Cisco Ransomware Defense：簡易防御 v1.4

最終更新日：2018 年 8 月 8 日

このデモンストレーションについて

この Ransomware Defense デモンストレーションのガイドには、次の内容が含まれています。

- 要件
- このソリューションについて
- トポロジ
- はじめに
- シナリオ 1：Cisco クラウド E メール セキュリティにより、ランサムウェアから電子メールを保護
- シナリオ 2：Cisco Umbrella により、ランサムウェアから DNS を保護
- シナリオ 3：Cisco AMP for Endpoints により、ランサムウェアからファイルを保護
- シナリオ 4：ランサムウェアの実行ファイルによるシステムの感染

要件

次の表に、本デモンストレーションに必要な要件の概要を示します。

表 1. 要件

必須	オプション
● Web ブラウザがインストールされたコンピュータ	● なし

このソリューションについて

Cisco Ransomware Defense ソリューションは、2 段階のフェーズに分かれています。「簡易防御フェーズ」では、迅速に導入できるクラウドベースのサービスを使用します。お客様は、現在ほとんど対策を行っていない場合でも、数時間または数日以内にサービスを実装し、即座に保護を導入できます。「高度防御フェーズ」には、販売と実装に長期間かかる製品が含まれています。簡易防御フェーズの要素を導入した後は、お客様との信頼関係を強化する必要があります。高度防御のコンポーネントは、強化された Web フィルタリング、ネットワークのセグメント化、ネットワーク分析、脅威インテリジェンスを追加します。これらは、境界を侵害する脅威を迅速に検出して封じ込めます。高度防御のコンポーネントについては、別のデモで説明する予定です。

Cisco Ransomware Defense ソリューションの簡易防御の要素は、導入しやすいクラウドベース アーキテクチャのソリューションです。システムおよびネットワークに対するランサムウェアの脅威を検出し、防止し、封じ込めます。

Cisco Ransomware Defense の簡易防御には、次の機能があります。

- ランサムウェアまたはランサムウェアを展開するエクスプロイト キットのホスト サイトに接続する前に、DNS 要求をブロックすることで、社内ネットワークの内外でデバイスを保護します。
- ランサムウェア ファイルがエンドポイントで実行されるのを防止します。
- 悪意のある電子メールの添付ファイルや URL を特定し、スパムおよびフィッシング電子メールを通じてもたらされるランサムウェアをブロックします。
- 攻撃が拡散する前に対応します。

簡易防御の製品は、クラウド サービスの提供に向かないお客様に対しては、ローカル アプライアンスとして導入できます。ただし、この場合は実装に要する時間が増えるため、「簡易」ではなくなります。

詳細については、http://www.cisco.com/go/ransomware を参照してください。

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定されたユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント資格情報は、アクティブ セッションの [トポロジ（Topology）] メニューのコンポーネント アイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

図 1. dCloud のトポロジ

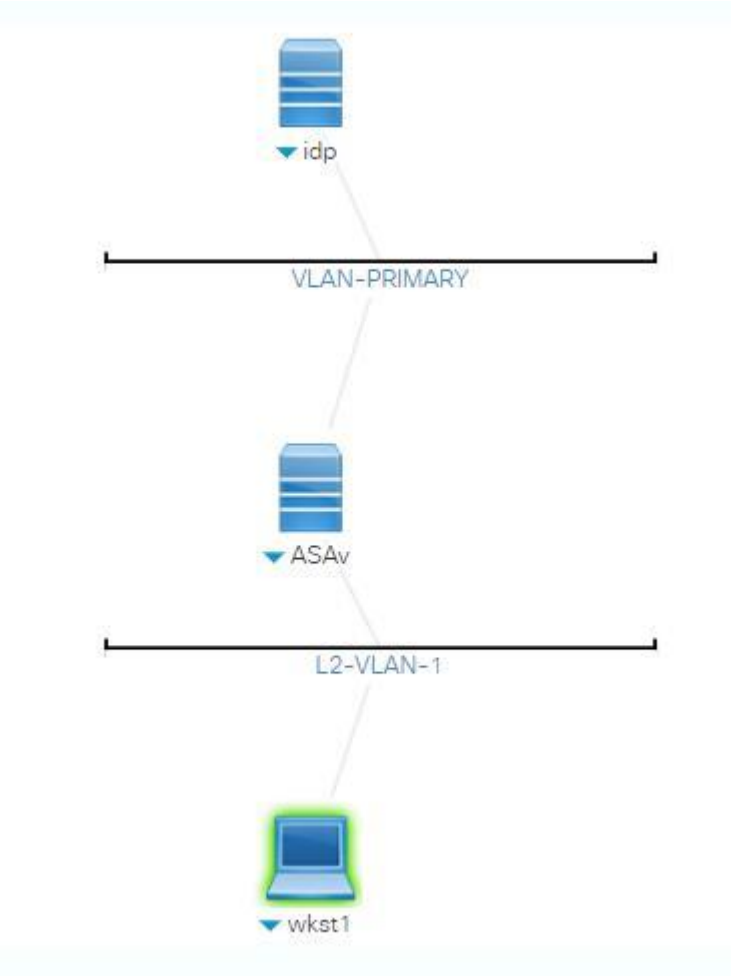
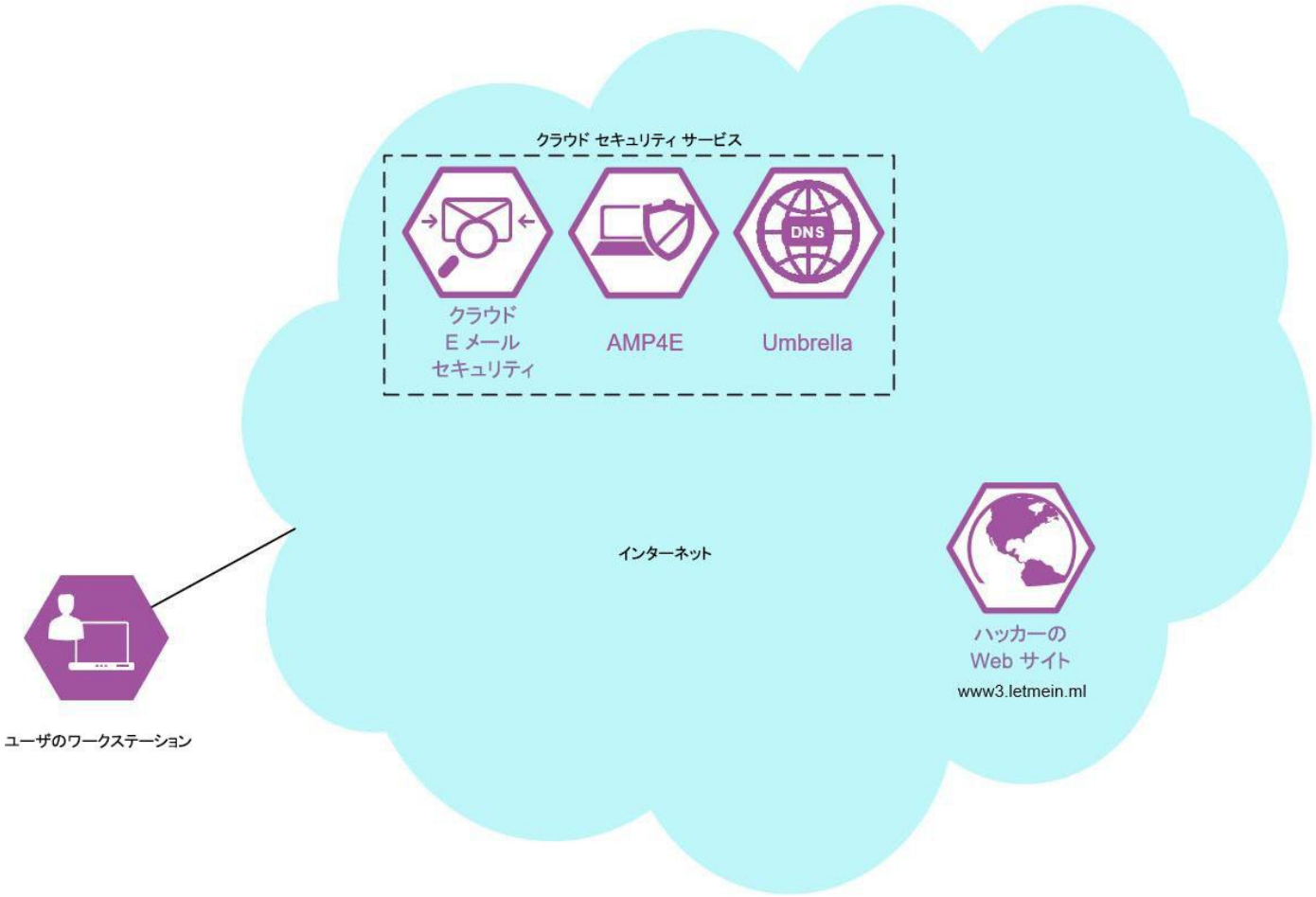


図 2. 論理トポロジ



はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるためには、入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[手順を見る]

注: セッションがアクティブになるまで最長で 10 分かかることがあります。

2. 安全上の理由から、ワークステーションへの接続には、提供されたリモート デスクトップ サービスのみを使用してください。このデモンストレーションでは、実際のランサムウェアのサンプルを使用します。そのため、VPN でこのラボに接続した場合にデバイスが感染する可能性があります。
   - Cisco dCloud リモート デスクトップに接続します [手順を見る] 。クレデンシャルは自動的に提供されます。

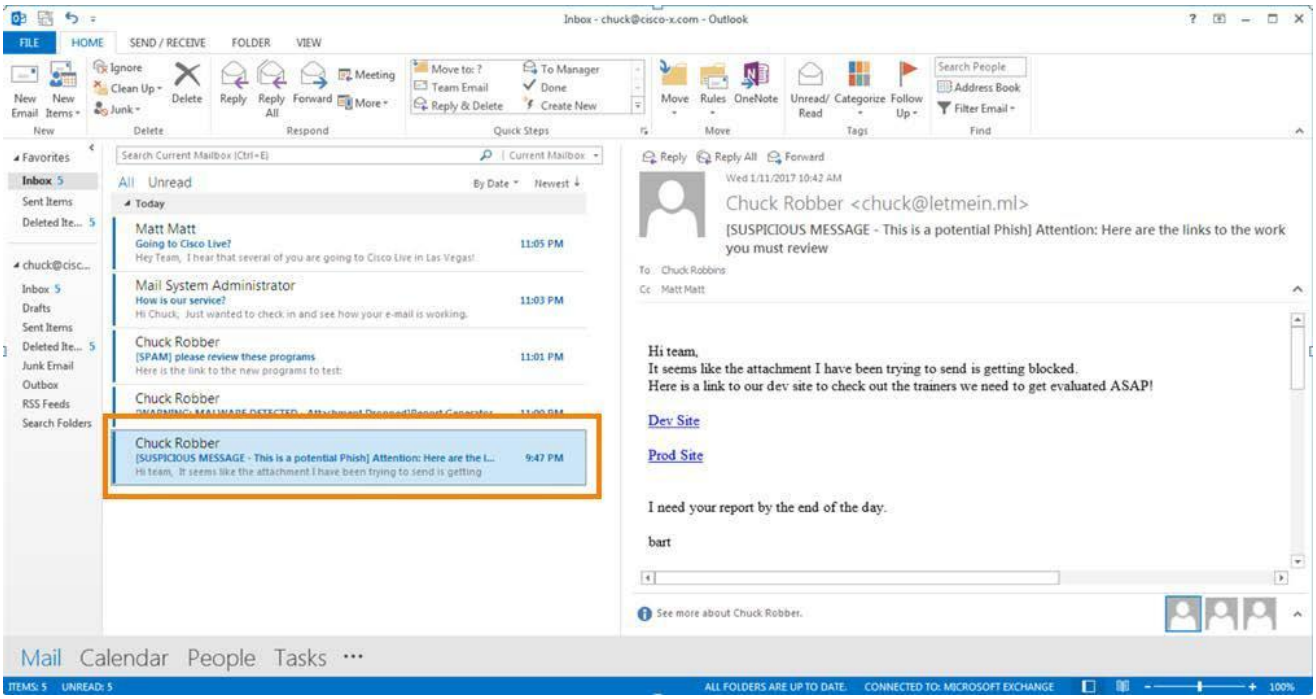
シナリオ 1.　Cisco クラウド E メール セキュリティにより、ランサムウェアから電子メールを保護

このシナリオでは、電子メールの本文や悪意のある添付ファイルに組み込まれた悪意のある Web サイト リンクによる電子メール ベースのランサムウェア攻撃から、Cisco クラウド E メール セキュリティがユーザを保護する仕組みを示します。

手順

1. デスクトップで Microsoft Outlook を開きます。
2. 受信トレイを確認します。いくつかの電子メールが、すでに Outlook クライアントで受信されています。

図 3.　いくつかの電子メールがある受信トレイ



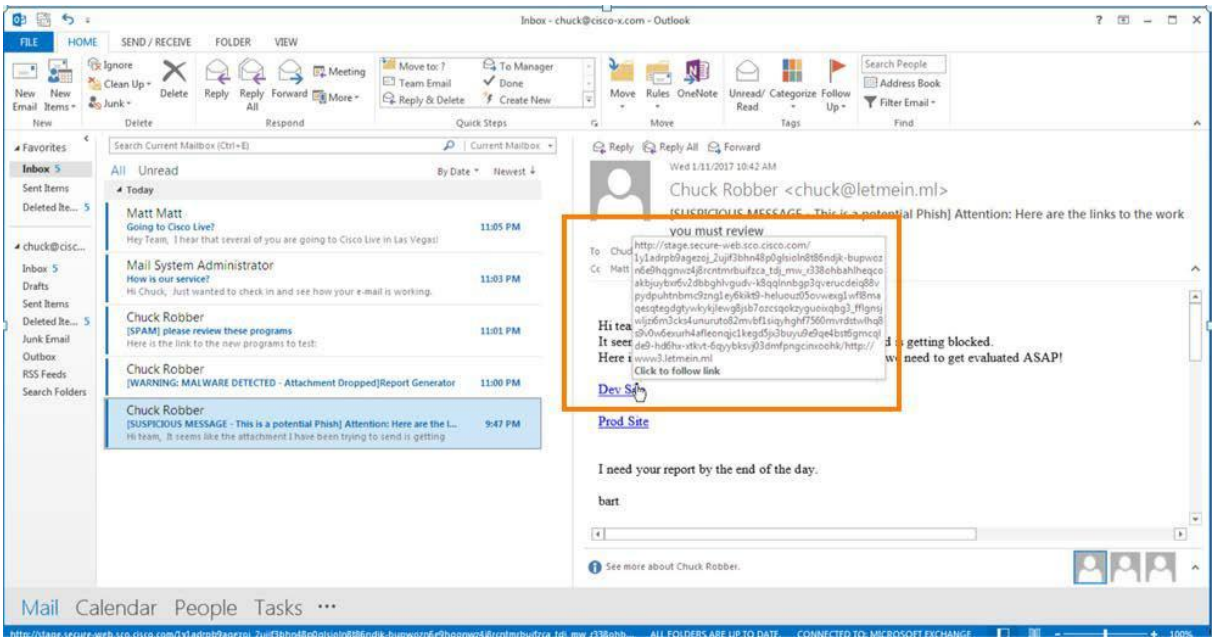
3. 「**SUSPICIOUS MESSAGE – This is a potential Phish**」（疑わしいメッセージ – これはフィッシングの可能性があります）という件名の電子メールを選択します。

注: この電子メールには、複数の組み込み Web リンクが含まれています。

4. マウス ポインタをリンクに合わせると、宛先が表示されます。

注:CES では、アクセスの際に CES ポータルをプロキシとして経由するようにリンクが書き換えられています。http://stage.secure-web.sco.cisco.com は CES ポータルです。URL の最後の部分が元のメッセージの URL を示しており、[Dev サイト(Dev Site)] に該当するのが http://www3.letmein.ml、[Prod サイト(Prod Site)] に該当するのが http://www.internetbadguys.com です。

図 4. リンク上にマウスオーバーした状態



5. [Dev サイト(Dev Site)] リンクをクリックします。

6. 10 秒後に、Cisco E メール セキュリティのポータルにリダイレクトされ、サイトへのアクセスを確認するメッセージが表示されます。

注:ネットワークの接続状況によって、サイト プレビューが表示される場合と表示されない場合があります。これによるデモンストレーションへの影響はありません。

図 5. サイトへのアクセスの確認

7. [このサイトを信頼する(I trust this site)] を選択する場合。ドメイン名がすでに脅威のある Web サイトとして検出されているため、Cisco Umbrella の DNS セキュリティによってアクセスがブロックされます。Umbrella は、次のシナリオでテストされます。このブラウザ ウィンドウはここで閉じて構いません。

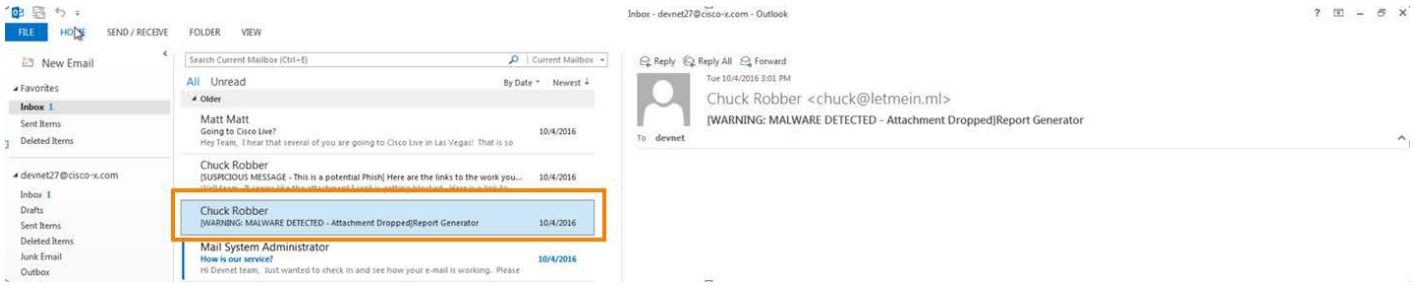
注: プレビュー画像を確認してサイトを信頼する選択を行った場合でも、Cisco クラウド E メール セキュリティが継続的に Web サイトのコンテンツを監視しており、クラウドの脆弱性データベースに基づいて、悪意のあるアクティビティやリンクを特定します。脅威がすでにデータベースで定義されている場合、ユーザがファイルやリンクにアクセスしようとするとすぐに阻止します。

図 6. サイトをブロック

8. Outlook に戻り、Chuck Robber（chuck@letmein.ml）からの別の電子メールを選択します。この電子メールの件名は、「**[WARNING: MALWARE DETECTED – Attachment Dropped] Report Generator**」（[警告：マルウェアが検出されました - 添付ファイルを廃棄しました] レポート ジェネレータ）です。

注：この電子メールにはランサムウェアの添付ファイルが含まれていましたが、AMP を備えた Cisco クラウド E メール セキュリティによって削除されました。セキュリティ システムは、添付ファイルのファイル ハッシュに基づいて悪意のあるファイルとして特定し、ポリシーに基づいて添付ファイルを削除しました。ただし、電子メール メッセージは、それでもユーザに配信されました。管理者は、もう 1 つの選択肢として、電子メール メッセージ全体の配信を禁止するポリシーを作成することもできます（推奨）。

図 7. マルウェアが検出された電子メール



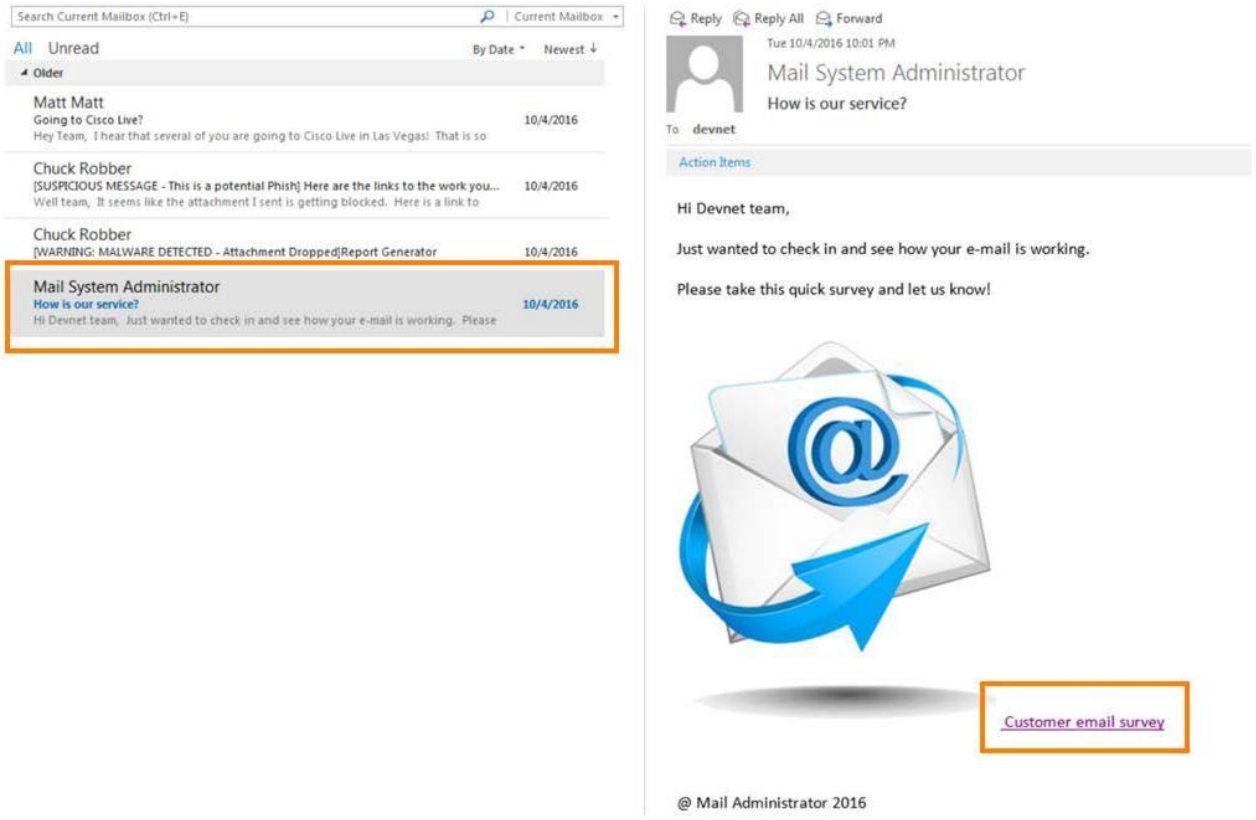
シナリオ 2.　Cisco Umbrella により、ランサムウェアから DNS を保護

このシナリオでは、悪意のある Web リンクにアクセスしようとすると、Cisco Umbrella ソリューションによってブロックされます。

手順

1. Outlook で、メール システム管理者からの「**How is our service?**」（私たちのサービスはいかがですか）という件名の電子メールにアクセスします。
2. [顧客の電子メール調査（Customer email survey）] リンクをクリックします。

図 8.　「How is our service?」（私たちのサービスはいかがですか）という件名電子メール



注:この電子メールは、外部ソースからの配信のように装われています。システムが Cisco クラウド E メール セキュリティで保護されていた場合、悪意のあるリンクを含む電子メールや、内部ドメインから送信されたように偽装している電子メールが特定され、ブロックされます。このデモンストレーションでは、Cisco Umbrella が悪意のあるファイルへのリンクをブロックする様子を観察するために、意図的にクラウド E メール セキュリティを回避してあります。

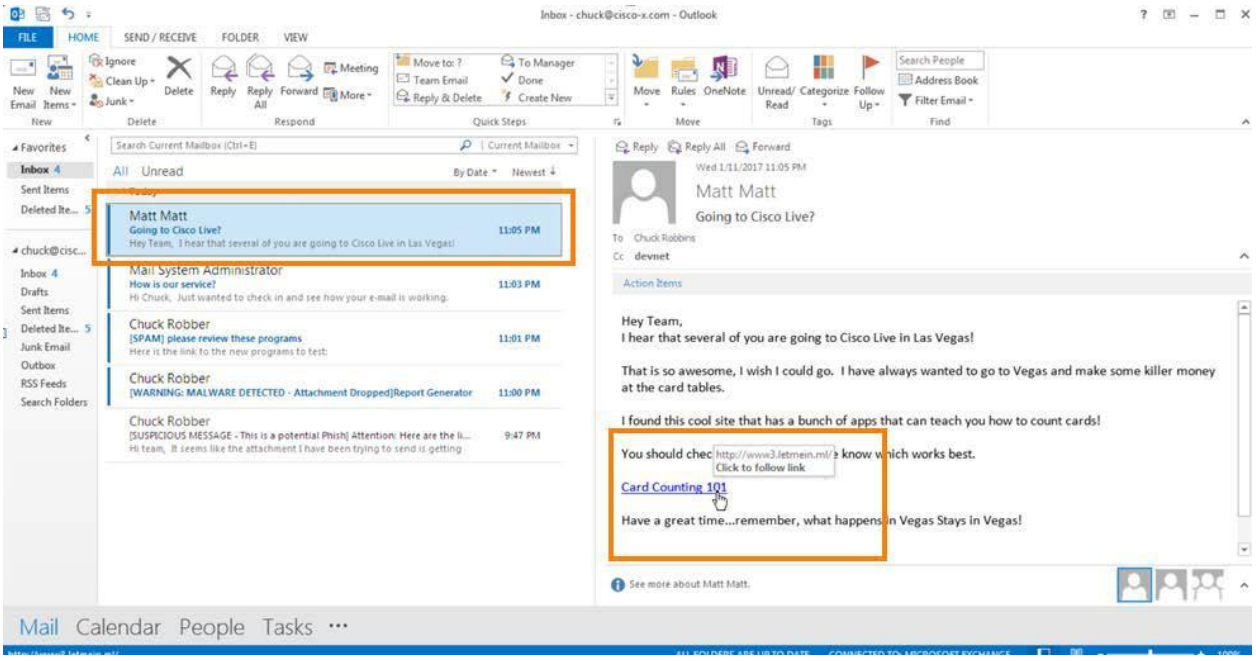
3. Cisco Umbrella には、ブロックされたメッセージが表示されます。

図 9. ブロックされた脅威

4. 次に、Matt Matt からの「**Going to Cisco Live?**」（Cisco Live に行きますか）という件名の電子メールを選択します。

5. [カードカウンティング 101（Card Counting 101）] リンクをクリックします。

図 10. [カードカウンティング 101（Card Counting 101）] リンク



6. Cisco Umbrella には、ブロックされたメッセージが表示されます。

図 11. ブロックされた脅威

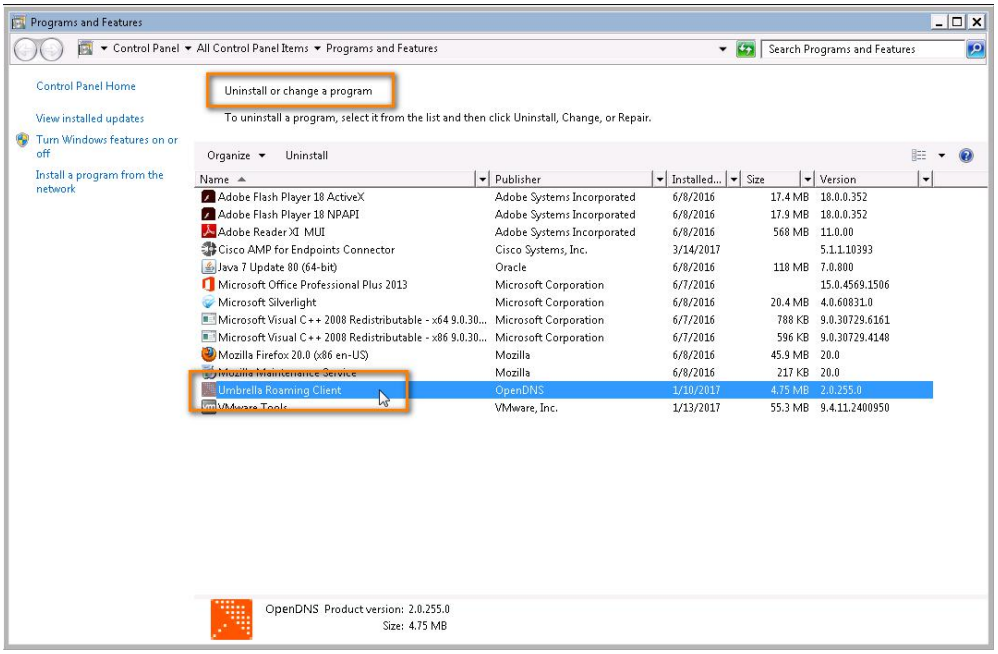
注:この電子メールは内部のメール ユーザおよびサーバから届いており、Cisco クラウド E メール ソリューションでは検査されていません。同様に、ユーザが Web ページやその他のクライアント(Gmail や Facebook など)で個人用メッセージを確認する場合、Cisco Umbrella ソリューションは、悪意が確認されたドメインから来る URL ベースのランサムウェアすべてからユーザを保護します。

7. ほかに思いつく不適切または悪意のある Web サイトに接続し、Cisco Umbrella がどのように反応するか確認します。

8. Umbrella の効果を確認できたら、Umbrella を削除します。デスクトップの [プログラムと機能(Programs and Features)] ショートカット アイコンをクリックします。[Umbrella ローミング クライアント(Umbrella Roaming Client)] をクリックし、[アンインストール(Uninstall)] を選択します。

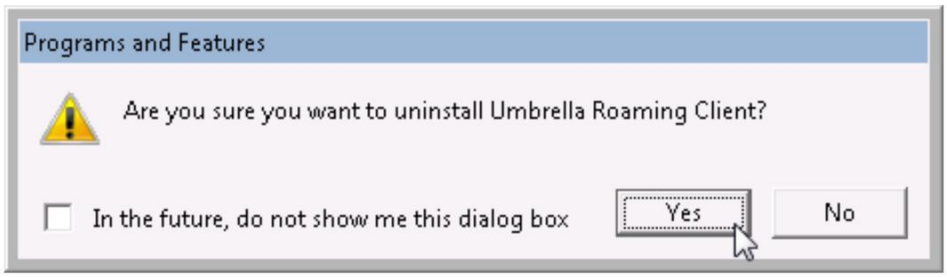
注:あるいは、[スタート(Start)] ボタンをクリックし、[コントロール パネル(Control Panel)] を選択することもできます。コントロール パネルで、[プログラムのアンインストール(Uninstall a program)] を選択します。

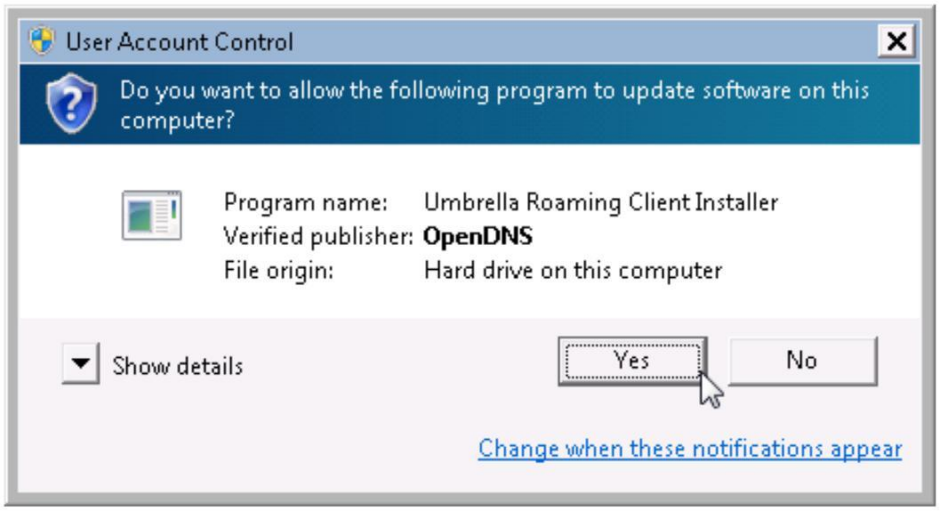
図 12. Umbrella ローミング クライアントのアンインストール

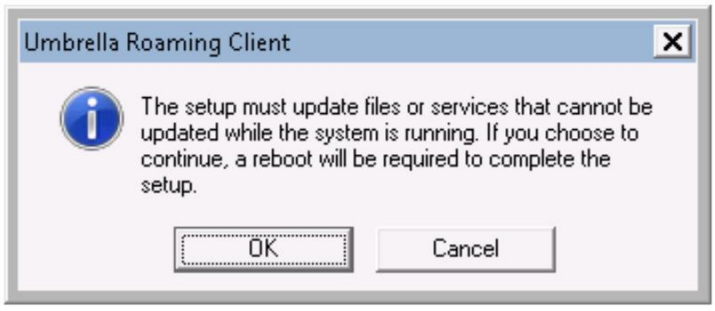


9. アンインストールを確認するためのプロンプトが数回表示されるので、[はい（Yes）]、[はい（Yes）]、[OK] の順にクリックします。

図 13. プログラムのアンインストールの確認







注：このデモでは、実際にシステムを再起動する必要はありません。システムをシャットダウンしないでください。

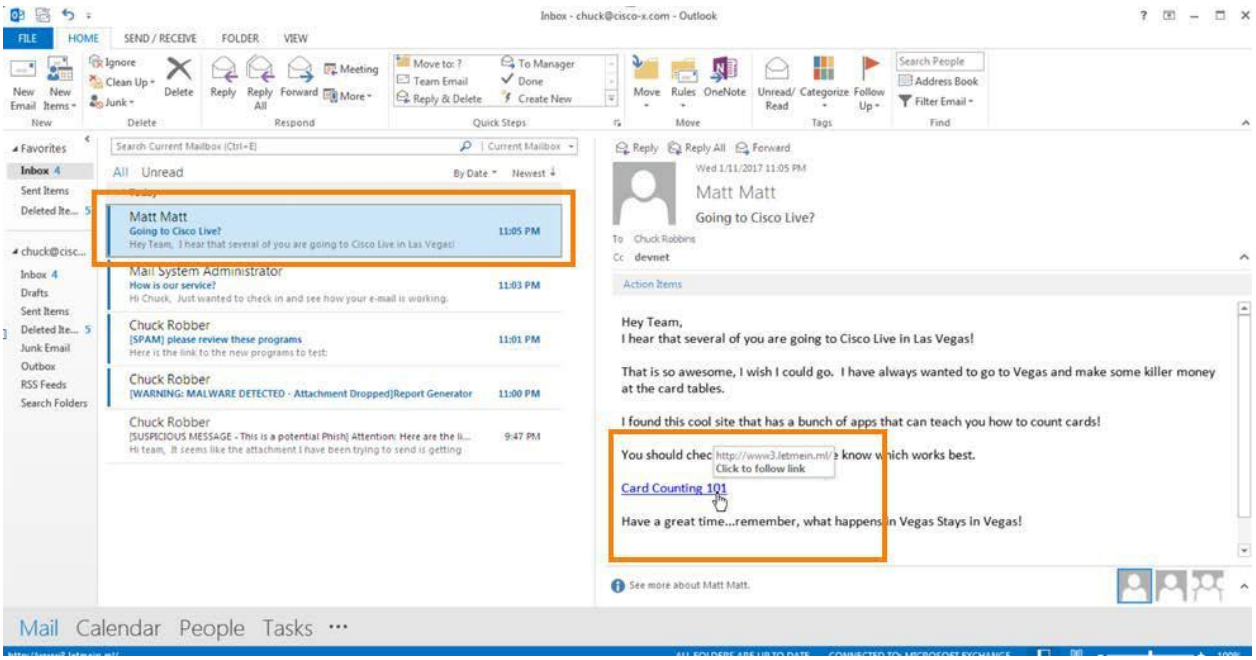
シナリオ 3.　Cisco AMP for Endpoints により、ランサムウェアからファイルを保護

このシナリオでは、Cisco Umbrella を正常にアンインストールした後、[カードカウンティング（Card Counting）] の Web サイトへのアクセスが許可されます。このサイトでは、動作中の実際のランサムウェアがホストされています。Cisco AMP for Endpoints がランサムウェアを検出し、実行されるアプリケーションをブロックする様子を確認します。

手順

1. Outlook で、Matt Matt からの「**Going to Cisco Live?**」（Cisco Live に行きますか）という件名の電子メールを選択します。
2. [カードカウンティング 101（Card Counting 101）] リンクをクリックします。

図 14.　[カードカウンティング 101（Card Counting 101）] リンク

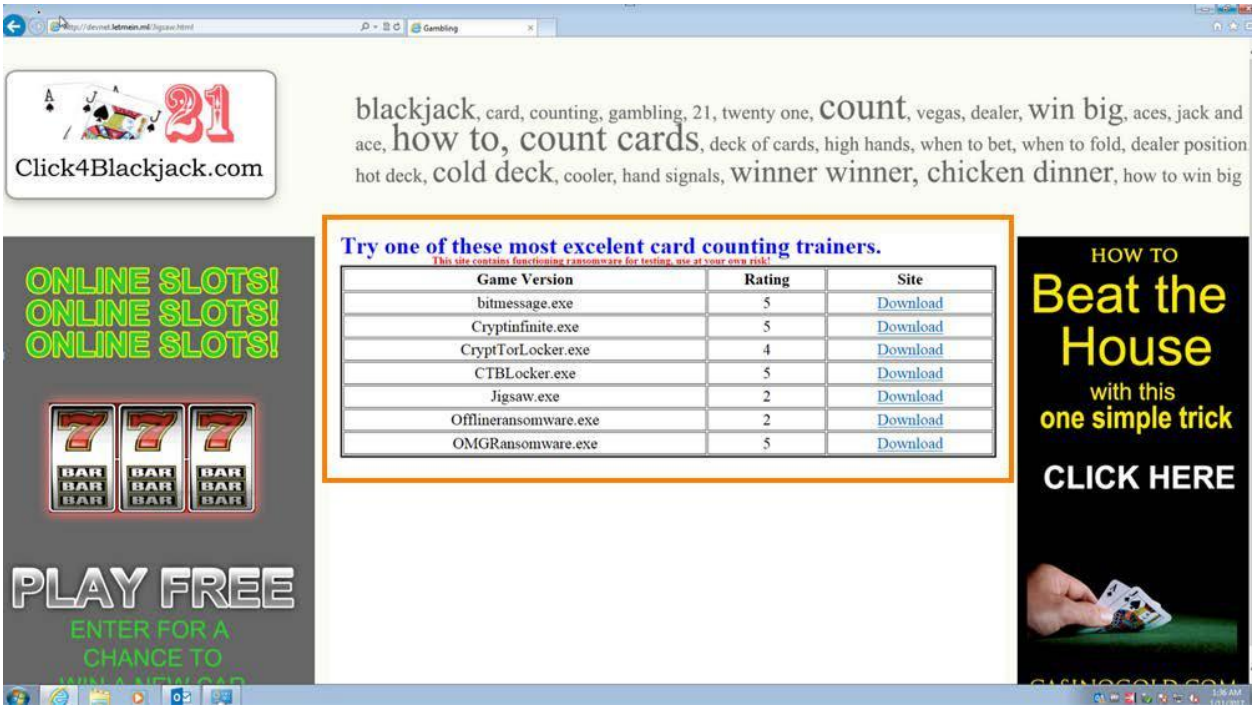


3. [いずれかのカードカウンティングトレーナーを試すにはここをクリック（Click here to try one of our card counting trainers!）] のリンクを選択します。

図 15. カード カウンティングのリンク

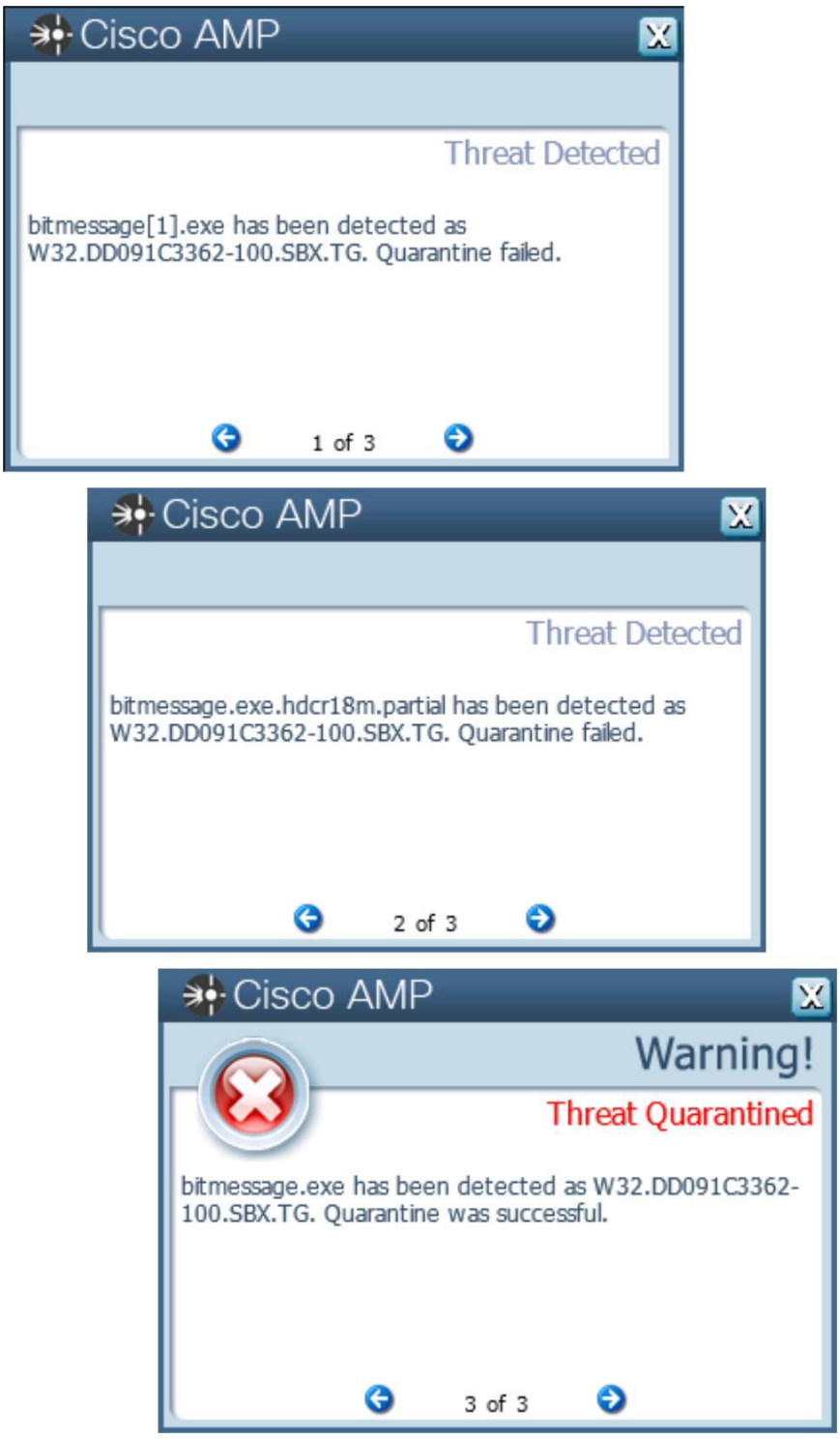
4. いずれかのランサムウェア（実行ファイル）の隣にある [ダウンロード（Download）] をクリックし、ファイルの**実行**を試みます。

図 16. ランサムウェアのダウンロード



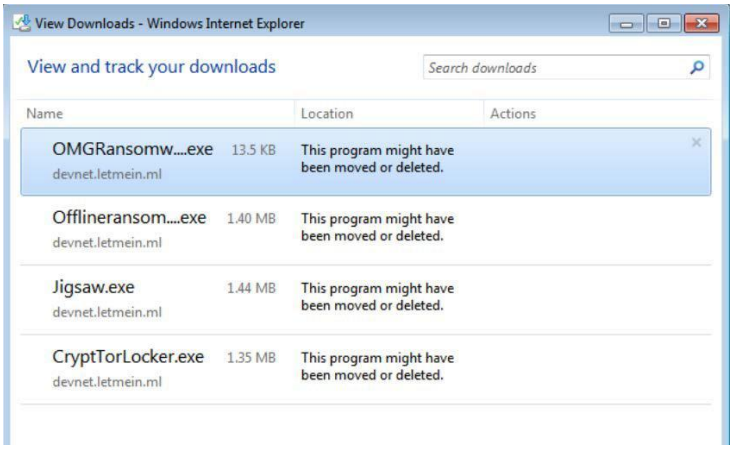
5. Cisco AMP for Endpoints は、脅威のあるファイルをすぐに隔離します。「ファイルが移動したか削除された可能性があります」というエラー メッセージが表示されます。ブラウザの通知ウィンドウにおいて。右矢印をクリックして Cisco AMP の警告を一通り確認して、関連する通知を探します。

図 17. 検疫された脅威



6. 他のランサムウェア ファイルを**ダウンロードし、実行します**。Internet Explorer の [ダウンロードの表示（View downloads）] ボタンをクリックし、ダウンロード フォルダを開きます。ダウンロードしたランサムウェア ファイルが AMP for Endpoints によって隔離され、削除されていることを確認します。

図 18. ブロックされたランサムウェア ファイルが表示された [ダウンロード（Download）] ウィンドウ

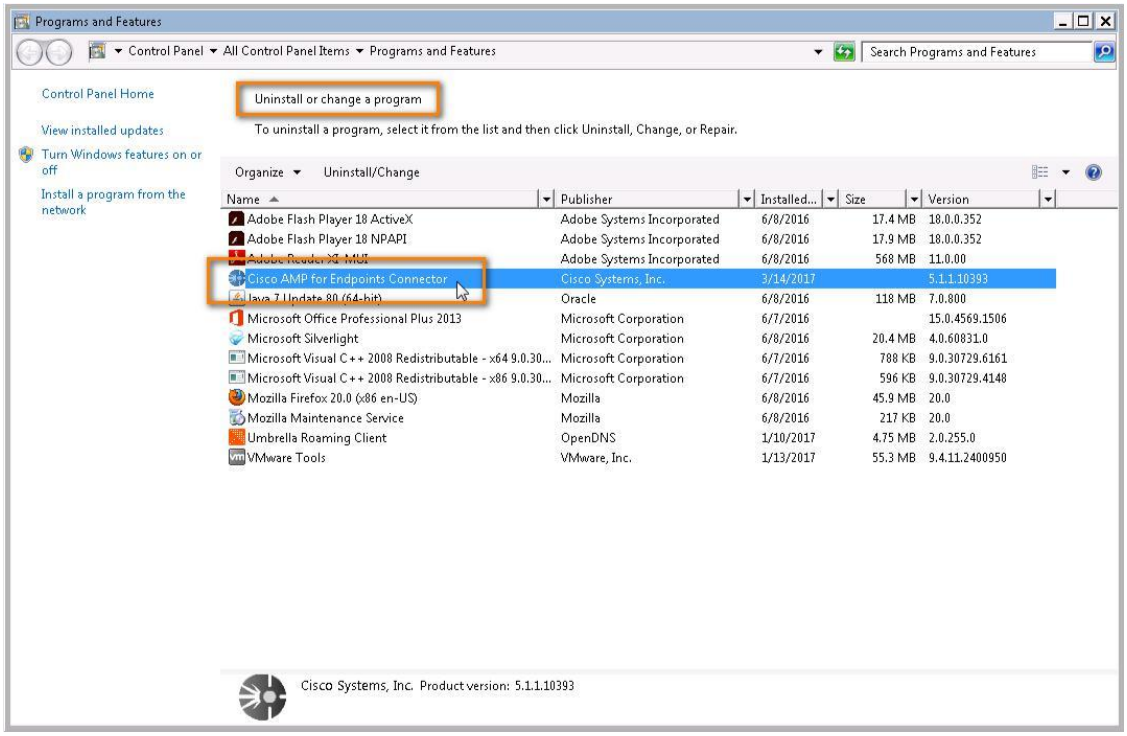


7. 悪意のあるファイルのブロックに関して AMP の効果が確認できたので、この最後の保護レイヤを削除します。[プログラムと機能（Programs and Features）] ウィンドウに戻り、[Cisco AMP for Endpoints コネクタ（Cisco AMP for Endpoints Connector）] をアンインストールします。

注：AMP コネクタを後日再インストールするか確認するメッセージが表示されたら、[いいえ（No）] をクリックします。

8. アンインストール中、確認のためのプロンプトが数回表示されます。[次へ（Next）]、[閉じる（Close）]、[いいえ（No）] の順にクリックし、最後に再起動するように求められたら、[いいえ（No）] を選択します。

図 19. Cisco AMP for Endpoints コネクタをアンインストールします。



シナリオ 4.　ランサムウェアの実行ファイルによるシステムの感染

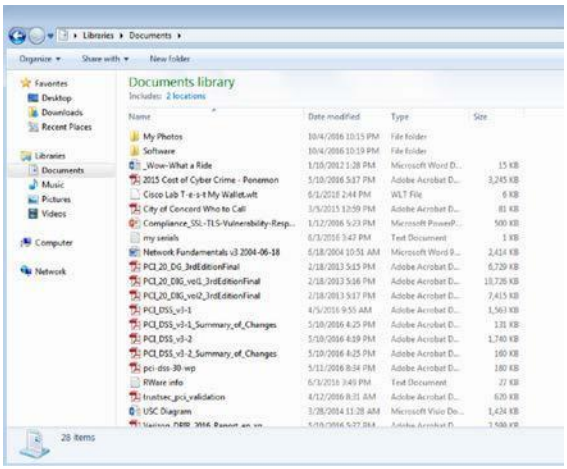
このシナリオでは、システムは Cisco Ransomware Defense ソリューションの製品によって保護されなくなりました。この保護がない場合、悪意のあるすべての Web サイトにアクセスでき、ランサムウェアの実行ファイルをダウンロードして実行する恐れがあります。ここでは、ユーザ ファイル（ドキュメント フォルダにあるサンプル ファイル）が瞬く間に暗号化され、金銭要求の通知が表示されるに至る過程を観察できます。

手順

1. [マイドキュメント（My Document）] フォルダを開き、デスクトップで確認できるようにします。

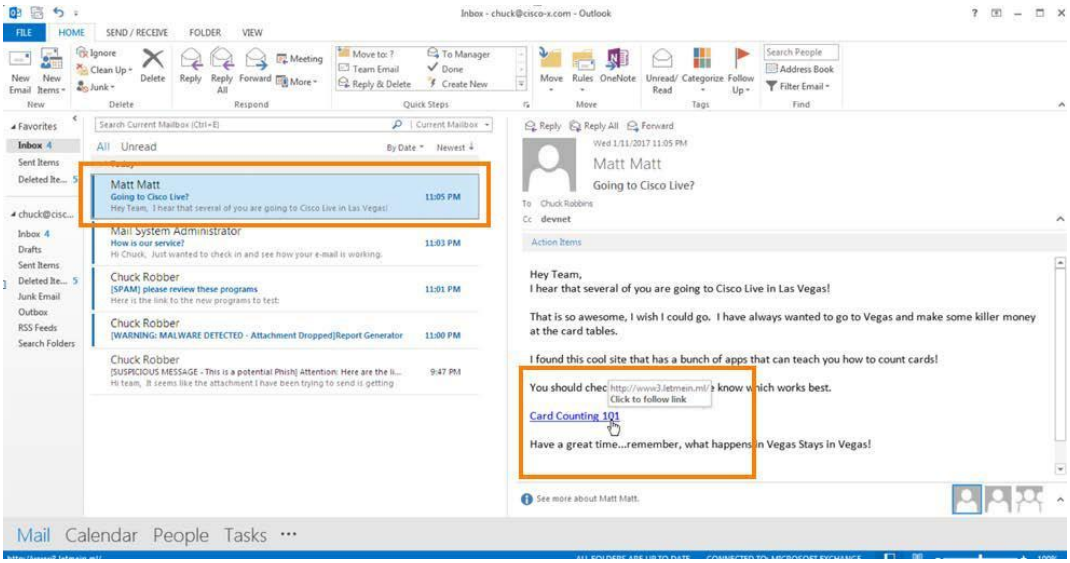
注：タスク トレイのクロックを右クリックし、[タスクマネージャ（Task Manager）] を選択して、システムのタスク マネージャを開き、実行中のユーザのプロセスを観察する方法でも確認できます。

図 20.　[マイドキュメント（My Document）]



2. Outlook で、Matt Matt からの「**Going to Cisco Live?**」（Cisco Live に行きますか）という件名の電子メールを選択します。
3. [カードカウンティング 101（Card Counting 101）] リンクをクリックします。

図 21. [カードカウンティング 101（Card Counting 101）] リンク



4. [いずれかのカードカウンティングトレーナーを試すにはここをクリック（Click here to try one of our card counting trainers!）] のリンクを選択します。

図 22. カード カウンティングのリンク

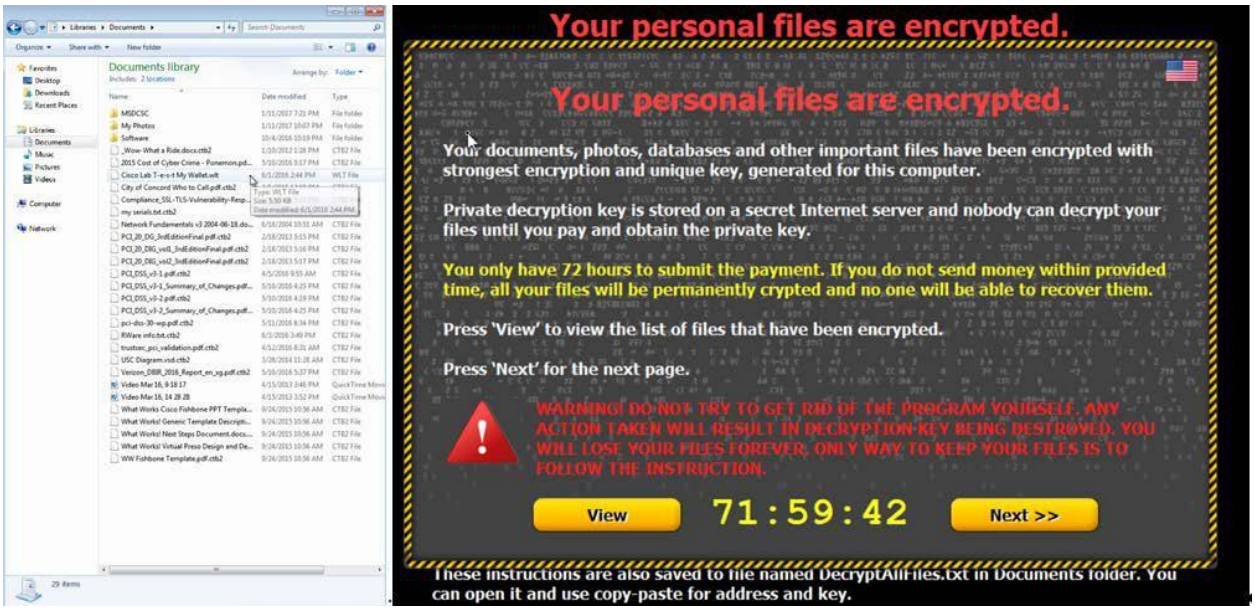
5. いずれかのランサムウェアの実行ファイルを [ダウンロード（Download）] し、**ファイルを実行します**。

注：実行ファイルは破損したアプリケーション ファイルとして実行されます。一部の実行ファイルは別のプロセスになりすまし、自身の正体を隠します。一部の実行ファイルは、何もインストールしないように見える場合もあります。ただし、ランサムウェアはしばしばバックグラウンドで動作します。また、ランサムウェアは、デスクトップや [マイドキュメント（My Document）] フォルダにテキストを残す場合があります。デスクトップの背景が金銭要求の文章に変更されるか、ポップアップ メッセージとして表示される場合もあります。[マイドキュメント（My Document）] フォルダ内のほとんど、またはすべてのドキュメントが暗号化されます。

図 23. ランサムウェアのダウンロード

6. **CTBLocker ランサムウェア**の例を次に示します。ワークステーションがランサムウェアに感染されると、[マイドキュメント（My Document）] の内容が 2 分以内に暗号化され、デスクトップの背景が金銭を要求する文章に置き換えられます。

図 24. CTBLocker ランサムウェア



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