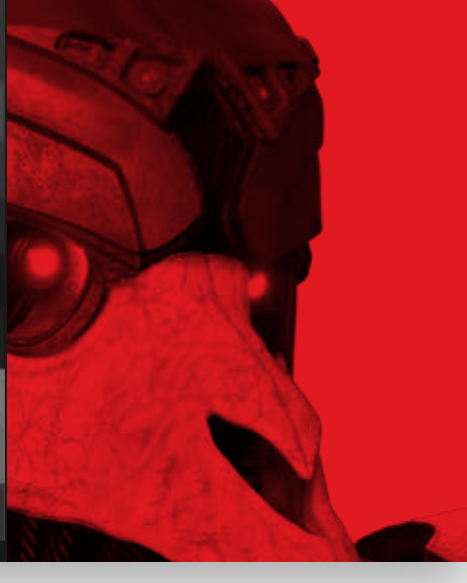


CROWDSTRIKE

攻撃者に逃げ場なし

アジア太平洋および日本（APJ）

クラウドストライク 2023年版 脅威ハンティングレポート

→ 詳細につきましては、レポート全文をダウンロードください。

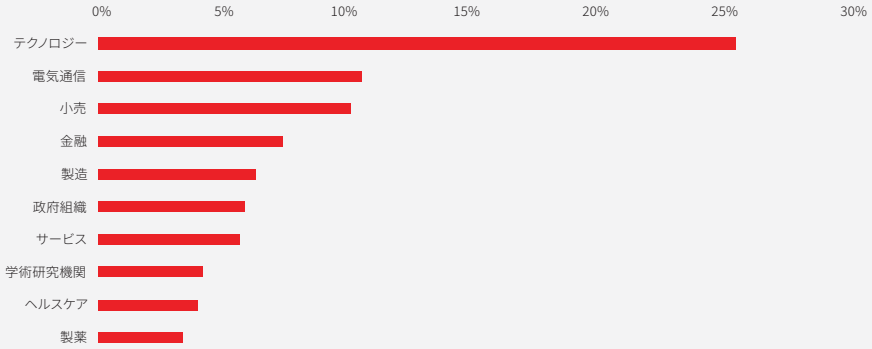
上位の業界

+ テクノロジー業界は世界で最も頻繁に影響を受けた業界であることに加え、3つの地域すべてで最も頻繁に影響を受けた業界でもありました。

+ **APJでは、電気通信業界が全攻撃の10%以上を占めました。電気通信業界に対する攻撃のかなりの割合が、中国由来の（PANDA）脅威アクターによるものと考えられています。**

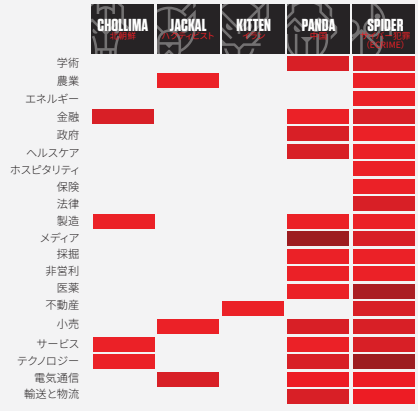
APJ：攻撃頻度別上位10業界

2022年7月～2023年6月



業界および攻撃者別の侵入

APJヒートマップは、この地域内で中国由来の（PANDA）脅威アクターがどれほど多く存在しているかを示しています。これらの脅威アクターは、APJ地域の14業界で観察されましたが、南北アメリカでは6業界、EMEAでは2業界に留まりました。



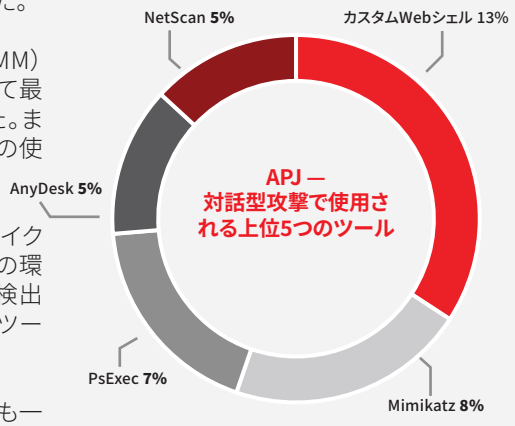
上位のツール

+ **AnyDesk、PsExec、NetScanの3つは、全3地域共通で上位5つのツール**にランクインしました。

+ **AnyDesk**はリモート監視および管理（RMM）ツールで、このレポート期間中に群を抜いて最も一般的に使用されたRMMツールでした。また、同時期には攻撃者によるRMMツールの使用も大幅に増加しました。

+ **PsExec**はリモート実行機能を提供するマイクロソフトのツールで、**NetScan**は、被害者の環境でネットワーク情報を収集するための検出アクティビティで使用できるスキャニングツールです。

+ **APJ**地域では、カスタムのWebシェルが最も一般的に観察されたツールで、全攻撃の**13%**で使用されました。カスタムWebシェルは、中国由来の（PANDA）脅威アクターによって頻繁に利用されていることを受け、APJ地域で高い普及率を示しています。



トップアクター #1 LABYRINTH CHOLLIMA #2 BITWISE SPIDER #3 ETHEREAL PANDA #4 SUNRISE PANDA #5 FRONTLINE JACKAL