新しいシスコ ネットワークと Stealthwatch による暗号化トラフィック分析

データのプライバシーを損なうことなく、暗号化されたトラフィックの信頼性を向上させます

暗号化トラフィックの急増により脅威状況が変化しています。デジタル ビジネスでは、今や膨大な数のデバイスやアプリケーションがネットワークにアクセスしています。このため複雑化が進み、情報保護のために暗号化することも増えています。2017 年の時点で、インターネットの全トラフィックの約半分が HTTPS で保護されているとされ[1]、ネットワーク上の暗号化トラフィックの量は増加し続ける一方です。

プライバシーを保護しセキュリティを確保できる暗号化は、モバイル、クラウド、Web アプリケーションに欠かせない要件です。一方で攻撃者も暗号化によりマルウェアを隠蔽し、従来のセキュリティ製品による検知を回避しています。つまり、安全性や信頼性を確保するためのプロトコルが、逆にサイバー犯罪を誘発してしまっているのです。データ漏洩は、組織に多大な影響を及ぼすおそれがあります。調査によれば、ネットワークの侵害を検出するための時間は平均で約 200 日、侵害によって発生するコストは平均で約 362 万ドルとなっています。[2]それにもかかわらず、暗号化トラフィックを復号せずに悪意のある活動を検出できる組織はほとんどありません。

2019 年までの予想：

全トラフィックにおける
暗号化の割合

ネットワーク攻撃において
暗号化が使われる割合

出典：Gartner

ソリューションの利点

- **可視性の強化：**ネットワークの分析機能と機械学習を活用することで、暗号化トラフィック内の脅威に関する情報を分析できます。リアルタイム分析により、ユーザとデバイスの情報に相互に関連するコンテキスト上の脅威インテリジェンスが得られます。
- **暗号化アセスメント：**企業が確実に暗号化プロトコルに準拠できるように、ネットワークで送信されるトラフィックの暗号化の有無および暗号化の強度を可視化して把握できるようにします。
- **迅速な対応：**暗号化トラフィックを復号せずにリアルタイムで脅威を検出することで、感染したデバイスやユーザを迅速に封じ込めます。
- **時間とコストの削減：**ネットワークをセキュリティ ポスチャの基盤として使用し、ネットワーク セキュリティに対する投資を十分に活用します。

「暗号化されたネットワーク トラフィックに含まれている脅威を特定することは非常に困難です。また、暗号化トラフィックの脅威やマルウェアを監視することは重要ですが、暗号化の整合性を維持することも必要です」[3]

– Advanced Security Research Group Blake Anderson 氏

ETA の仕組み：

ソリューションの構成要素

- エンタープライズ スイッチ：Cisco® Catalyst® 9000 スイッチング プラットフォーム（Cisco IOS® XE ソフトウェア リリース 16.6.1 以降）
- ブランチ ルータ：Cisco ASR 1000 シリーズ、4000 シリーズ ISR、1000 シリーズ ルータ、クラウド サービス ルータ 1000V、サービス統合型仮想ルータ（Cisco IOS XE ソフトウェア リリース 16.6.2 以降）
- ネットワーク可視性とセキュリティ分析：Cisco Stealthwatch® Enterprise（リリース 6.9.2 以降）

過半数のインシデント対応チームにとって、暗号化されたネットワーク トラフィックの中身や安全性を判断することは大きな負担になっています。従来の脅威検査では、大量のデータを復号してから分析し、その後再度暗号化するため、コストと時間の両面で現実的ではありませんでした。たとえ検査できたとしても、ネットワーク トラフィックを復号するためユーザのプライバシーを確保できません。すべての暗号化形式には対応できないという課題もあります。

暗号化トラフィックの分析

シスコは、ネットワーク インフラストラクチャ分野における専門知識を活用して大規模な調査を実施し、革新的な技術を導入しました。それが暗号化トラフィック分析（ETA）です。新しいタイプのデータ要素やテレメトリを使用することで、暗号化方式を問わず、復号せずにトラフィックを可視化できます。

暗号化トラフィック分析では、主要なデータ要素として、次の 4 つのデータを抽出します。

1. **パケット長とパケット時間のシーケンス（SPLT）：**SPLT はパケット間の着信時間の間隔に加えて、各パケットのアプリケーション ペイロードの長さ（バイト数）を伝えます。
2. **初期データ パケット（IDP）：**IDP は、フローの最初のパケットからパケット データを取得するために使用します。IDP により、HTTP、URL、DNS ホスト名、IP アドレスなどの分析に役立つデータを抽出できます。
3. **バイト分布：**バイト分布は、フロー内のパケットのペイロードに特定のバイト値が現れる可能性を表します。
4. **TLS に固有の特徴：**TLS ハンドシェイクは、分析に利用できる非暗号化メタデータを持つ複数のメッセージで構成されます。メタデータは、暗号化スイート、TLS のバージョン、クライアントの公開鍵のキー長などの抽出に使用します。

これらのデータ要素や拡張テレメトリを使用することで、高度なセキュリティ分析を適用し、暗号化トラフィックから悪意のあるアクティビティを検出できます。また、データを大量に復号する必要がないため、暗号化トラフィックの整合性も維持されます。

暗号化トラフィックに潜むマルウェアの検出

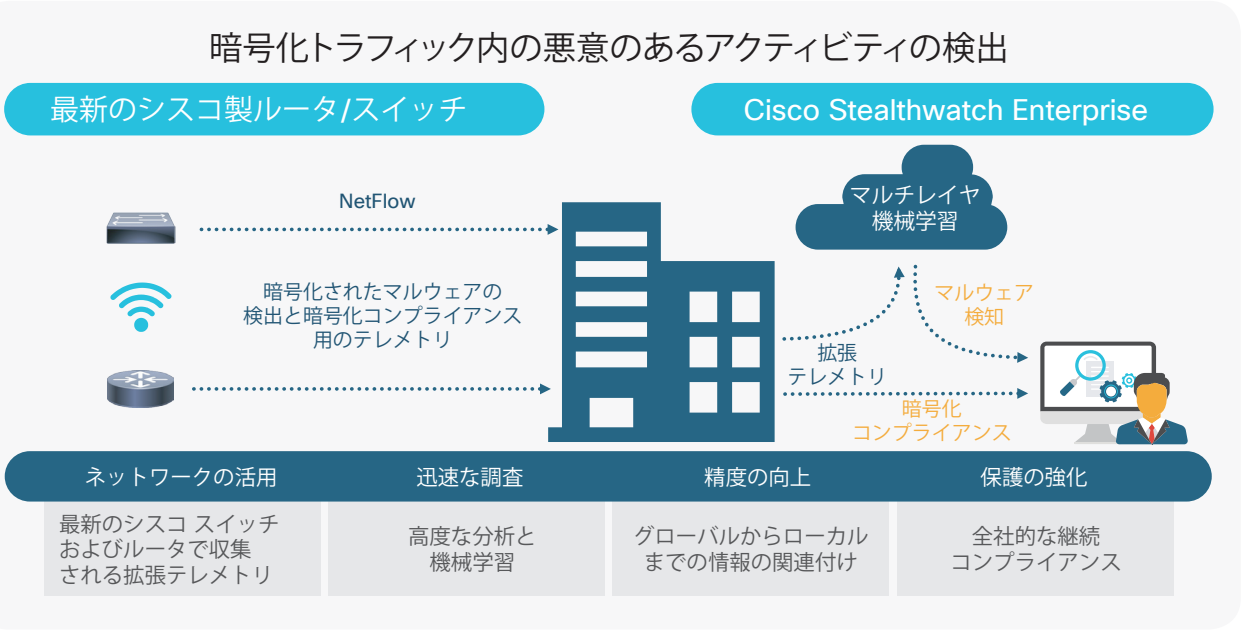
Cisco Stealthwatch Enterprise は、最新のシスコ ルータやスイッチから収集した拡張ネットワーク テレメトリを活用して、包括的なネットワーク可視性とセキュリティ分析を実現します。高度なエンティティ モデリングとマルチレイヤ機械学習機能を備え、ネットワークに接続しているユーザやその振る舞いを常に監視して異常な動作をリアルタイムで検出し、脅威を特定します。さらに、グローバル脅威マップを活用して既知の脅威を特定し、ローカル環境と関連づけることで、暗号化トラフィックにおけるマルウェア検出の精度を大幅に改善します。また、復号しないため、エンドツーエンドでの秘密保持や通信経路の整合性も確保します。これは業界で初めて実現されたことです。

まとめ

ネットワーク チームとセキュリティ チームが連携し、企業全体のトラフィックを可視化する必要があります。シスコの直感的なネットワークを活用すれば、暗号化トラフィックに潜んでいる脅威でさえ検出できます。ネットワーク全体を可視化するシスコのセキュリティ ソリューションの詳細については、https://www.cisco.com/jp/go/eta を参照してください。

出典:

1. 電子フロンティア財団（EFF）、2017 年 2 月、https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web [英語]
2. Ponemon Institute [英語]、2017 年 6 月
3. ブログ『暗号化されたマルウェア トラフィックを復号化せずに検出』、2017 年 6 月



暗号化におけるコンプライアンスの遵守

データ プライバシーとセキュリティのために暗号化する場合、デジタル ビジネスに必要な暗号化の強度や使用範囲を明確に把握しておく必要があります。この 2 点は、暗号化ストリームに侵入するという初期段階から攻撃を防ぐために非常に重要です。これまでは、暗号化トラフィックがポリシーに準拠しているかを確認するには、不正な TLS 通信が発生していないか定期的に検査するしかありませんでしたが、ビジネスで発生するトラフィックの量とデバイスの数を考慮すると、ベストな対策だとは言えません。暗号化トラフィック分析では復号しないため、コストや時間を無駄にすることなく常に監視できます。また Stealthwatch Enterprise では、拡張テレメトリを収集することで、暗号キー交換、暗号化アルゴリズム、キー長、TLS/SSL バージョンなどのパラメータの検索、閲覧が可能となり、暗号化におけるコンプライアンスを遵守できます。

C45-740079-00 05/18