネントにパッチを適用する
- > 戦いに備える：
  一秒が差を生む状況に備えましょう

フルレポートをダウンロード

相手の手口を知ることが
勝つための唯一の手段です。

CrowdStrike について

CrowdStrike Holdings, Inc. (Nasdaq: CRWD) はサイバーセキュリティのグローバルリーダーであり、エンドポイント、クラウドワークロード、アイデンティティ、データを含む企業におけるリスクを考える上で重要な領域を保護する世界最先端のクラウドネイティブのプラットフォームを提供して、現代のセキュリティを再定義しています。CrowdStrike Falcon® プラットフォームは、CrowdStrike Security Cloud とワールドクラスの AI を搭載し、リアルタイムの攻撃指標、脅威インテリジェンス、進化する攻撃者の戦術、企業全体からの充実したテレメトリーを活用して、超高精度の検知、自動化された保護と修復、精鋭による脅威ハンティング、優先付けられた脆弱性の可観測性を提供します。Falcon プラットフォームは、軽量なシングルエージェント・アーキテクチャを備え、クラウド上に構築されており、迅速かつスケーラブルな展開、優れた保護とパフォーマンス、複雑さの低減、短期間での価値提供を実現します。

CrowdStrike: **We stop breaches**

詳細はこちら : **https://www.crowdstrike.jp/**
ソーシャルメディア：

無料トライアル : **https://go.crowdstrike.com/try-falcon-prevent-jp.html**
© 2023 CrowdStrike, Inc. 無断複製禁止。

CROWDSTRIKE
Protection that powers you