DARKTRACE

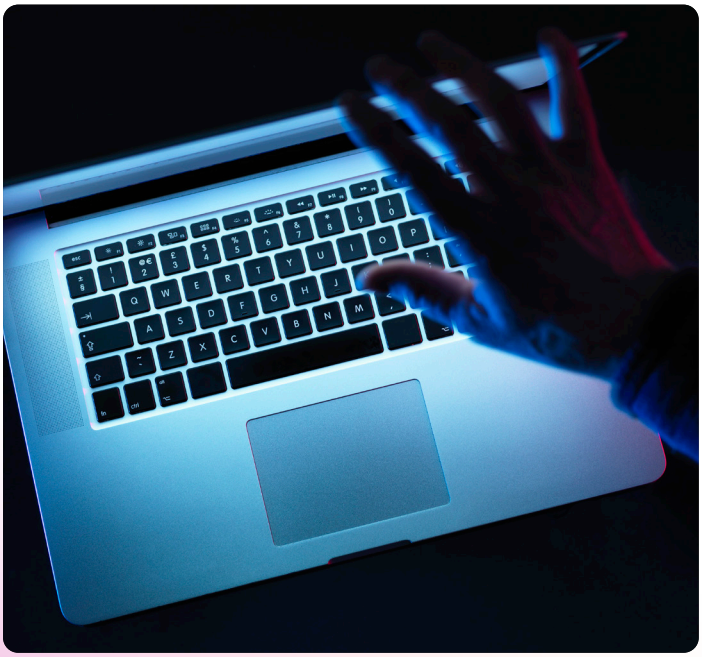
CRIMSON ECHO
中国系サイバー諜報技術を理解する
～ビヘイビア分析を通じて

多くのエグゼクティブにとって、サイバーリスクの議論はインシデント、侵害、稼働停止、そして業務の混乱が中心となります。しかし、ダークトレースが行った中国系サイバーアクティビティに関する調査は、それとは異なる現実を示唆しています。

数十件の中～高確度の侵入事例を含む、3 年間にわたる組織中心型のビヘイビアデータの分析を行った結果、明確なパターンが確認できました。それは、高度なサイバー作戦は、単独のイベントやインシデントとしてではなく、長期にわたる戦略的な配置の一形態として展開されている傾向が高まっていることを示しています。

“Crimson Echo：中国系サイバー諜報活動をビヘイビア分析を通じて理解する” レポートにまとめられた調査結果は、多くの場合サイバーアクセス自体が目的であり、攻撃者は即座に妨害や窃盗を行うためではなく、経済的競争力、サプライチェーン、および重要インフラを支えるシステムに対する永続的な可視性を得るための足場を確立しようとしていることを示しています。

ビジネスリーダーにとってこのことは 1 つの変化を表しています。サイバーリスクはもはやさまざまなインシデントとして理解するべきではなく、構造的な、長期的ビジネスリスクとして、財務リスクやサプライチェーンレジリエンスに対するのと同じ厳格さを持って管理しなければなりません。



調査データが示していること

ダークトレースは 2022 年 7 月から 2025 年 9 月の間に検知された異常なアクティビティを精査しました。ビヘイビア分析、脅威ハンティング、そして構造的なアトリビューション手法を使って、中国系グループが関与したとみられる数十件の中～高確度の侵入事例を特定しました。

調査からの主なデータ：

観測されたケースの 88% は、輸送、通信、重要製造業、医療、テクノロジーなどの戦略的に重要な産業を含む、重要国家インフラと分類される組織で発生していました。

88%

観測されたケースの 22.5% は、米国の組織に関係するものであり、データセット内で最も大きなシェアを占めています。ドイツ、イタリア、スペイン、米国で観測されたケースと合わせると、ケース全体の 55% 以上が主要な西側経済圏の戦略的に重要なセクターで発生していました。

22.5%

侵入の 63% 近くがインターネットに接続されたシステムのエクスプロイトから始まっており、外部に露出したデジタルインフラのリスクが増大していることを浮き彫りにしています。

63%

10 日間

観測された侵害の期間の中央値は約 10 日間であり、多くのインシデントは急速に展開していました。

しかし、いくつかの非常に戦略的な標的ではより長い滞留時間が見られ、少数ながらも重大なインシデントが数か月または数年にわたって持続していました。

調査からの考察

中国系サイバー作戦は 2 つのモデルに従って展開されている

" スマッシュアンドグラブ（SMASH-AND-GRAB）" 型

短期的作戦

観測された事例の大多数は、ステルス性よりもスピードを重視した、迅速な侵入でした。これらの作戦は、重要製造業、通信、輸送および物流、先端材料および産業システムなどの分野で頻繁に見られました。これらの分野は、一帯一路構想のような中国の産業政策や外交政策と密接に関連しています。

これらは、知的財産やサプライチェーン情報の取得を通じて産業の競争優位性を達成するために最適化されているように見えます。これらの場合、スピードと規模が作戦上のアドバンテージをもたらすため、検知されるリスクは許容している可能性があります。

" ローアンドスロー（LOW AND SLOW）" 型

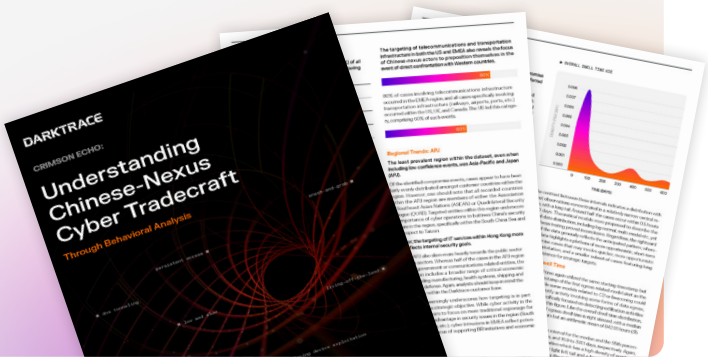
長期的作戦 & 戦略的配置

少数ながら、より影響が重大な一部の侵入事例は、はるかに長い滞在時間を特徴とし、直ちににデータや知的財産を盗むよりも、永続性を優先していました。

攻撃者はアイデンティティシステムや正規の管理ツールを通じて永続的なアクセスを確立し、多くの場合、突発的な偵察や水平移動以外には長期間休眠状態を維持していました。これらの事例の多くは、交通システム、通信ネットワーク、デジタルサービスプロバイダーなどの、重要な国家インフラ環境内で発生していました。

これは、アクセス権が長期間にわたり維持し活用すべき戦略的資産であることを示唆しています。

レポート全文をダウンロード ↗



ビジネスにとって重大な意味を持つ理由

現代の企業は深く相互接続されたデジタルエコシステムで業務を行っています：クラウドプラットフォーム、アイデンティティプロバイダー、物流ネットワーク、そしてサードパーティがほとんどのグローバル企業の運用の基盤を形成しています。

3 つの要点：

01 **サイバー露出**はますます企業の境界を越えて発生しています。デジタルインフラ、クラウドサービス、サプライチェーンは、中核業務システムへの間接的な経路を作り出しています。

02 **永続的アクセス**により戦略的情報が取得される可能性があります。システムの中断やデータ窃盗が発生しなくても、攻撃者が業務、依存関係、産業プロセスに対する可視性を獲得するリスクがあります。

03 **サイバーリスク**はますます競合情報収集に似てきています。内部システムへのアクセスにより、サプライチェーンの構成、製品開発タイムライン、戦略的意思決定などが知られる恐れがあります。

この文脈において、サイバーリスクは**時おり発生する障害ではなく**、長期にわたる競争上および作戦上の諜報活動に似ています。

戦略的コンテキスト

中国関連サイバーアクティビティは、単発的なハッキングキャンペーンというよりも、長期にわたる戦略的な競争状況を反映するようになってきています。

各国がサイバー能力を経済的、技術的、地政学的戦略に統合するなかで、デジタルビジネス環境、とりわけ重要インフラ、サプライチェーン、先端テクノロジーにつながる環境は、重要な戦場となりました。

このことはビジネスリーダーにとって、サイバーリスクは単なるITの問題やインシデント対応の課題ではなく、構造的ビジネスリスクとして扱わなければならないことを意味します。

このような環境においては、デジタルシステムの依存関係、アイデンティティシステム、クラウドインフラに対し、財務上および業務上のリスク管理と同様の厳密なガバナンスを実現できる組織が、最も優位に競争することができるでしょう。

北米：+1 (415) 229 9100　ヨーロッパ： +44 (0) 1223 394 100　日本： (03) 5456 5537　ラテンアメリカ：+55 11 4949 7696

darktrace.com/ja | japan@darktrace.com