デセプションの実例

Zscaler Deceptionで検出した
世界の脅威トップ10

標的型攻撃に対するデセプションベースのアクティブディフェンス

デセプションは、人手による攻撃を検出する最も効果的な戦略の1つです。この戦略は、攻撃者を混乱させてミスを誘導し、検知につなげることを目的としています。

Zscaler Deceptionプラットフォームには、攻撃者が環境内を移動する方法を考慮した戦略が導入されており、世界的な組織に影響を及ぼす深刻な脅威を検出してきました。

本書では、当社の世界的なデコイの網でとらえた上位の攻撃を紹介します。

世界各地で検出された脅威トップ10

1. **北朝鮮からのAPT**
2. **人手によるランサムウェアの戦術 (感染前)**
3. **内部偵察とスキャン**
4. **クレデンシャルスタッフィング**
5. **MikroTikルータの悪用**
6. **分散型総当たり攻撃**
7. **X線装置のコントローラへの侵害**
8. **MedusaLockerランサムウェアの拡散**
10. **ランサムウェアに対する早期の警戒**
11. **シャドーRDP**

ケーススタディ 1

大手国際複合企業への北朝鮮からのAPT攻撃

インシデント

デコイのSMBポートスキャンが検出を実行

- NTLMユーザ名を検知
- コンテキストにより、これが侵害されたユーザであることが判明

トリアージと調査

- 正規のドメインと類似するC2ドメイン
- 当社の調査により、既知の無署名の2つのDLLを隔離
- DLLに含まれていたのは、ハードコードされた資格情報と追加のコマンドを受信するためのローダーコード
- 「Hidden Cobra」グループによる北朝鮮からの標的型攻撃の試みを、チームからオフラインで確認

デセプション戦略

- インフラストラクチャの中で攻撃を受ける可能性が高い重要部分を特定し、これらのセグメントにデコイを配置
- エンドポイントの調査とトリアージを目的としたZscalerの脅威ハンティングによるサポート

成果

- Zscaler Deceptionは、この環境で警告を発した唯一のソリューション

ポイント

環境上の制約と期待する結果に沿ったデセプション戦略は、アクティブディフェンスを成功に導く最も重要な要因の1つです。

小売業者を標的とするランサムウェアオペレータの感染前検出

インシデント

ゼロ号患者により実行されたデコイのサービスアカウント

- 2021年5月8日、システムがサービスプリンシパル名 (SPN) のプロパティ用のActive Directoryデコイをスキャン

ゼロ号患者からSMB上のデコイへの水平移動

- 2021年5月13日、NTLM認証によりSYSTEMアカウントの侵害が判明

WinRMを介したランサムウェアの拡散

- 2021年6月10日、デコイがポート5985上でのポートスキャンを検知

2021年6月13日、WinRMを介してランサムウェアがデプロイ

- タイムリーなレスポンスの欠如により、ランサムウェアがネットワーク上の複数のサーバに感染

デセプション戦略

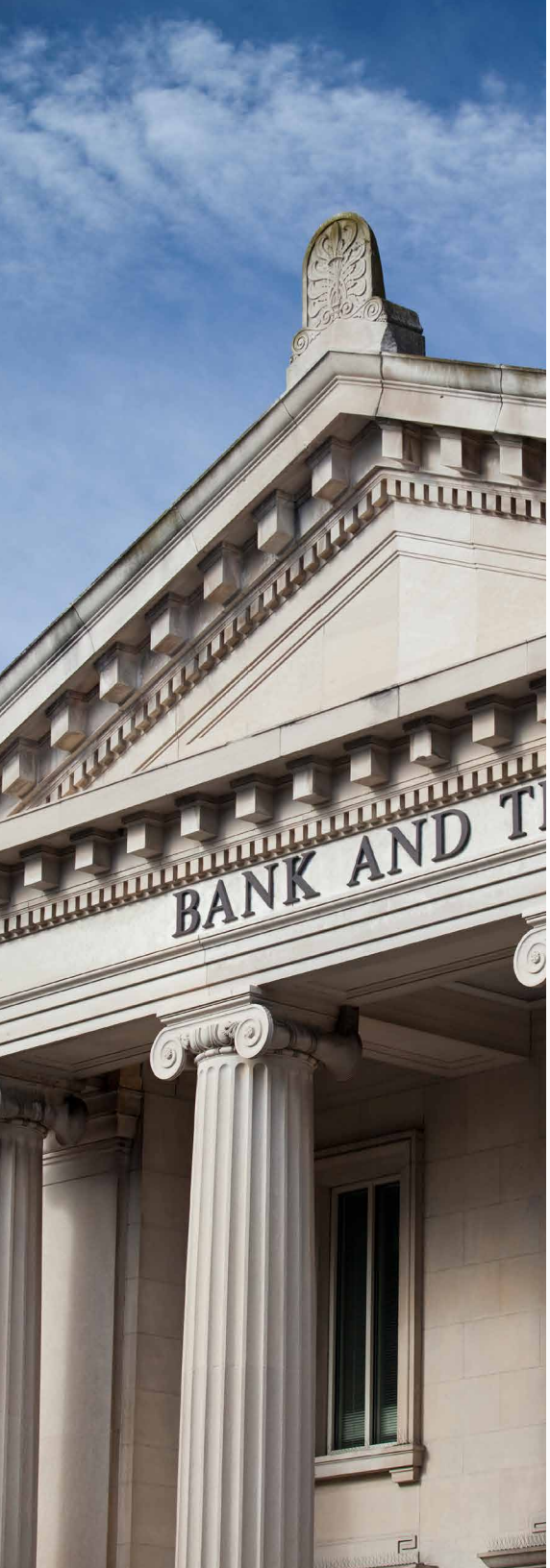
- アカウント侵害を検出するActive Directoryデコイ
- 水平移動を検出するDCおよびDMZ内のネットワークデコイ

成果

- Zscaler Deceptionは、インシデントの1か月前にランサムウェア攻撃が差し迫っていることを警告

ポイント

Active Directoryデコイは、ランサムウェア攻撃における差し迫った感染を警告する最も信頼できる情報源の1つです。セキュリティチームは、これらを優先して調査する必要があります。



大手銀行での内部偵察とスキャン

インシデント

攻撃者は侵害されたルータを介して足場を入手

- SSHを含む複数のポート上のデコイとの広範なやりとりの発信源となったのは侵害されたルータ

攻撃者は3つのSSHデコイで、数百ものコマンドを実行するのに6時間消費

- root/rootでログイン
- 状況認識コマンド
- カスタムネットワークスキャナのバイナリをコンパイルする試み
- /etc/passwd + /etc/shadowからパスワードを窃取
- デコイをピボットとして使用する試み（ブロック済み）
- TCPDumpを使用してネットワークを傍受する試み

デセプション戦略

- 攻撃者の検出だけでなく、その戦略と意図を明らかにするのに十分な期間攻撃者を引き付けておける相互作用の高いネットワークデコイ

成果

- 顧客がルータを確認してアクセスしている間に攻撃者がデコイに時間をとられていたため、攻撃による影響を回避

ポイント

人手による攻撃は、標的相手の防御機能を考慮するため、従来の検出制御を完全に回避します。このケースでは、攻撃者はルータを標的にしました。これは通常EDRがインストールされていないデバイスです。セキュリティチームは、巧妙な攻撃者を検出するためにこのようなデバイスのデコイを設置する必要があります。

知名度の高いクライアントを抱える法律事務所へのクレデンシャルスタッフィング攻撃

インシデント

インターネットに面したCitrixデコイがクレデンシャルスタッフィングの警告を発令

- デコイが200以上の侵害されたドメイン資格情報を受信
- 攻撃元はロシアのクラウドサービスプロバイダのインフラストラクチャ

対応および封じ込め対策の実施

- オーケストレーション機能を使用したファイアウォールでの動的ブロックリスト
- デコイをピボットとして使用する試み（ブロック済み）
- TCPDumpを使用してネットワークを傍受する試み

デセプション戦略

- 資格情報の検証を目的とする攻撃者は、通常、インターネットに面したデコイのアプリケーションを攻撃
- マネージド脅威ハンティングサービス

成果

- Zscaler Deceptionは、キルチェーンの開始と同時に本物の資産への攻撃を遮断

ポイント

ゼロデイや既知の脆弱性を持つリモートアクセスサービスやアプリケーションを模倣したインターネットに面したデコイが、侵入前の攻撃を遮断します。

MikroTikルータを悪用する活動

インシデント

カスタムMikroTik SSHデコイが警告を発令

- 8291/tcp、8728/tcp、22/tcp (SSH) といった既知のMikroTikルータOSポート上のデコイがスキャン
- GOベースのツール (SSH-2.0-Go) を使用してカスタムMikroTikデコイのSSHサービスと交信
- クレデンシャル総当たり攻撃を確認
- 複数の状況認識コマンドを検知
- インターネットから取得して実行するスケジュール化タスクを作成

デセプション戦略

- 環境で積極的に使用される特定のコンポーネントを模倣するカスタマイズデコイ

成果

- 発信源を分離
- ログを使用することなく、資格情報やコマンドなどのテレメトリへ事前にアクセス

ポイント

デセプションは、信頼性が高ければ高いほど有効です。デコイは、攻撃者を引き付けるのに十分な見た目と機能を備えている必要があります。このケースでSSHデコイは、攻撃者を混乱させて、C2サーバを検出することができました。

大手金融機関への総当たり攻撃

インシデント

境界におかれたデコイが複数の総当たり攻撃の試みを検出

- 攻撃は複数の発信源に由来
- 公開されているデフォルトの資格情報の組み合わせを使ったデコイに対する攻撃の試み
- BurpSuiteとNuclei Scannerを使用したタイムスタンプに基づき特定された完全に手動のウェブアプリケーションの悪用

対応および封じ込め対策の実施

- オーケストレーション機能により、資格情報を送信するすべての発信源に対するファイアウォールでの動的ブロックリスト
- 3日後までどの脅威インテリジェンスでも特定されなかった攻撃源

デセプション戦略

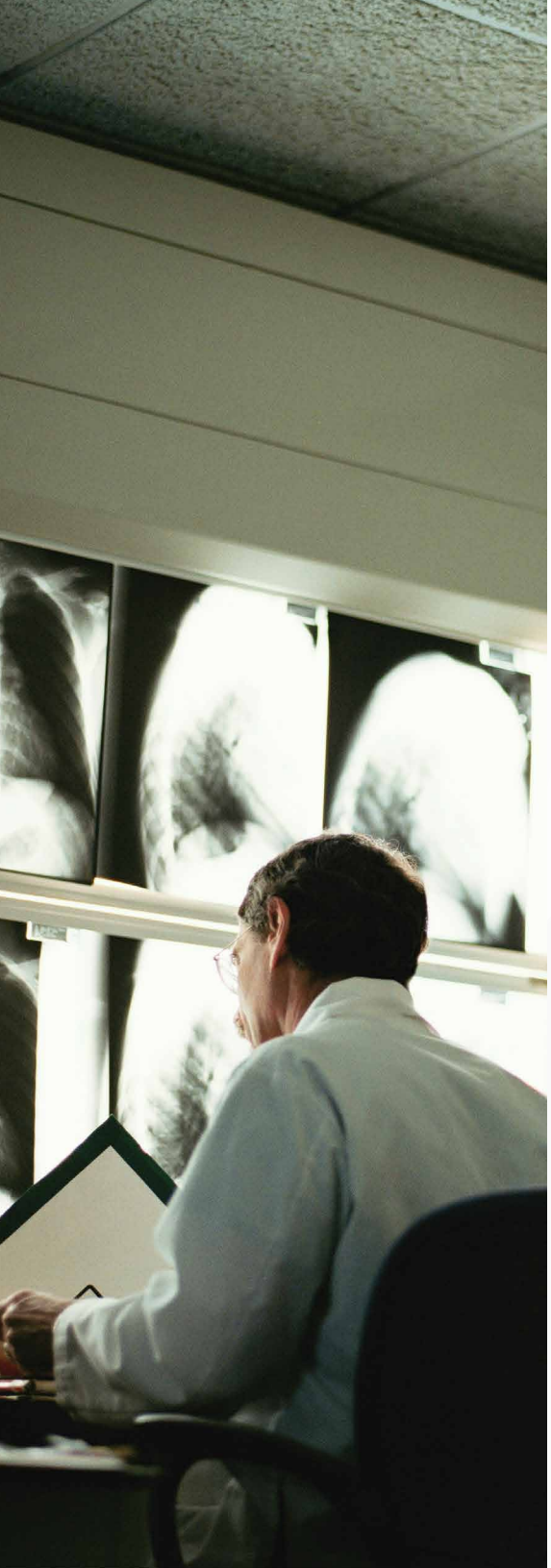
- インターネットに面し、既知の脆弱性やゼロデイを持つリモートアクセスアプリケーションとその他のサービスを模倣するデコイ
- マネージド脅威ハンティングサービス

成果

- 戦術に基づき複数の発信源をブロックする機能を活用することで、影響を抑制

ポイント

Zscalerが提供するインターネットに面したデコイは、従来の脅威インテリジェンスのフィードでは検知できない貴重なプライベート脅威インテリジェンスを生成し、差し迫った攻撃に対し早期に警告を発する信頼できる情報源です。



病院への人手による標的型攻撃

インシデント

通常、APTグループに関連するPsExecに似た動作がデコイに対して行われていることを確認

- X線装置のコントローラが発信源
- デコイ上のDCE/RPC経由でサービスコントロールマネージャにアクセスし、サービスを開始 (PsExecの動作)
- 複数のデコイでの一般的な水平移動ポート (135、445、3389) のポートスキャン
- 一般的なリモートアクセスソフトウェアを検出 (RemCom RemoteAdmin)
- 調査により、Mimikatzのようなツールを確認

デセプション戦略

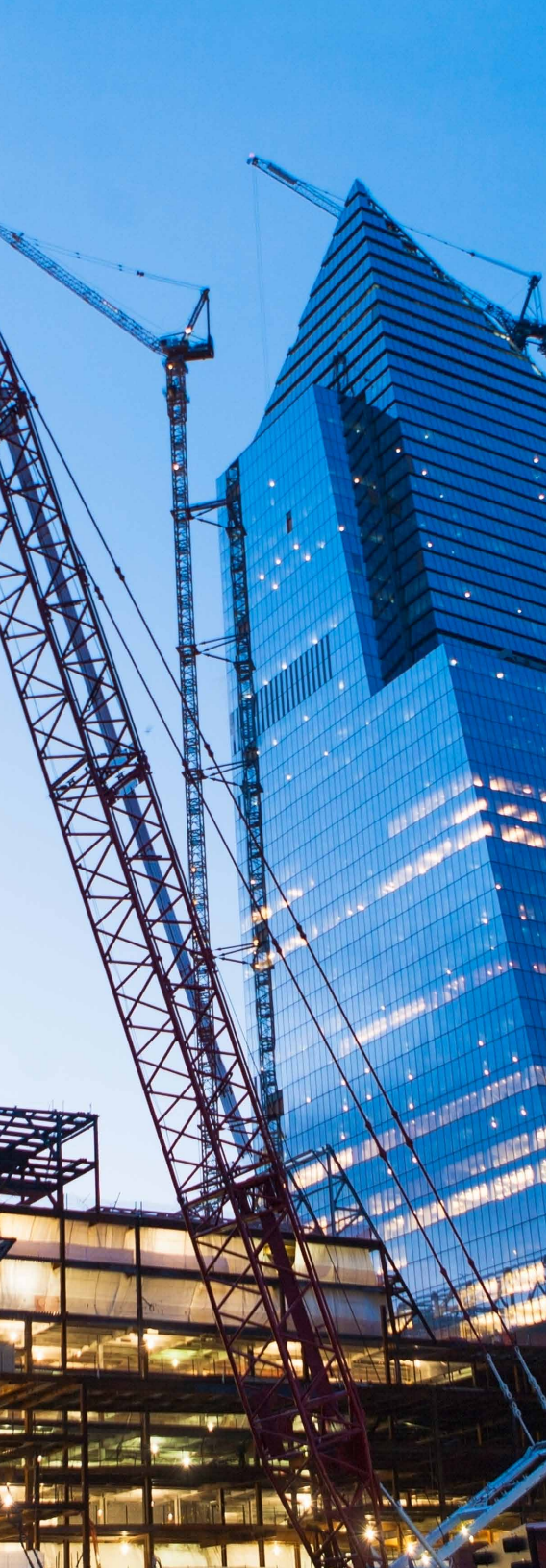
- 病院の重要設備をホストするセグメントへのデコイの戦略的な配置
- デコイに向かっているエンドポイントのルアー

成果

- 標的型攻撃のタイムリーな検出と封じ込め

ポイント

デセプションは、従来の脅威検出コントロールが導入できない病院の設備、IoTデバイス、PoSシステムといった資産に効果的です。



複合企業でのMedusaLocker ランサムウェアの拡散

インシデント

デコイのファイル共有の暗号化時に警告が発令

- 50以上の発信源がデコイのSMB共有にアクセス
- デコイのファイル名が拡張子「.ReadInstructions」に変更
- 検知したユーザ名は特権資格情報

デセプション戦略

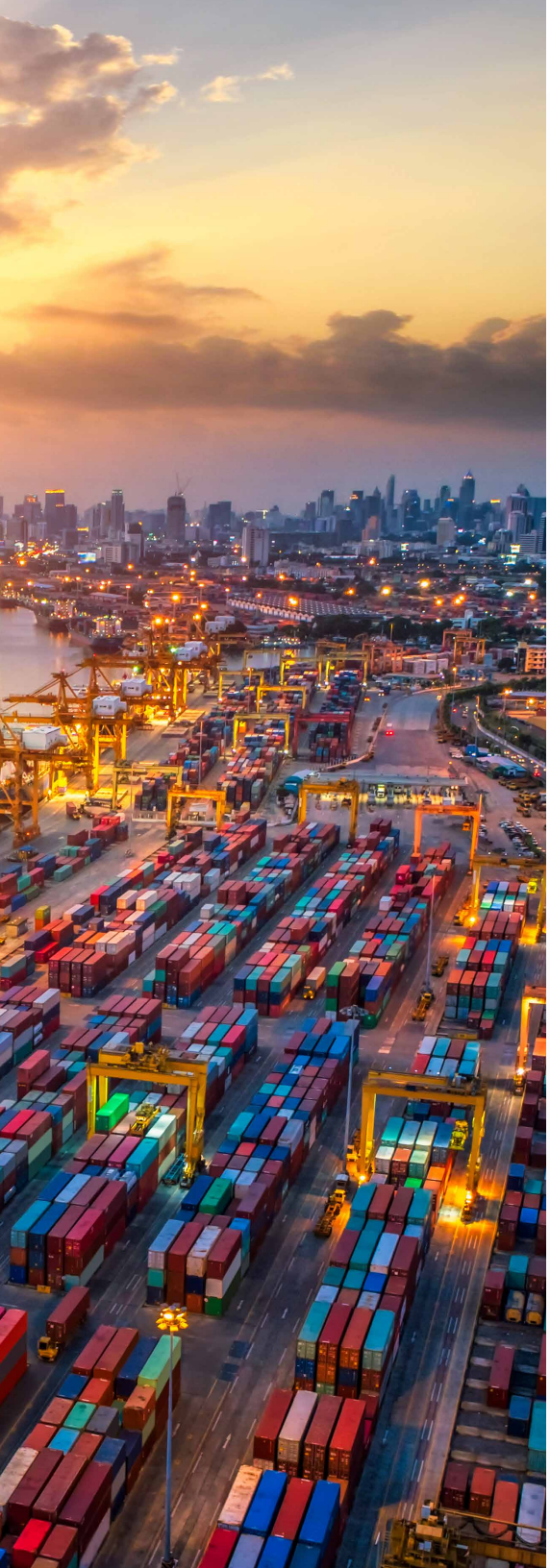
- ランサムウェアのユースケース用に特化した、主要なセグメントでのSMB共有デコイの戦略的デプロイメント

成果

- サーバーセグメントの迅速な分離がランサムウェアの拡散を抑制

ポイント

デコイは、たとえ1つでも十分な効果を期待できます。すべての環境に配備する準備が整っていなくても、限定的かつ戦略的なデプロイメントは、いざという時に大きな力を発揮します。



差し迫った侵害に対する早期の警戒

インシデント

世界的な製造組織でデコイでの特権資格情報の使用に関する警告が発令

- 発信源は複数のデコイの共有にアクセス
- 検知されたNTLMユーザ名が、ThreatParseルールをトリガし、*adm*、*svc*、*bkp*といったキーワードに基づき、特権を持つ可能性のあるアカウントを特定
- アカウントは侵害されたドメイン管理者であることを確認

デセプション戦略

- 多くの制約がある環境へのデセプションデプロイメント。Active Directoryとエンドポイントのルアーで攻撃者をデコイに誘い込む
- 特定のデコイとの交信のための、カスタムルールと電話による警告

成果

- FBIが同社に切迫したランサムウェア攻撃を警告する1週間前に、ダークウェブから収集した情報に基づいて脅威を検出

ポイント

組織は、環境上の特定の制約に対処する必要がある場合があります。広範囲でなければ効果を発揮できない従来の検出コントロールとは異なり、デセプションは非常に狭い範囲でも目標を達成できます。

FMGC企業でのシャドーRDPの検出

インシデント

デコイユーザのログオン失敗を確認

- デコイアカウントでの複数のログオン失敗
- キャプチャしたWindowsログでは、発信源が不明
- 顧客との密な協力によるRCA（認証フローの追跡を含む）
- RDPがインターネットに公開されているAzureシステムを発見

デセプション戦略

- ADデコイユーザの1人が、共通辞書で利用可能な名前を使って作成

成果

- これまでに類のない検出のユースケースが判明
- ビジネスに深刻な影響を及ぼしかねない構成ミスを特定
- この学習を活用して、このユースケースをその他のマネージドサービスのクライアントに拡張し、プロアクティブに3つの同様の発生事例を特定

ポイント

デセプションは、署名やヒューリスティックではなく、攻撃者の意図に基づき攻撃を検出するため、ときには「未知の未知」を効果的に検出します。

ハンティングの世界では、デコイは決して新しいものではありません。しかし、現代のデジタルワールドでは、デコイは違った形をとります。動的、戦略的かつ隠密に攻撃者を罠にはめることは、脅威を軽減するだけでなく、インテリジェンスを獲得する手段でもあります。そして、このインテリジェンスは、Zscalerのセキュリティクラウドに直ちに追加されます。

セキュリティ戦術の1つであるデコイの詳細は、こちらをご覧ください:
https://www.zscaler.jp/products/deception-technology

Zscalerについて

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタルトランスフォーメーションを加速しています。Zscaler Zero Trust Exchangeは、ユーザ、デバイス、アプリケーションをどこからでも安全に接続させることで、何千人ものお客様をサイバー攻撃や情報漏洩から保護しています。世界150拠点以上のデータセンタで稼働するSASEベースのZero Trust Exchangeは、世界最大のインライン型クラウドセキュリティプラットフォームです。詳細は、zscaler.jpをご覧いただくか、Twitterで@zscalerをフォローしてください。