ネットワーク・トラフィック分析：復号化をすべきか否か

著者： Kiran Dhurjaty

はじめに

セキュリティ担当者はよく、「見えないものは守れない」と言います。このような担当者は次のように述べることもあります。

- 暗号化は多くのネットワーク・セキュリティ・ソリューションを破壊する。
- 暗号化は効果より害の方が大きい。
- すべてのトラフィックを復号化することは、安全な組織を維持するための唯一の選択肢である。

これらは真実なのでしょうか。多くのことがそうであるように、その答えは場合によります。それは組織のリスク・プロファイル、プライバシー、コンプライアンス規制、ニーズ、ユースケースによって異なります。

この問題については、すべての場合に当てはまる答えはありません。事前の継続的な運用上および監査上の影響を考慮せずに復号化を必要だとするベンダーには注意が必要です。

本ホワイトペーパーでは、ネットワーク・トラフィック復号化の可能性、長所と短所の概要を説明します。

TLS ハンドシェイクの概要

まず、基本として、TLS ハンドシェイクについて簡単に振り返ってみましょう。最初の 3 ウェイ TCP ハンドシェイクが完了すると、TLS ネゴシエーションが開始されます。

1. クライアントが「Hello」メッセージを送信します。
2. サーバーがクライアントに証明書と公開鍵を送ります。
3. クライアントは、信頼されたルート認証局でサーバー証明書を検証します。
4. クライアントとサーバーは、双方がサポートできる、可能な限り強力な暗号化を選択します。
5. クライアントは、事前マスター鍵をサーバーの公開鍵で暗号化し、サーバーに送り返します。
6. サーバーは、クライアントの通信を秘密鍵で復号化して、事前マスター鍵にアクセスできるようにします。
7. クライアントとサーバーの双方が事前マスター鍵からセッション鍵を計算します。
8. これで、クライアントとサーバーの間で送信されるデータの暗号化と復号化にセッション鍵（対称暗号）が使用されるようになります。

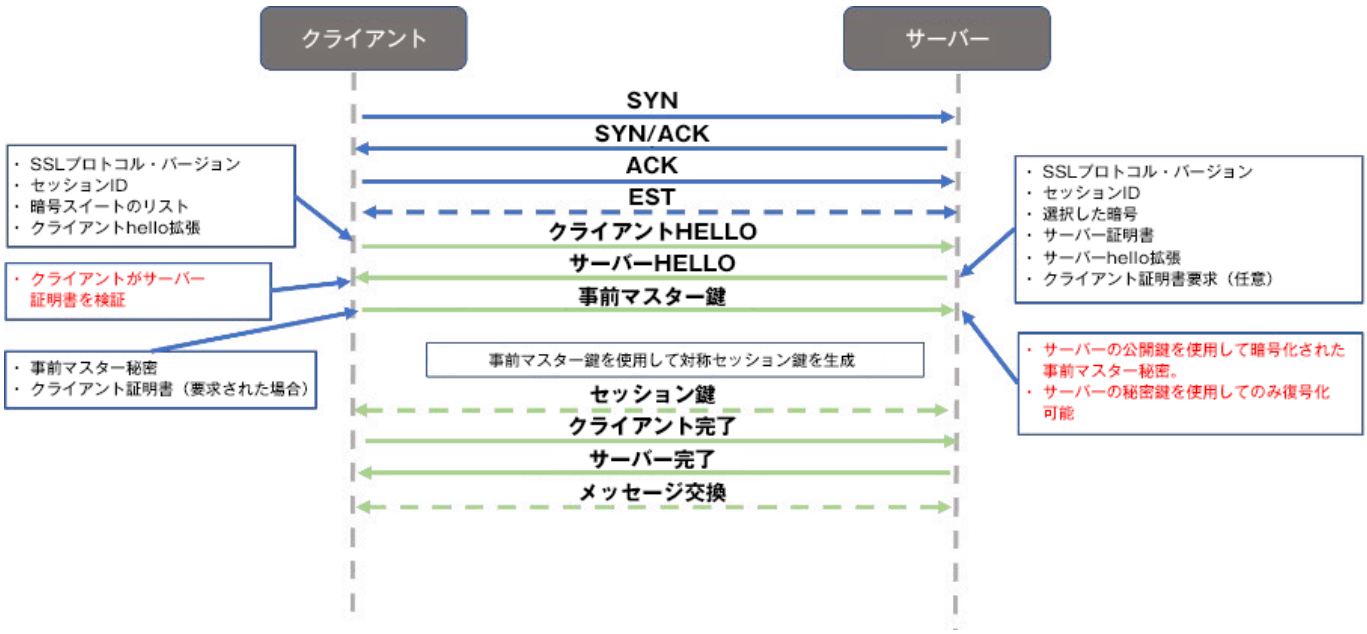

図 1：TLS ハンドシェイク

ここからは、クライアントがサーバー証明書を検証するステップ 3 を中心に説明します。

TLS オフロード

標準的なデータセンターのシナリオについて考えてみましょう。Web サーバーは、自身の公開鍵に基づいて暗号文を復号化するための秘密鍵を保持します。これは、この秘密鍵があれば誰でも事前マスター鍵を復号化してセッション鍵を入手できることを意味します。

そのため、TLS インターセプトの一般的な手法では、データセンター内（通常は Web サーバーの前）にオフロード・エンジンを配置します。このエンジンに秘密鍵を与えてトラフィックを復号化できるようにし、平文のペイロードを Web サーバーやその他のトラフィック検査ツールに送信できるようにします。

このようなオフロード・エンジンは、ワイヤスピードで暗号化と復号化を行うための専用デバイスであり、多くの場合、Web サーバーがこれらの処理を行う負荷を減らすために使用されます。ほとんどの場合、アプリケーション・ロード・バランサーがこの役割を果たします。このシナリオでは、オフロード・アプライアンスはトラフィックとインラインで配置する必要があります。クライアントはオフロード・アプライアンスとの接続を確立しますが、クライアントはそれを認識せずに Web サーバーに割り当てられた有効な証明書を取得します。図 2 に示すように、オフロード・デバイスから Web サーバーへのトラフィックは平文トラフィックであるため、ここでネットワークを TAP してトラフィック分析を実行できます。

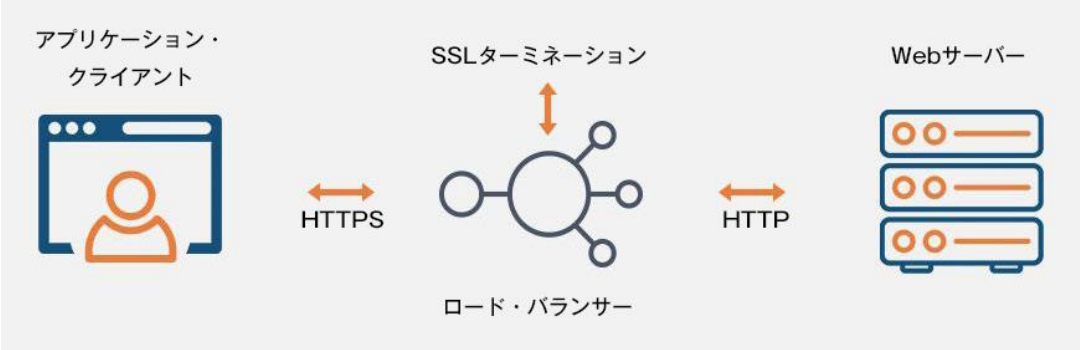

図 2[1]:ロード・バランサーを使用する TLS ターミネーション

考えられるもう 1 つの方法は、オフロード・デバイスをパッシブ・モードで展開することです。このアプローチでは、トラフィックが Web サーバーに到達する前にタップして復号化します。この場合、Web サーバーとパッシブ・デバイスの両方が秘密鍵を持っているため、トラフィックを並行して復号化することができます。この受動的なアプローチは、複数の場所で秘密鍵を共有する必要があり、Web サーバー自体の暗号化と復号化の計算負荷を軽減することにならないため、あまり一般的ではありません。

HTTPS プロキシ・ソリューション

次に、暗号化されたトラフィックをクライアント側からモニタリングする課題について考えてみましょう。TLS ハンドシェイクの後、クライアントとサーバーは安全な伝送のために対称暗号化セッションを使用します。その結果、Web サーバーを管理している組織以外では、誰も Web サーバーの秘密鍵を持っていないため、TLS オフロードを使用できません。したがって、クライアント組織がトラフィックを復号化したい場合は、別のメカニズムが必要になります。

一般的に考えられる解決策は、TLS プロキシ・サーバーを使用することです。これは通常の Web プロキシ・サーバーに似ていますが、TLS トラフィックを検査する機能が追加されています。この場合、クライアント・ブラウザが HTTP(S)ポート 80 と 443 でサーバーにコンタクトしようとすると、まずプロキシ・サーバーにヒットします。すべての TLS 要求に対して、プロキシ・サーバーは自身の証明書でクライアントに応答し、ネゴシエーションを完了します。同時に、クライアントが接続しようとしているサーバーとの新しい接続を確立します。そのため、プロキシは TLS セッションごとに 2 つのセッション鍵を保持します。1 つはクライアントからのトラフィックを復号化するためのセッション鍵、もう 1 つは Web サーバーへのトラフィックを再暗号化するためのセッション鍵です。図 3 を参照してください。

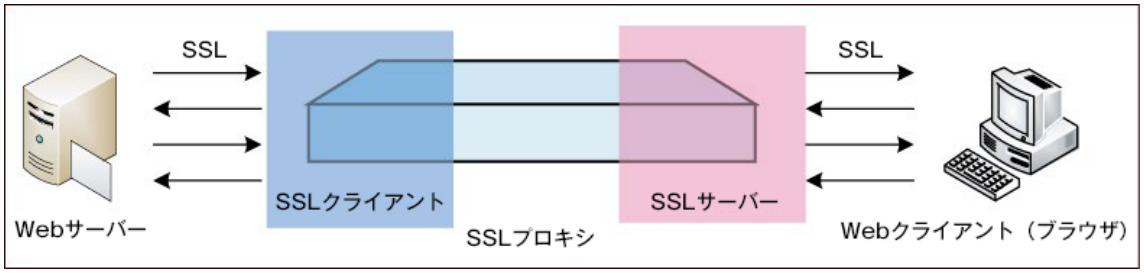

図 3:TLS プロキシ検査[2]

[1] https://www.ssl2buy.com/wiki/ssl-offloading
[2] https://www.hillstonenet.com/support/4.5/en/config_nbctask_sslproxy_intro.html

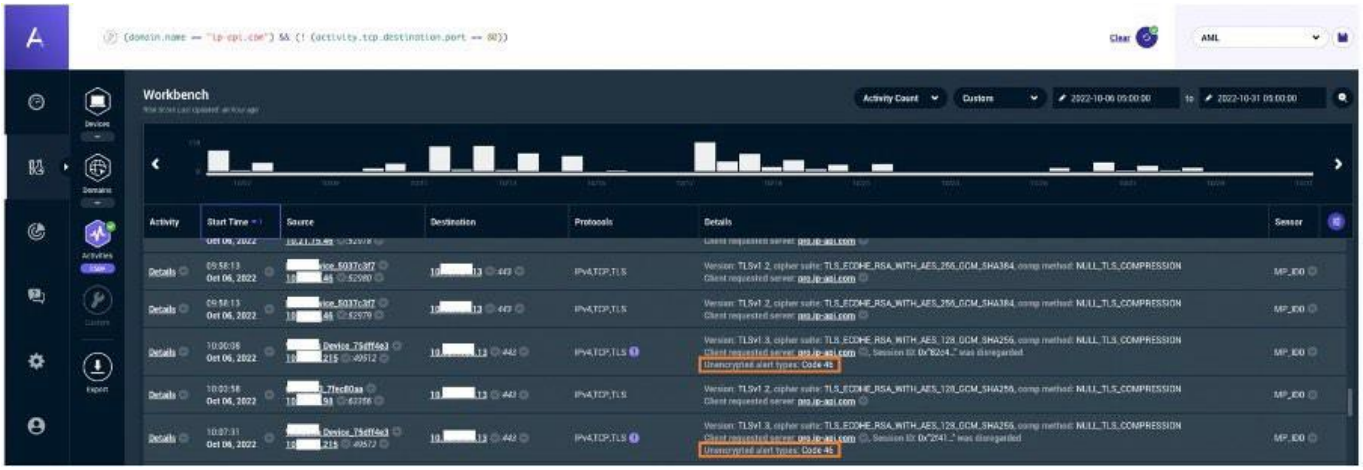

図 4:プロキシ使用時の証明書検証の失敗

多くの場合、この証明書検証の課題を解決するために、組織でローカル CA を作成して信頼される証明書をプロキシに発行し、ローカル CA 証明書をクライアント・エンドポイントの信頼される証明書ストアにインストールします。

SSL 可視化ソリューション

もう 1 つの選択肢は、SSL(または TLS)可視化アプライアンスを使用する方法です。このアプライアンスはすべてのトラフィックを見ることのできるインライン・デバイスです。これは HTTPS プロキシと動作が似ていますが(図 5)、それよりも広範なネットワーク・プロトコルを可視化します。多くの場合、これらのデバイスは、ワイヤスピードで SSL を可視化するための特殊なハードウェア(ASIC)を使用します。

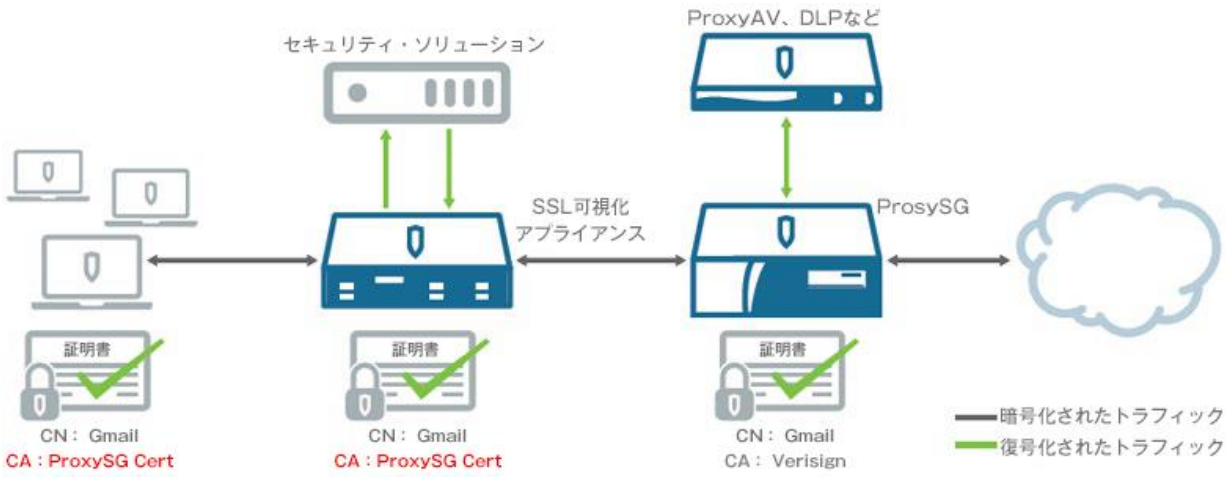

図 5:SSL 可視化アプライアンス[3]

これらのソリューションの多くが、侵入検知システム、データ損失防止ツール、アプリケーション・ファイアウォールなどのツールを使用して、優れた可視化と復号化されたトラフィックを分析する能力をセキュリティ・チームに与えることは明らかです。また、無効な証明書を受け入れるヒューマン・エラーのリスクの解消にもなります。

[3] https://www.edgeblue.com/SV2800.asp

復号化をすべきか否か

TLS とさまざまな復号化の選択肢を踏まえ、次に検討する必要があるのは、ネットワーク・トラフィックを復号化すべきかどうか、そして復号化の利益はコストに見合うかどうかという 2 点です。次の項目を考慮すると、組織の判断に役立ちます。

- 地域的または事業のグローバル展開により、組織に適用される個人情報保護法はあるか？
- トラフィックが復号化される可能性があることを、どのようにユーザーに知らせるのか？自社のポリシーは、任意またはすべてのトラフィックを検査する権利があることを明記しているか？
- アプライアンスやテクノロジーで特定のトラフィックを検査から除外できるか？
- 組織のデータ保護フレームワークは、新しいセキュリティ・リスクを招くことなく、復号化によって発生する平文トラフィックの処理に対応できるか？

これらは、法律や規制に関する考慮事項の一部にすぎません。復号化の選択肢を検討する組織は、技術的課題とビジネス上の課題も考慮する必要があります。まず、復号化ソリューションの総所有コスト（TCO）について考えましょう。先行設備投資においては、検査するトラフィックの量の復号化に必要なインターセプト・デバイスの数とサイズを考える必要があります。あるいは、復号化をセキュリティ・ツールの組み込み機能の 1 つとして考える場合もあります。たとえば、ネットワーク脅威検出・対応（NDR）、侵入検知システム（IDS）、次世代ファイアウォール（NGFW）、Web アプリケーション・ファイアウォール（WAF）などです。

このような設計は、組織のセキュリティ・プログラムを断片的に開発している場合や、リスク、コンプライアンス、情報セキュリティの別個のチームで各ソリューションを実施している場合に特によく見られます。この設計の長所の 1 つは、復号化されたトラフィックが問題のデバイスから離れることがなく、保存する必要もないことです。短所は、鍵がネットワーク上の複数の場所に分散するため、運用上のセキュリティの懸念が生じることです。

さらに、これらのインライン復号化ソリューションのそれぞれでは、複雑さ、遅延、ネットワーク・パスにおける潜在的な障害点が増大します。これはユーザー・エクスペリエンスだけでなく、セキュリティとネットワークの可用性にも影響する可能性があります。すべての復号化ソリューションで一貫したポリシーを維持することは困難です。ソリューションごとに、バイパスなどの機能を実行するための独自のメカニズムがあるからです。たとえば、医療記録やクレジットカード番号など特定のデータ・タイプの復号化を回避することが必要になる場合があります。これに不備があると、HIPAA や PCI-DSS のような規制や標準に関する監査やコンプライアンスのリスクが高まる可能性があります。

コストもサイジングの要因になります。トラフィックの復号化と再暗号化は多大なコンピューティング・リソースを消費します。そのため、トラフィックをサンプリングするのみとするか（部分的な可視化のみを実現）、そうでなければ、これらのアプライアンスのサイズを、モニタリングするトラフィック量にのみ必要なサイズの倍にすることが必要となり、必要なハードウェア・コンポーネントの数が増える可能性があります。多くのベンダーは、広く利用されているインターセプト・ソリューションを単にホワイトラベル化（自社ブランド化）して提供しています。このような要因がすべて積み重なることで、コストが大幅に増大する可能性があります。

前述のような課題があるため、ほとんどのお客様は、TLS 可視化デバイスを 1 台導入し、そこで復号化を一度行い、暗号化されていないトラフィックを必要とする他のすべてのセキュリティ・ソリューションにミラーリングしています。

復号化で完全な可視化は実現するか

残念ながら、この質問の答えは「ノー」です。なぜなら、暗号化にはユニバーサルな標準がないからです。さらに、攻撃者が勧告や標準に従う可能性は明らかに低く、古い暗号や廃止された暗号、TLS/SSL ではなくカスタムの暗号化アルゴリズムなど、あらゆる暗号を使用する可能性があります。

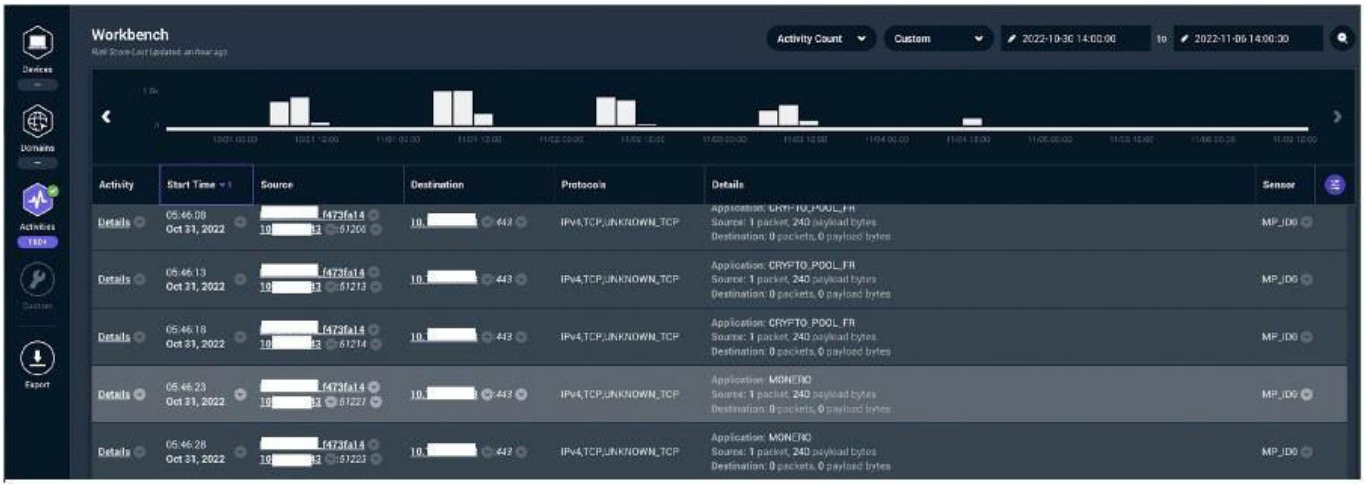

図 6：クリプトマイニング・トラフィック

たとえば、図 6 は侵害されたエンドポイントからクリプトマイニング・プールへの通信を示しています。これはポート 443（HTTPS）を経由していますが、有効な TLS トラフィックではないため、TLS プロキシでプロトコルを識別できず、復号化することもできません。

同様に、ランサムウェア攻撃におけるコマンド・アンド・コントロール（C2）通信を分析した結果、攻撃者は C2 通信に対称鍵暗号と非対称鍵暗号の両方を使用しており、最初の通信にはハードコードされた鍵を使用して、C2 サーバーが侵害されたエンドポイントと安全なチャネルを介してデータ暗号鍵を共有できるようにしていることがわかりました。C2 通信の詳細については、MITRE ATT&CK フレームワーク戦術を参照してください。（https://attack.mitre.org/tactics/TA0011/）

復号化技術では、証明書のピン留めやハードコードされたサーバー証明書のような手法を使用するアプリケーションに対応することも困難です。たとえば、広く使われているメッセージング・アプリケーション WhatsApp は、各チャットにエンドツーエンドの暗号化を提供していますが、証明書を交換しません（図 7）。同様に、デジタル署名された電子メールは、TLS インターセプト・ソリューションでは復号化できません。したがって、TLS を使用していない暗号化されたトラフィックを単純にドロップするポリシーを実装することは困難です。

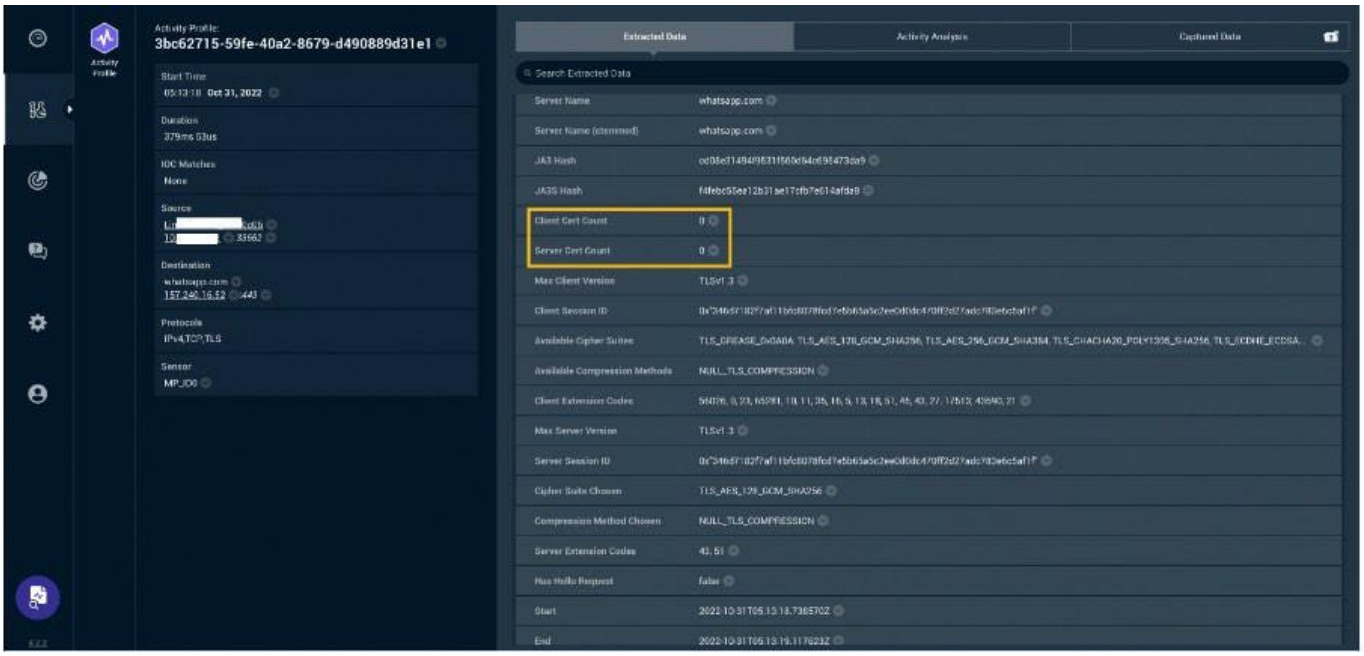

図 7：エンドツーエンドで暗号化され、証明書交換のない WhatsApp トラフィク

TLS インターセプトのその他のリスク

多くの場合、機密データを平文で処理することは、可視化しないことより危険です。たとえば、復号化されたデータがどこかに保存されないとは限らず、復号化されたデータへのアクセスが十分にロックダウンされているとは限りません。通常、NGFW や IDS などのソリューションは機密データを保存しませんが、これらのデバイスが生成するログやアラームはどうでしょうか。SIEM ソリューションはログを分析し相関付けるため、この情報が流出する可能性があります。同様に、NDR ソリューションはローアンドスロー攻撃を検出するように設計されており、そのためにはメタデータとパケットを長期間保存する必要があります。当然ながら、このデータが一度保存されれば、正規のアクセス権を持つ内部関係者になりすますインサイダー攻撃や標的型攻撃を受ける危険が生じます。

Arista NDR の暗号化トラフィック分析アプローチ

アリスタのアプローチは、脅威の状況および攻撃者の戦術と技術に重点を置いています。たとえば、MITRE ATT&CK フレームワーク TTP のリストでデータソース「Network Traffic」[4] の項を確認すると、復号化が有益となる可能性のある TTP の割合は、リスト全体のごく一部であることがわかります。そのため、アリスタは、復号化がポリシーに及ぼす影響も考慮し、お客様にネットワーク・トラフィックの復号化を強制しない戦略を考案しました。

Arista NDR は、データ・サイエンスに基づく暗号化トラフィック分析（ETA）を復号化なしで行い、プライバシーとポリシーの制約の範囲内で、セキュリティ・チームに有益な情報を提供します。このプラットフォームでは、この目的のためにさまざまなデータ・サイエンス技術を使用します。たとえば、C2 である可能性のある異常な特性を持つ TLS セッションを特定するために、教師なし機械学習（ML）を使用し、攻撃者の TTP に関連するアクティビティのパターンを特定するために、教師あり ML を使用します。これにより、リモート・アクセス・ツール、リバース・シェル、不正なコマンド・アンド・コントロール、データ流出に使われるドメインなどを特定することが可能です。また、ディープ・ニューラル・ネットワークとデシジョン・ツリーを使用して、暗号化されたセッションをトラフィックの性質（リモート・シェル・アクティビティ、Web ブラウジング、ビデオ会議、ファイル転送など）に基づいて分類します。図 8 を参照してください。

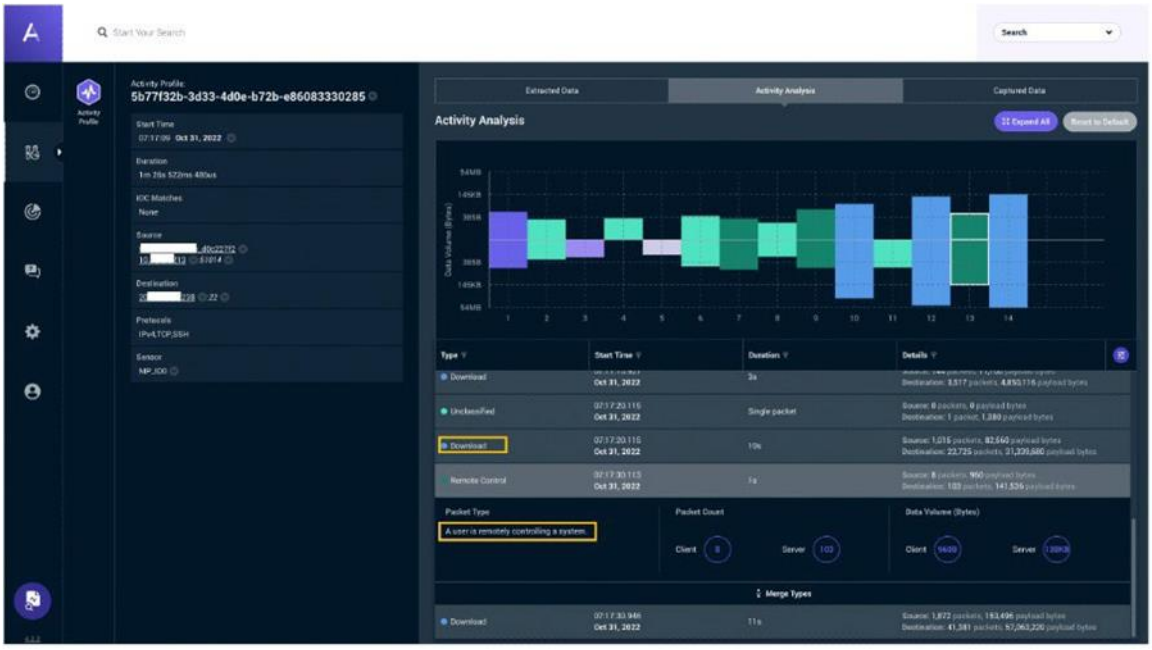

図 8：SSH アクティビティ分析

[4] https://attack.mitre.org/versions/v12/datasources/DS0029/

暗号化されたトラフィックを分析するためのこれらの手法と併せて、送信元アプリケーションやデバイスの性質、宛先ドメイン、IP アドレス、自律システム・ネットワーク、およびその他のネットワーク・パラメーターなどの他のコンテキストもアナリストにとって非常に関連性が高く、役に立ちます。たとえば、暗号化されたファイルが電子メールや Zoom 会議セッションを介して社内ユーザー間で転送されるのは問題ないかもしれません。一方、そのファイルが社内ファイル共有アプリケーションを使わずに PowerShell スクリプトや IoT デバイスから Dropbox アカウントに転送されるとしたら、注意が必要です。

他のセキュリティ製品では、トラフィックを復号化せずに脅威を特定するために、JA3、JA3S、JARM ハッシュなどの技術と、侵害の指標や他の形態の脅威インテリジェンスを組み合わせて使用しています。このような検出技術だけでは、ノイズが多く発生する可能性があります。ただし、Arista NDR のさらに綿密な ETA エンジンを組み合わせると、復号化の負担を必要としない利点と併せ、目覚ましい成果を挙げることができました。実際、一部の検出は、暗号化プロセスとプロトコル情報を分析することで初めて可能になると考えられます。たとえば、無効な TLS 証明書や無料の認証プロバイダが発行した証明書は、攻撃者がよく使う特徴的な戦術であるため、Arista NDR はこのような証明書の使用を分析します。

まとめ

結論として、組織はネットワーク・トラフィックの復号化を決定する前に注意が必要です。コスト、プライバシー、継続的な運用上の課題、監査、内部脅威など、さまざまなトレードオフを考慮する必要があります。ほとんどの組織では、リスク・プロファイルを評価すると、復号化が最善のアプローチではないことがわかります。それよりも暗号化トラフィック分析のような技術を利用する方が、少ないコストと労力で大きな利益を得ることができ、復号化がもたらすリスクと困難を回避できます。

アリスタネットワークスジャパン合同会社

〒100-0004　東京都千代田区大手町 1-7-2　東京サンケイビル　27F
Tel:03-3242-6401

西日本営業本部
〒530-0001　大阪市北区梅田 2-2　ヒルトンプラザウエストオフィスタワー　19F
Tel: 06-6133-5681

お問い合わせ先

Japan-sales@arista.com

www.arista.com/jp

2023 年 8 月 24 日　02-0110-01