ケース スタディ

シスコのソリューションで攻撃前、攻撃中、攻撃後のセキュリティ対策を実現

Cisco Cloud Web Security Premium が国際的石油ガス企業のランサムウェア駆除に貢献。

課題

企業データの盗難や侵害を狙う攻撃が増えている現代では、コンテンツのセキュリティを守ることがこれまで以上に難しくなっています。シスコ年次セキュリティ レポート（2014 年）によると、調査対象となったすべてのビジネス ネットワークで、マルウェアをホストしている Web サイトへのトラフィックが確認されました。[1] また、このアクティビティを監視した結果、こうしたネットワークは侵入を受けるとしばらくの間は危険にさらされる可能性が高いこと、そして中枢部への侵入は検出されない可能性が高いことがわかりました。[2]

脅威の検出と予防が特に困難になっている背景には、次のような要因があります。

- **モバイルとクラウド**：適切なセキュリティ対策が行われていないモバイルやクラウドは、可視性を低下させ、セキュリティを複雑にします。クラウド コンピューティング、仮想化、モバイル勤務やリモート勤務、個人所有デバイスの持ち込み（BYOD）といったトレンドを採用する企業が増えるにつれて、企業のコントロールが及ばないデータの存在が問題になってきています。ネットワークは脆弱になり、攻撃されやすくなります。また、ビジネスクリティカルなサービスがクラウドに移行し、企業のセキュリティ境界の外側でアクセスされるケースが増えているため、攻撃対象領域（Attack Surface）は広がる一方です。
- **高度な攻撃者**：*シスコ年次セキュリティ レポート（2014 年）*によれば、高度な攻撃者は「どのようなセキュリティ ソリューションが導入されているかを事前の準備で突き止めており、より見えにくく、より検出しにくい行動パターンをとることで脅威を巧妙に隠蔽」しています。[3]この戦略のため、セキュリティ ソリューションや専門家が簡単に検出できるような脅威は減少しており、組織は「悪意のある人物が実際のトラフィックと区別がつかない指揮統制（C&C）チャネルを構築するために行うトラフィックの暗号化や、スクランブル化、ランダム化」に直面することになります。[4]

お客様のプロファイル

業種：石油・ガス
従業員数：～15,000 名
事業範囲：グローバル
セキュリティ担当者：12 名
その他のセキュリティ対策：ウイルス対策、ファイアウォール、侵入検知システム（IDS）、セキュリティ情報/イベント管理（SIEM）

課題

- 従来のセキュリティ ソリューションをすり抜けて Web ベースのトラフィックから企業ネットワークに入り込む高度な脅威の検出
- 対応すべき脅威の優先順位付けに役立つ実用的インテリジェンスの生成
- 分散環境への導入、既存のセキュリティ インフラとの統合、攻撃コンティニューム全体にわたるセキュリティの実現という要件をすべて満たす単一ソリューションの特定

ソリューション

- Cisco CWS Premium（Cisco CWS Essentials の全機能を含む上位ソリューション）
- Cognitive Threat Analytics（CTA）と Advanced Malware Protection（AMP）で Web トラフィック内のリスクの高い脅威を自動検索し、社内ネットワークで活動している高度な攻撃を可視化

導入効果

- 以前には発見できなかった継続的なマルウェア感染の問題を解決
- 攻撃コンティニューム全体にわたる脅威対策を実現
- セキュリティ チームが重大度の高い脅威に重点的に取り組める環境に

[1] *シスコ 年次セキュリティ レポート（2014 年）*：http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[2] 同上。
[3] 同上。
[4] 同上。

脅威をとりまく情勢は複雑かつ継続的に進化しており、コンテンツ セキュリティの最新アプローチでは、防御よりも検出に重きが置かれるようになっています。現在の企業は、ネットワーク内にすでにある脅威を視覚化するコンテンツ インスペクション、動作異常検出、高度な診断といった機能に注目する必要があります。つまり、「攻撃後」のフェーズが重要になります。

図 1. 新しいセキュリティモデル：攻撃後の継続的なセキュリティ

Cisco® Cloud Web Security（CWS）Premium は、企業の拡張ネットワークで継続的にセキュリティを維持するために役立ちます。Cisco Web セキュリティのクラウド版である Cisco CWS プラットフォームは、Web セキュリティの範囲をモバイル デバイスや分散環境にも広げます。シスコの世界的な脅威インテリジェンスと、高度な脅威防御機能、ローミング ユーザ保護を通じて、ユーザを安全に保護します。Cisco CWS Premium には、Cisco CWS Essentials の全機能と、Web トラフィック内のリスクの高い脅威を自動検索する 2 つの革新的なマルウェア検知システムが含まれています。

- **Cognitive Threat Analytics（CTA）**は、機械学習と高度な統計を使用してネットワーク上の異常なアクティビティ、つまりセキュリティ侵害の指標（IOC）を見つけるほぼリアルタイムのネットワーク動作分析システムです。CTA は異常を見つけ、問題の可能性をセキュリティ アナリストに知らせることで、セキュリティ アナリストの負担を減らし、対応すべき脅威の優先順位を付けることに貢献します。
- **Advanced Malware Protection（AMP）**は、ファイル レピュテーション、ファイル サンドボックス、レトロスペクティブ ファイル分析を併用することで、攻撃コンティニューム全体にわたって脅威を特定、阻止します。

CWS Premium は、これらのソリューションの組み合わせによって、セキュリティ業界が以前は検出できなかった新しい指揮統制（C&C）チャネルを特定します。

このケース スタディでは、ある国際的な石油ガス企業が以下を達成するうえで、CWS Premium がどのような役割を果たしたかを検証します。

- 増え続ける大量の Web トラフィック（1 日あたり 3,500 万以上の HTTP/HTTPs 要求）の可視性の向上
- 脅威対処チームが対応すべき脅威の優先順位を判断するために役立つ実用的な脅威インテリジェンスの生成
- 既存のセキュリティ インフラに統合され、攻撃コンティニュームの全体（攻撃前、攻撃中、攻撃後）にわたって保護を提供する単一ソリューションの導入

ソリューション

シスコは、ネットワークの可視性を向上させて、脅威対策チームが対応すべき脅威の優先順位を判断しやすくするために、CTA と AMP を含む CWS Premium へのアップグレードを提案しました。

AMP のレトロスペクティブ分析により、境界防御を通過したときには「クリーン」と思われたファイルが、実際には巧妙に偽装された高度なマルウェアであることが判明する場合があります。その場合、AMP はただちにセキュリティ管理者に警告し、感染した可能性のあるネットワーク ユーザと感染の時期を特定します。

一方の CTA は、防御をすり抜けて社内ネットワークで活動しているステルス性の高い脅威を検出するために役立ちます。これは、セキュリティが侵害されているデバイスを動作分析と異常検出によって特定する革新的なマルウェア検知システムです。CTA は高度な統計モデルと機械学習を使用して新しい脅威を個別に識別します。収集したデータから学習し、時間経過とともに適応を深めていくため、調整や設定を行う必要はありません。

この石油ガス企業の事例では、CTA によってネットワーク上のマルウェアの活動の証拠が特定され、報告されました。このマルウェアは、いくつかのモジュールの集合体という形をとっており、これらのモジュールが 1 つのマルウェア エンティティによって制御されていました。このマルウェアのペイロードは Cryptolocker ランサムウェアでした。これは、身代金を支払うまで攻撃対象のコンピュータのファイルを暗号化してデバイスを「ロック」するタイプのマルウェアです。[5]

図 2 に示すように、この攻撃者は攻撃を実行するために指揮統制インフラを操作しました。この攻撃は主に 4 段階で行われました。

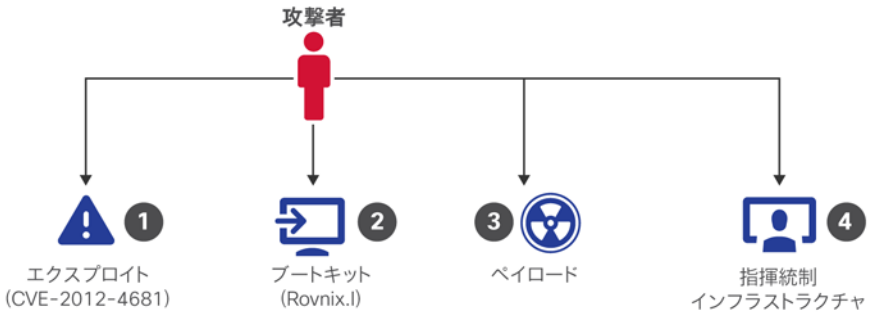
ステップ 1. 攻撃者は、Oracle Java SE 7 Update 6 の Java Runtime Environment（JRE）コンポーネントの脆弱性を悪用するために、エクスプロイト（CVE-2012-4681）を利用しました。これによって攻撃者は、セキュリティ マネージャをバイパスしてリモートでコードを実行できます。

ステップ 2. 次に、マシン上での永続性を保証するためにブートキット（Rovnix.I）がインストールされました。

ステップ 3. マルウェアを完全に機能させるために、ペイロードが提供されました （この場合のペイロードは Cryptolocker ランサムウェア）。

ステップ 4. 攻撃によって指揮統制チャネルが確立され、活動がアクティブになりました。

図 2. 攻撃の主な 4 段階

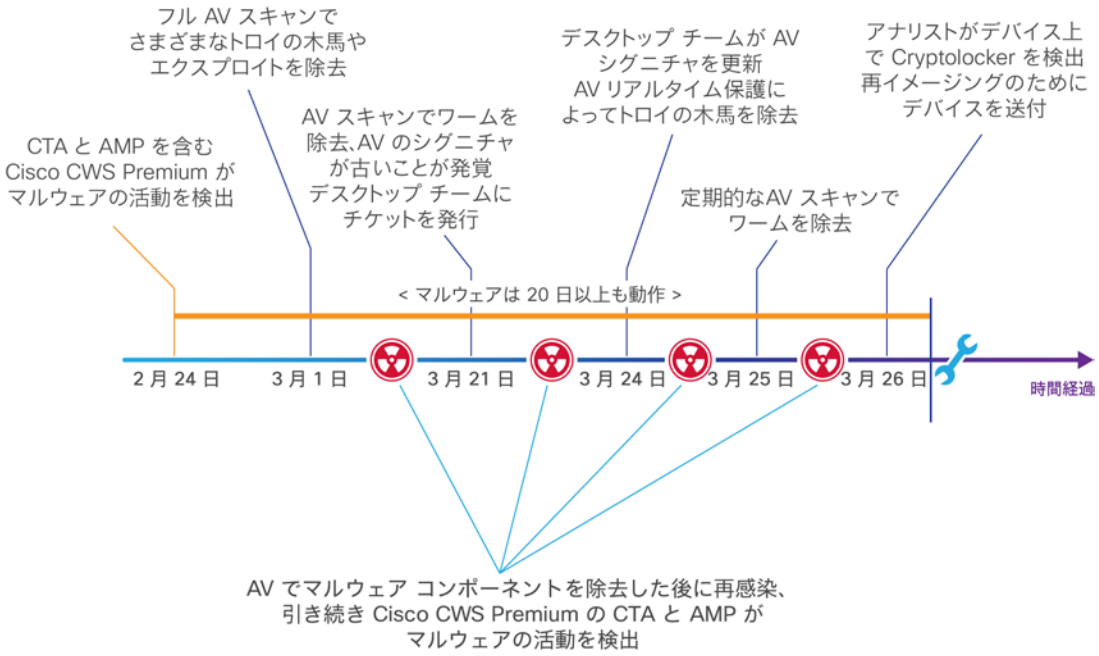


[5] Cryptolocker の分散にはマルバタイジング（マルウェアの拡散に使用されるオンライン広告）が重要な役割を果たしました。Cryptolocker はすでに無効化されていますが、マルバタイジングとランサムウェアは、今もなお攻撃者が Web を通じてターゲットを絞ったキャンペーンを展開する際によく利用される手法です。 詳細については、2014 年次シスコ中間セキュリティ レポート（http://www.cisco.com/web/offer/grs/190720/SecurityReport_Cisco_v4.pdf）[英語] を参照してください。

当初、この石油ガス企業のセキュリティ チームはアンチウイルス（AV）ツールで脅威を解決しようと試みました。しかし、これはルートキットの感染だったため、マルウェアは感染したシステムの奥深くまで入り込んでいました。AV ソリューションにより除去できるのは、一部のマルウェアのコンポーネントのみです。感染が完全に解消されるまで、CTA は悪意のあるアクティビティの存在を警告し続けました。

図 3 は、このマルウェアの活動を検出してから脅威が解決されるまでの全体的なタイムラインです。

図 3. マルウェアの活動タイムライン：検出から解決まで



同社が経験した状況は、「攻撃後」フェーズにおける CWS Premium の価値をよく表しています。また、この例からわかるように、AV 製品で高度な攻撃に対抗するのは困難です。CTA システムは指揮統制チャネルが活動している証拠を明らかにし、 データの抜き出しに使用されていた他のいくつかのドメインも特定しました。このような感染は、企業のインフラに長期にわたって潜伏していたセキュリティ侵害を示しています。

結果

今日のセキュリティ チームは日々大量のインシデントの対応に追われており、「干し草の中で針を探す」ような探索をする時間はありません。セキュリティ チームが高度な攻撃に重点的に取り組めるようにするためのサポートが必要であり、そのような攻撃を検出、分類する仕組みが CTA システムです。

この Cryptolocker ランサムウェアの感染事例では、CWS Premium がマルウェアの活動を検出し、既存のセキュリティ インテリジェンスを適用して、感染デバイスに由来するいくつかの指揮系統チャネルをブロックしました。しかし攻撃者は、レピュテーションが不明な別の IP アドレスを使用してきました。この新しいチャネルは、感染期間全体を通して有効でした。この事例は、シグニチャベースや Web レピュテーションベースの検出システムの長所と短所を示しています。自動ブロックができることは長所ですが、新しいチャネルはブロックされないという短所があるため、このシステムのみに頼ることは危険です。攻撃後においても継続的な保護が必要なのはこのためです。

以下に、CWS Premium の CTA システムによって特定された指揮統制チャネルの分析と、サンプルの Web トラフィック要求と統計を示します。

表 1. 攻撃インフラ

段階	リモート サーバ	対象 IP アドレス	対象国	要求数	アクティビティ ステータス
1	C&C サーバ #1	109.XXX.XXX.XXX	オランダ	17 回（試行）	Web レピュテーションによるブロック
2	**C&C サーバ #2**	**94.XXX.XXX.XXX**	**ルクセンブルク**	**75**	**アクティブ チャネル**
3	C&C サーバ #3	fistristy.com	ルクセンブルク	175 回（試行）	Web レピュテーションによるブロック
4	C&C サーバ #4	ffeed5.com	ロシア	7 回（試行）	Web レピュテーションによるブロック

表 2. CTA で識別されてデバイスから削除された脅威

脅威の名前	削除
Cridex Worm	3 月 19 日
Cridex.E worm	3 月 19 日
Tesch.B trojan	3 月 19 日
Java Exploit/CVE-2012-4681	3 月 19 日
Trojan downloader Win32/Upatre	3 月 19 日
Cridex worm	3 月 21 日
Trojan Win32/Viknok.C	3 月 24 日
Cridex worm	3 月 24 日
Crypto Defense	3 月 26 日

C&C サーバ # 1（109.XXX.XXX.XXX）への通信

通信の特性：

- このサーバに対して試行された要求の総数は 17 でした。すべて C&C 通信で、レピュテーションによりブロックされました。
- URL ストリングを通信チャネル（C&C）として使用しようとしたところを CTA が検出しました。URL（次の「HTTP 要求の例」を参照）は、エンコード済みメッセージです。この攻撃で使用された複数の URL で、同じ構造の URL ストリング（IP アドレス /m/IbQ.*）が共有されていました。この通信がレピュテーション システムによってブロックされたことも、状況的な証拠になります。
- 攻撃者は、マルウェアが確実に動作を続けられるように、まだレピュテーション フィードの一部に含まれていない第二の C&C チャネルをサーバ上にセットアップしました。URL 自体は、エンコード済みメッセージです。

HTTP 要求の例（一部のみ抜粋し匿名化）

http://109.XXX.XX.XXX/m/IbQXXXVjjpcE6+54HXXXdmmGcNZxtMZdvqyB5EkJAUmL/1sOXXXvq5zzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXX.g+fq4XXXOTYke6uhGHDOEeqje76v7z7i+wgqXXXFBuMz5k08yocxOH63bwQ9JMfwy8uNRM…

C&C サーバ # 2（94.XXX.XXX.XXX）への通信

通信の特性：

- サーバに試行された要求の総数は 75 でした。すべて C&C 要求でした。
- CTA が、2 回の C&C 試行を **IP アドレスへの HTTP トラフィック（ドメイン未指定）**として検出しました。この動作カテゴリは、純粋な IP アドレスに対するシーケンス外通信を表す異常な要求を突き止めます。このようなアクティビティは、マルウェアがまだアクティブであるかを確認する「キープアライブ」チェックとしてマルウェアが実行している可能性があります。または、単なるデータの抜き出しや、悪意のあるインフラ（C&C）からの追加命令の受信である可能性もあります。このタイプのトラフィックは、通常のインターネット ブラウジングで発生することはありません。
- 75 の C&C 要求のすべてが、シグニチャベースおよびレピュテーションベースのテクノロジーでは検出されませんでした。

HTTP 要求の例（一部のみ抜粋し匿名化）

http://94.XXX.XXX.XXX/m/IbQXXXVjj7iA+O54XXXodmmGcNZxtMZdvqyB5EkJAUmLb3pvGIRvqizzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXXog+fq4XXXaE0qfJf1FwalZJKnDc7U0H30+XkiXXXIApkslTo5yvM0TkHrZncwIvumxLCQ+fq4XXXOT…

C&C サーバ #3（fistristy.com）への通信

通信の特性：

- fistristy.com ドメインへの要求の総数は 175 でした。すべて C&C 通信でした。
- Web シグニチャベースとレピュテーションベースのテクノロジーがすべての要求をブロックしました。

HTTP 要求の例

hXXp://fistristy.com/aa/

C&C サーバ #4（ffeed5.com）への通信

通信の特性：

- ffeed5.com に対する要求の総数は 7 でした。すべて CWS Premium によってブロックされた C&C 通信でした。
- CTA は、**異常な HTTP トラフィック** カテゴリとして 6 個の要求を検出しました。この動作カテゴリには、一般的に継続的な CTA の分析によって確立された動作のベースラインに適合しないマルウェアの動作が含まれます。「ベースライン」という用語は、Web トラフィックの分析によって傾向と特性を「学習する」CTA システムによって作成された統計モデルの状態を表しています。CTA は、最適な検出を行うために、ネットワークの変化（たとえば、夜間や日中）に応じて自動的にベースラインを調整します。
- CTA は、ネットワーク動作の長期的なモデリングを使用して、一見ばらばらなアクティビティを関連付けます。そのデータはネットワーク全体にわたる個々のユーザの動作と比較され、隠れた持続的な脅威を検出する機能を強化するために利用されます。

HTTP 要求の例

hXXp://ffeed5.com/cmd?version=1.5&aid=555&id=24c6b407-5010-4d8d-a266-ffdac7d6f901&os=6.1.7601_1.0_64

まとめ

この石油ガス企業のセキュリティ チームは、15,000 以上のユーザが 1 日あたり平均 3,500 万以上の Web トランザクションを生成するネットワークのアクティビティを監視し、セキュリティ イベントの優先順位付けを行うための効率的な手段を必要としていました。また、脅威をブロックするだけでなく、各種の防御をすり抜けてしまう脅威をすばやく特定するソリューションも必要でした。同社が求めていたのは、脅威が完全に解消されるまで、疑わしいアクティビティの存在をセキュリティ担当者に警告し続けるように設計されたテクノロジーです。

Cisco CWS Premium には CTA が含まれているため、これにより、同社は機械学習や高度な統計情報に基づいてネットワーク内の IOC をほぼリアルタイムに検出するネットワーク動作分析システムを手にすることになりました。Cryptolocker ランサムウェアの感染事例では、CTA はセキュリティ チームが感染を完全に解消するまで、悪意のあるアクティビティについての警告を続けました。また、セキュリティ チームはマルウェアの動作に関する CTA のインサイトに基づいて、攻撃前、攻撃中、攻撃後の各フェーズで最も重大な脅威のみに集中して対処できるようになりました。

詳細

CTA と AMP を含む Cisco CWS Premium は、現在および将来における企業のセキュリティ課題にいかに対応するかというシスコの戦略に合致するもので、脅威を検出して理解し、阻止するために貢献します。継続的な分析とリアルタイム セキュリティ インテリジェンスをクラウドから提供し、あらゆるセキュリティ ソリューション間で共有することで、有効性を高めます。この 3 つのソリューションの組み合わせによって、CWS Premium は、セキュリティ業界が以前は検出できなかった新たな指揮統制チャネルを認識し、組織が攻撃コンティニューム全体にわたるセキュリティ課題に対処できるようにします。

CWS Premium の詳細については、http://www.cisco.com/go/cws [英語] を参照してください。

CTA の詳細については、http://www.cisco.com/go/cognitive [英語] を参照してください。

AMP の詳細については、http://www.cisco.com/go/amp [英語] を参照してください。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

Printed in USA C36-733153-00 10/14