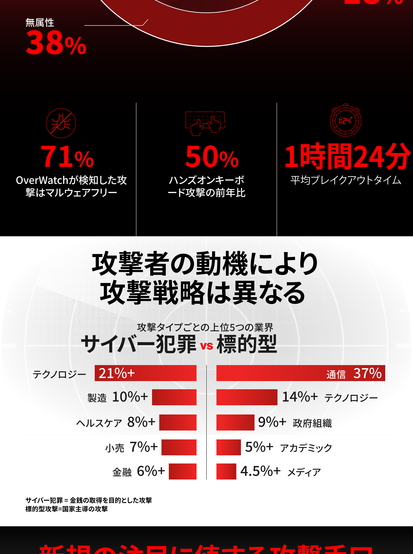
CROWDSTRIKE

攻撃者に逃げ場なし

2022年版Falcon OverWatch脅威ハンティングレポート

CrowdStrikeのプロアクティブな24/7脅威ハンティングチームFalcon OverWatch™は毎年、過去12カ月間にチームが発見した、既知および新たな攻撃者の手口、および新たな攻撃傾向の詳細な調査結果とテクニカル分析を公開しています。2021年7月1日から2022年6月30日までが含まれる 昨年度は特に、攻撃者が攻撃を設計、配備する方法に大きな変化が確認されました。

攻撃は激化、複雑さがエスカレート



71%
OverWatchが検知した攻撃はマルウェアフリー

50%
ハンズオンキーボード攻撃の前年比

1時間24分
平均ブレイクアウトタイム

攻撃者の動機により攻撃戦略は異なる

攻撃タイプごとの上位5つの業界

サイバー犯罪 vs 標的型

サイバー犯罪		標的型	
テクノロジー	21%+	通信	37%
製造	10%+	テクノロジー	14%+
ヘルスケア	8%+	政府組織	9%+
小売	7%+	アカデミック	5%+
金融	6%+	メディア	4.5%+

サイバー犯罪 = 金銭の取得を目的とした攻撃
標的型攻撃=国家主導の攻撃

新規の注目に値する攻撃手口

IceApple

目的
防御回避、クレデンシャルアクセス、データ抜き出し

標的型
IISサーバー

特徴
- .NETベースの攻撃後の巧妙なフレームワーク
- 反射的にロードされた.NETアセンブリをエクスプロイト
- フォレンジックフットプリントが小さく、メモリ内に存在する

fscan

目的
発見

標的型
内部ホスト、環境マッピング

特徴
- 2021年終盤から2022年初期に増加した攻撃ツール
- 高度なフィンガープリンティング用に転用された脆弱性スキャナ
- 公開鍵の変更、SSHコマンドを介した攻撃

Sweet Potato

目的
特権昇格

標的型
Windows OSクレデンシャル、セキュリティトークン

特徴
- システム認証に転送中の認証情報を取得するよう強制
- 最初のバリエーション「Hot Potato」は2016年に発見
- 自動化されたスクリプトは複数のバリエーション（Juicy Potato、Lonely Potato）を試行

Webサーバーゼロデイ

目的
（Web Shellを介した）永続化、対話型偵察、クレデンシャルハーベスト、データ抜き出し

標的型
Confluenceサーバーとデータセンターインスタンス

特徴
- 認証されていないリモートコード実行を可能にする脆弱性
- サイバー犯罪および標的型攻撃で観察された
- 段階的な攻撃には、Webシェルの展開、対話型偵察、クレデンシャルの収集、リモートツールの取得が含まれる

プロアクティブな脅威ハンティングは単なるツールではなく使命

手口と
攻撃者を知り
容赦なくハンティング

2022年度Falcon OverWatch脅威ハンティングレポート

完全版レポートをダウンロード

詳細：https://www.crowdstrike.jp/services/
フォローしてください！

CROWDSTRIKE

We Stop Breaches