FireEye

FireEye SmartVision

企業ネットワーク内の疑わしい横展開移動を検知

ハイライト

- 従来は検知できなかった疑わしい横展開移動を検知
- ネットワーク内の不審なトラフィックを可視化
- ネットワーク・イベントに対する高度な相関分析および解析エンジン、機械学習テクノロジー、120以上の侵入検知ルールを搭載
- FireEyeネットワーク・セキュリティの一部として多様な導入形態をサポート

めまぐるしく変化する脅威トレンド

脅威トレンドが絶えず進化する中、防御重視のセキュリティ対策は高度なサイバー攻撃への有効性を失い、劣勢を余儀なくされています。サイバー攻撃が力尽くで行われる時代は、もはや過去のものとなりました。今日の高度な攻撃者は、ネットワークに侵入した後、長期間にわたって活動を継続します。水面下で偵察活動を展開しながら、最終的な目的、つまり価値ある情報の窃取というミッションを果たすのです。

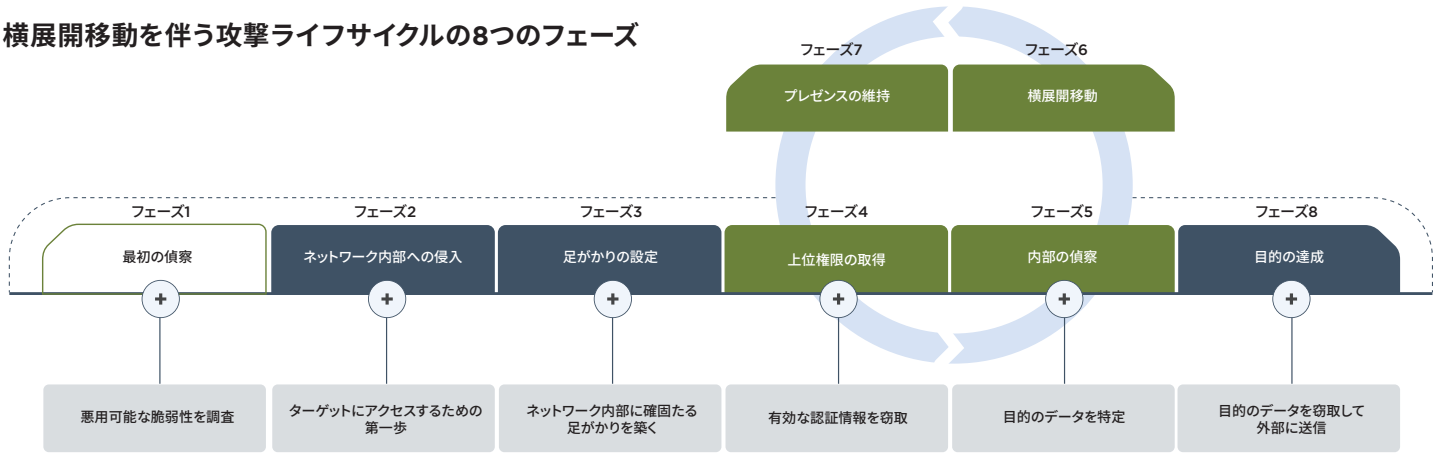
さらに攻撃者は、フォレンジック対策技術に磨きをかけており、横展開（east-west）移動とその電子的な痕跡を巧みに隠ぺいします。このような攻撃者の多くは、侵入先の環境に合わせて構成したカスタム・バックドアをシステムに仕掛け、いつでもネットワークに出入りできる体制を整えています。

侵入後の活動の検知は困難

残念ながら、侵入後の横展開の検知に利用できる既存のツールは、効果が限られているか、まったく無力という状態です。たとえば、セキュリティ情報およびイベント管理（SIEM）システムは、設定が煩雑で管理が複雑なため、横展開移動を見逃しがちです。場合によっては、大量の誤検知を発生させ、セキュリティ・チームの負担増大を招くことさえあります。

また多くの組織では、攻撃者の移動を制限し被害の拡大を防ぐために、複数のファイアウォールを導入しています。しかしファイアウォールは、導入と運用が高コストで複雑であるうえ、疑わしい横展開移動の検知と阻止に失敗するケースも少なくありません。攻撃者はその時点で、一定レベルの信頼性の高い認証情報を入手しており、ファイアウォールを完全にすり抜けることができるからです。

横展開移動を伴う攻撃ライフサイクルの8つのフェーズ



FireEye SmartVision

FireEyeは、ネットワーク内でのデータ窃取活動を示唆する固有のインジケーターとアクションを複数特定しています。このインテリジェンスを元に開発されたのが、従来は見逃していた横展開移動を検知するための新技術、FireEye SmartVision™です。

FireEyeネットワーク・セキュリティ・プラットフォームとSmartVisionを組み合わせて使用すると、ネットワークのコア内やサーバー間のトラフィックに加えて、境界をまたがるトラフィックを詳細に可視化し、さまざまな手口による疑わしい横展開移動を検知できます。

SmartVisionを構成する主なコンポーネント

高度な相関分析および解析エンジン

外部へのデータ送信を検知する機械学習モジュール

些細なセキュリティ侵害の証拠（IOC）も発見する120以上の侵入検知ルール

検知困難な活動を見逃さないSmartVisionの仕組み

SmartVisionは、ネットワークで展開されている多数の不正活動を検知します。横展開移動を伴う攻撃ライフサイクルでは特徴的な動きが見られるため、それに基づいて特定の活動を検知し、アラートを発します。

上位権限の取得

このフェーズでは、次の活動を検知します。

- **Pass the Hash：**ユーザー・パスワードの土台となるNTLMハッシュまたはLanManハッシュを使用して、リモートのサーバーまたはサービスの認証を受けるハッキング手法です。
- **ファイルレス・マルウェア：**「mimikatz」などのファイルレス・マルウェアを検知します。mimikatzは、プレーンテキストのパスワード、ハッシュ、PINコード、Kerberosチケットを抽出する代表的なツールです。

内部の偵察

このフェーズでは、次の活動を検知します。

- **ネットワーク・マッピング：**攻撃者は、SNMPベースの手法や能動的なプローブ、ルート解析などの方法で、エンドポイントやサーバーなどネットワーク上のデバイス、そのオペレーティング・システムや接続状態を把握しようとする場合があります。
- **ホストとサービスのリストアップ：**攻撃者は、各種のツールを使用して、ユーザー名やワークグループ、共有リソース、開いているポート、リモート・ホスト、その他ネットワーク・サービスに関する情報の収集を試みます。
- **ユーザー・ハンティング：**攻撃者は、管理者権限を持つユーザーを特定するため、WinAPIコールを使用するツールで、サーバーやActive Directory、ドメイン・コントローラ、エンドポイント上のユーザー・アカウントについての情報を収集します。

横展開移動

攻撃者は、SMB/SMB2プロトコルを使用して、マルウェアや各種ファイル、パスワード・ダンプ・ツールを転送しようと試みます。SmartVisionは、これらのプロトコル経由のトラフィックを検知します。

外部へのデータ送信

SmartVisionは、外部へのデータ送信を検知する機械学習モジュールを使用して、データ窃取に関連する不自然なファイル転送を検知します。

SmartVisionの導入

SmartVisionはFireEyeネットワーク・セキュリティの一部の機能であるため、さまざまなネットワーク構成や要件に合わせて最適な方法で導入できます。FireEyeネットワーク・セキュリティ・センサーは、サーバー方向のトラフィックを制御する内部ファイアウォールの背後に設置するのが一般的です。このように配置すると、クライアントとサーバー間、またはピア・システム間のトラフィックを検査できます。

SmartVisionは、インライン構成とスパン・タップ構成に対応しており、オンプレミス環境とネットワーク・パケット・ブローカー/TAP環境で利用できます。

まとめ

セキュリティ脅威トレンドが絶えず進化する中、防御重視のセキュリティ対策は高度なサイバー攻撃への有効性を失い、劣勢を余儀なくされています。攻撃者は、検知を免れながら、ネットワーク内をいとも簡単に移動する手口に磨きをかけており、発生した侵害を速やかに検知するための対策がかつてないほど重要になっています。

ネットワーク内の横展開移動を伴うサイバー攻撃は、分析が非常に困難で、従来型のセキュリティ・ソリューションでは対処しきれません。しかし、FireEyeでは、ネットワーク内でのデータ窃取活動を示唆する固有のインジケーターとアクションの特定に成功しています。

このインテリジェンスを元に開発されたのが、従来は検知できなかった攻撃手法、つまり横展開移動を検知するための革新的なテクノロジー、FireEye SmartVisionです。FireEyeネットワーク・セキュリティ・プラットフォームの一部として機能するSmartVisionは、多様なネットワーク・アーキテクチャに対応しています。SmartVisionを導入すれば、攻撃者の横展開移動を可視化して対処し、組織を安全な状態に保つことができます。

FireEye製品の詳細については、次のWebページをご覧ください。
www.FireEye.jp

ファイア・アイ株式会社 | 〒101-0054 東京都千代田区神田錦町3-22 テラススクエア8階 | 03−4577−4401 | Japan@fireeye.com | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com

© 2019 FireEye, Inc. All rights reserved. FireEyeはFireEye,Inc.の商標です。本資料のその他のブランド名、製品またはサービス名はそれぞれその所有者の商標またはサービスマークとして登録されている場合があります。
— SB.FSV.JA-JP-032018