なりすましメールからの保護

Office 365向けセキュリティソリューション

» メールで使用される偽装手法の分析とトレンドマイクロの SaaS 型メールセキュリティ製品が提供する保護ソリューション

目次

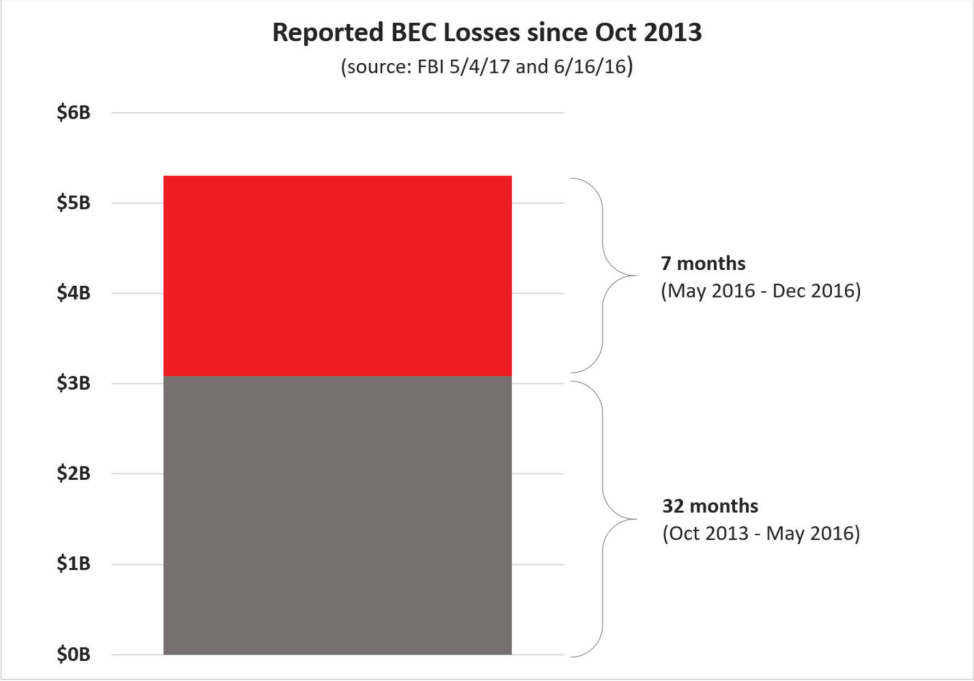
はじめに

長年にわたり、メールは多くの企業や組織で主要なコミュニケーションツールとして利用されてきました。簡単な会話のやり取りから情報の共有、重要な取引の履行に至るまで、メールは私たちの日常に欠かすことのできないツールとなりました。しかしメールの普及と利用者の増加は、悪意のある攻撃者によるメールの不正使用や脆弱性悪用の機会を増大させました。

攻撃者がその手段にメールを好んで使用する理由には、メールの使いやすさと偽装の容易さがあります。SMTP (Simple Mail Transfer Protocol) における送信者認証メカニズムの欠如は、メール送信者の偽装を可能にしました。

多くの攻撃者は何らかの手法でメールを偽装して標的を欺こうとします。フィッシング攻撃、なりすまし攻撃、およびビジネスメール詐欺 (BEC) 攻撃には、様々な手法のなりすましメールが使われています。なりすまし攻撃の脅威は 2015 年の半ばごろ拡大し、2016 年の下半期には、その攻撃の激しさはより顕著なものになりました。

この攻撃手法は頻繁に悪用され、2017 年 5 月に米連邦捜査局 (FBI) が発表したレポートによると、2013 年以降に世界中の被害者から報告された**BEC 単独による被害総額は 50 億米ドルを超えました**。トレンドマイクロは、この種の攻撃が今後も増加の一途をたどり、よりグローバルな規模で利用されるであろうと予測しています。



正当な送信者からのメールであるかのように見せかけた、なりすましメールを作成する機能を持つマルウェアも存在します。KLEZ ワームをはじめとした多くの最新のマルウェアは、感染したシステムから標的のメールアドレスを探し出し、なりすましメールを送信して感染を拡大させることができます。

サイバー犯罪による攻撃もより複雑に進化しており、見た目では判断できないほど巧妙に偽装したメールが使用されています。こうした偽装を見破るには、メールヘッダを詳しく分析する必要があります。しかし専門知識のない一般的なユーザは、メールヘッダを分析する方法を知りません。

この種の攻撃に対処するには、従来のスパムメール対策フィルタにおいて、メール認証の既存の技術に新しい機能を組み合わせる必要があります。このホワイトペーパーでは、これらの技術を Trend Micro Hosted Email Security (以下、HES) および Trend Micro Cloud App Security (以下、CAS) をはじめとしたトレンドマクロの Office 365 向けスマートプロテクションで活用し、Office 365 ユーザをなりすましメールから保護する方法について説明します。

なりすましメールによる攻撃の種類

なりすましメールの作成にはメールの偽装が不可欠です。フィッシング攻撃および BEC 攻撃では、送信者のメールアドレスを偽装して、メールが正規の送信元から送信されたかのように見せかけます。その結果、標的となった人物は、何も知らずに機密情報を公開したり、身元不明のアカウントに送金したり、マルウェアに感染してしまうことさえあります。

メールの偽装手法には次のものがあります。

- 「エンベロープ From」の偽装
- 「メッセージ From」の偽装
- 類似ドメインの悪用
- 無料メールアカウントの悪用
- メールアカウントの侵害

「エンベロープ From」と「メッセージ From」

メールの偽装手法について詳しく説明する前に、メールで使用される送信者情報について説明しておきます。

メールには通常、「エンベロープ From」アドレスと「メッセージ From」アドレスの 2 種類の送信者情報が含まれています。「エンベロープ From」アドレスは、「メール From」アドレスや「SMTP From」アドレスと呼ばれることもあります。これは SMTP セッションで MAIL FROM: コマンドに指定される送信者アドレスです。

「エンベロープ From」アドレスには、メール配信で問題が発生した場合にバウンスメッセージやエラーが返されます。このアドレスは受信者に表示される場合も、されない場合もあります。一方の「メッセージ From」アドレスは、Outlook などメールアプリケーションの「送信者」フィールドに表示されるアドレスで、受信者が確認できます。

「エンベロープ From」アドレスを確認するには、メッセージヘッダを表示する必要があります。表示方法は、使用されたメールクライアントアプリケーションや Web メールアプリケーションによって異なります。ほとんどの一般的なメールでは、「エンベロープ From」と「メッセージ From」は同じになります。これは特に、組織内で使用する個人および個別のメールアドレスに当てはまります。

これらの送信者情報に異なるアドレスを指定する正規のメールもあります。一部の自動メール送信ソフトは、バウンスメッセージを中央リポジトリのメールボックスに、ユーザの返信を「メッセージ From」に指定された別のアドレスに送信します。

「エンベロープ From」の特別なエラー処理用メールボックスの使用については、RFC 5321 で次のように定義されています。

"It is possible for the mailbox in the return path to be different from the actual sender's mailbox, for example, if error responses are to be delivered to a special error handling mailbox rather than to the message sender. When mailing lists are involved, this arrangement is common and useful as a means of directing errors to the list maintainer rather than the message originator. (return path 内のメールボックスが実際の送信者のメールボックスと異なることも可能である。例えばエラー応答がメッセージ送信者にではなく特別なエラー処理用メールボックスに配送されるべき場合である。メーリングリストが関係する場合、エラーをメッセージ発信者ではなくリスト管理者に向ける方法として、この処置は一般的かつ便利である。)"

Return-Path は「エンベロープ From」アドレスを示す指標ではありますが、必ずしも正しいアドレスが示されているとは限りません。他のメールヘッダ同様、前述のサンプルのように変更することができます。

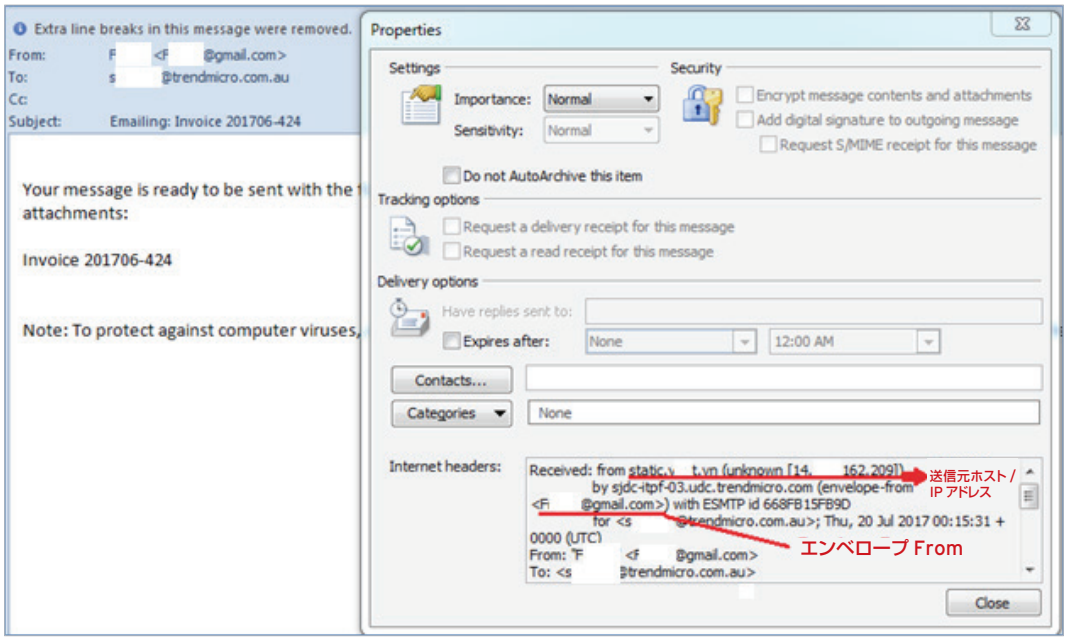
もう一つ注意すべき点として、基本的な SMTP またはメールプロトコルでは、いかなる場合も送信者アドレスの認証が必要になりません。初期の形式では、任意の送信者アドレスを「エンベロープ From」または「メッセージ From」のいずれかのフィールドに指定しておけば、メールサーバまたはプログラムでブロックされない限り送信者アドレスが拒否されることはありませんでした。

攻撃者が悪用したのは、こうしたメールシステムの中核にあるチェック体制の甘さでした。

「エンベロープ From」の偽装

メールの「エンベロープ From」を偽装する場合、多くの攻撃者は、受信者のドメインと同じになるように送信者のメールアドレスを装います。あるいは、世間一般によく知られた信頼のあるドメインや組織を利用することもあります。これには、Yahoo! や Gmail など Web ベースのメールサービスプロバイダや金融機関が使用されます。

内部ドメインや信頼のあるドメインを装うことで、メールが正規の送信元から送信されたかのように見せかけ、受信者を信頼させることができます。これにより攻撃者は、詐欺メールとわかれば通常回避されてしまう操作を受信者に行わせることができるのです。



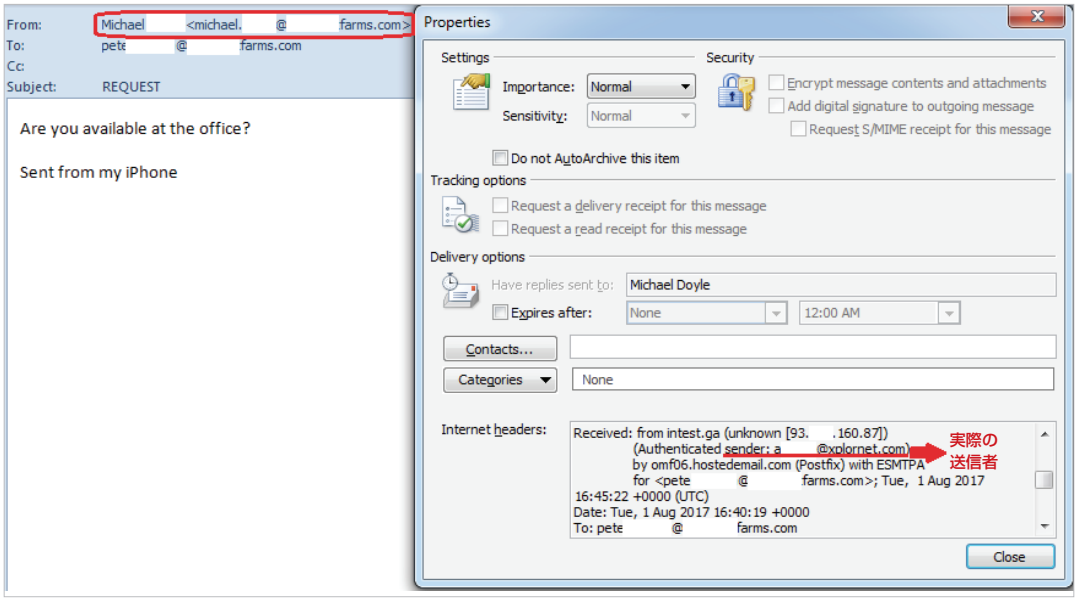
この例では、「エンベロープ From」または「メール From」が gmail.com のメールアドレスとして表示されています。しかし、メール送信元の IP アドレスおよび完全修飾ドメイン名は、明らかに gmail.com ドメインに属するものではありません。

「メッセージ From」の偽装

このケースでは、「エンベロープ From」に正規の送信者ドメインを使用し、「メッセージ From」ヘッダを偽装します。「エンベロープ From」の場合と同様、「メッセージ From」アドレスを偽装して、メールが内部ドメインまたは世間一般によく知られた信頼のある機関から送信されたかのように見せかけます。

専門知識のない一般的なメールユーザは「エンベロープ From」アドレスを確認する方法を知らず、メールアプリケーションの「送信者」アドレスに表示されている情報をそのまま信じてしまう傾向があります。精巧に作り込んだメールコンテンツを組み合わせることで、何も知らない受信者をだまして攻撃者の指示に従わせ、多くの場合、個人情報を盗み出すなどの不正行為を行います。

「エンベロープ From」の送信元ドメインが「メッセージ From」のドメインと一致しない場合でも、メールプロトコルにはそれを拒否する特定のルールやガイドラインがないため、こうしたメールはメールサーバで受け入れられます。

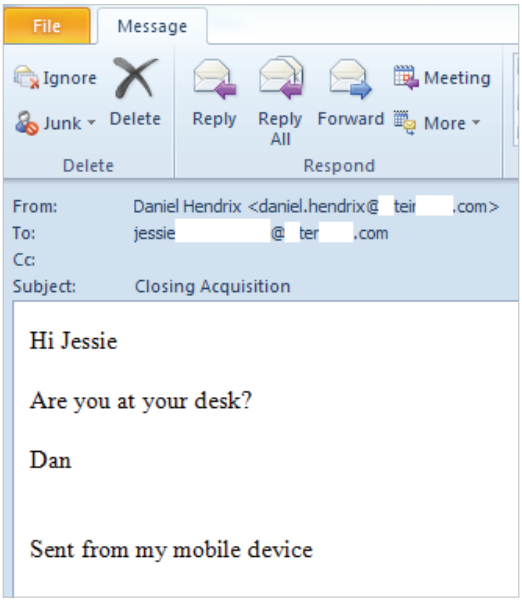


前述のサンプルでは、メールが Michael Doyle という内部ユーザから送信されたかのように「メッセージ From」が偽装されています。しかし実際の送信者は @xplornet.com に属する何者かです。これには受信者をだまそうとする明らかな意図があります。

類似ドメインの悪用

類似ドメインとは、有効な送信先ドメインと同じに見えるよう意図的に作成されたドメイン名のことです。「l（エル）」の代わりに数字の「1」を、「m（エム）」の代わりに「rn（アールエヌ）」を使用するなど、通常、ドメイン名の1つ以上の文字を見分けがつきにくい別の文字に置き換えます。1文字をドメイン名に追加したり、ドメイン名から削除したりすることもあります。注意深く観察しなければアドレスの操作に気づかれることはなく、偽装した正規のドメインからメールが送信されたかのように受信者を欺くことができます。

以下の攻撃の例では、受信者 Jessie のドメイン interface.com によく似たドメインが使用されています。ドメイン名の「e」と「r」の間に「i」の1文字が挿入されています。



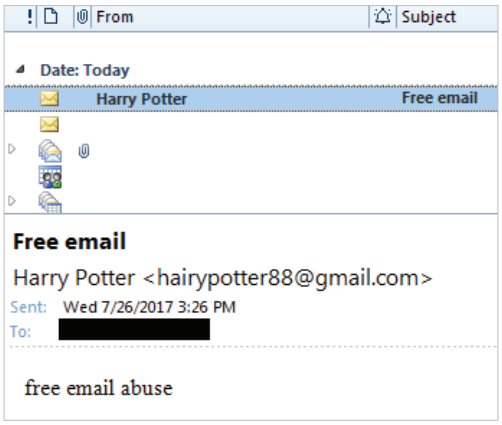
類似ドメインを「エンベロープ From」や「メッセージ From」の偽装手法と組み合わせることもできます。「メッセージ From」アドレスの偽装と組み合わせることで、偽のアドレスはさらに正規のアドレスに見えるようになり、標的がだまされる確率も高くなります。この場合、**Reply-To** ヘッダには類似ドメインが指定されるので、受信者がなりすましメールに返信すると、その応答は攻撃者に送信されることになります。以下に例を示します。

From: Mandy <Mandy@company.com>
To: Kathy@trend.com
Reply-To: Mandy <Mandy@comqany.com>

無料メールアカウントの悪用

この偽装手法には、Yahoo!、Gmail、AOL などの有効な無料メールアカウントが使用されます。メールアカウントの表示名には、社内の正規ユーザ (一般に会社役員) の表示名が使用されますが、そのドメインには無料メールのドメインが設定されています。

正規のメールドメインを使用しているため、メールは SPF (Sender Policy Framework)、DKIM (Domain-Keys Identified Mail)、さらには DMARC (Domain-Based Message Authentication, Reporting, and Conformance) のチェックさえ問題なく通過します。

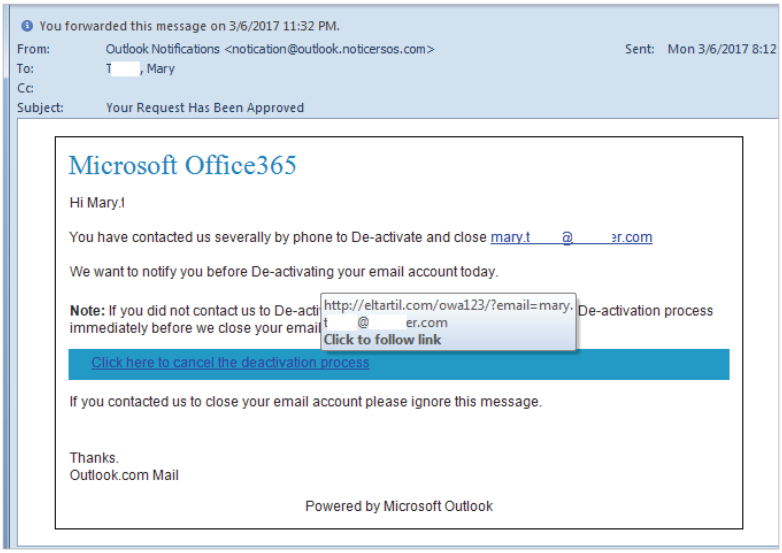


前述の例では、送信者は組織内の「Harry Potter」という人物を装い、メールアドレスに Gmail のドメインを使用しています。その人物を知っているか「Harry Potter」という役員に心当たりのあるユーザは、実際のメールアドレスを気にせずに、疑うことなく偽装された表示名に返信を送ってしまい、攻撃者に侵入の糸口を与えることになります。

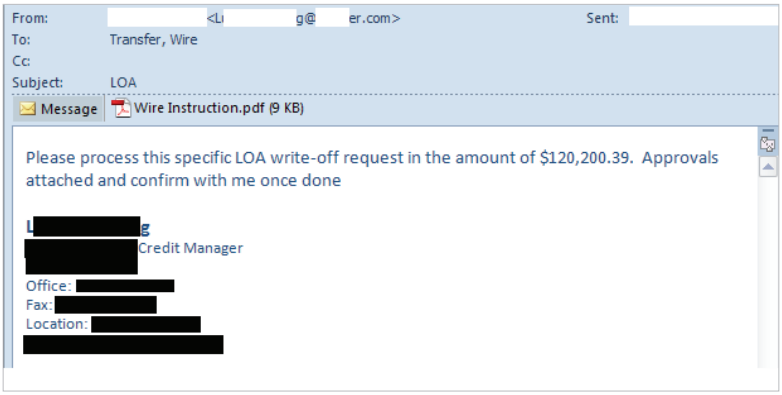
メールアカウントの侵害

メールヘッダを検査しても、この偽装手法を簡単に見破ることはできません。幸運なことに、攻撃者にとっても、この手法の遂行は容易なことではありません。ユーザのアカウントまたはメールボックスを乗っ取り、制御する必要があるためです。

この攻撃は、ユーザにフィッシングメールを送りつけてアカウント情報を入手することから始まります。以下の例では、Outlook の通知を装ったフィッシングメールがアカウントの無効化をキャンセルするようユーザに依頼しています。ただしメール内のリンクには、HTTP を使用した、明らかに Outlook ではない不正な URL が指定されています。このリンクをクリックすると、実際にはユーザのアカウント情報を収集する攻撃者のサイトに転送されます。



フィッシング攻撃に成功した攻撃者は、乗っ取ったアカウントを使用して社内のユーザにフィッシングメールや BEC メールを送りつけます。実際のメールを以下に示します。



メールは正規ユーザのメールボックスから送信されているため、メールヘッダや送信者アドレスに不審な点はありません。さらにメールは社内のメールシステムを経由しているので、従来のスパムメール対策フィルタで検出することはできません。

トレンドマイクロのソリューション

29 年にわたるセキュリティ業界での実績とメールセキュリティに関連した特許の取得により、トレンドマイクロは、ユーザを未知の脅威から保護するセキュリティソリューションのリーダー企業としてその存在を確立してきました。従来の環境およびホスト環境全体で 160 億件を超える Web サイト、メール送信元、およびファイルを日々検索することにより、スパムメールをはじめとしたメールの脅威からユーザを保護するセキュリティ機能を継続的に強化しています。

Office 365 または Exchange Online のユーザは、トレンドマイクロのメールセキュリティ製品である HES および CAS を利用できます。HES はメールゲートウェイとして機能し、インターネットを経由して侵入する脅威や攻撃からユーザを守ります。CAS は API 統合によってメールボックス階層で動作し、Exchange Online、SharePoint Online、および OneDrive for Business 向けの高度な脅威対策機能と情報漏えい対策機能で Office 365 のセキュリティを強化します。HES と CAS のサンドボックス技術を使用すれば、不審なファイルやメール添付ファイルを詳細な挙動分析とシミュレーションによって分析することができます。これら 2 つの製品が連携することで、多階層にわたる防御が可能となり、社外からの攻撃だけでなく社内からの情報漏えいも最大限に防御できるようになります。

以降の各項では、BEC 対策技術の概要について説明した後、このホワイトペーパーに記載した偽装手法それぞれに対処するよう HES と CAS を設定する方法について詳しく見ていきます。

人工知能 (AI) ベースの BEC 対策技術

2017 年 8 月のリリースにおいて、HES と CAS の両製品が刷新され、業界標準の送信者認証プロトコルとトレンドマイクロの高度な BEC 検出手法を統合した新たな BEC 対策技術が導入されました。

この新しい BEC 対策技術には、偽装されたメールをより正確に識別するための、エキスパートルールシステムと機械学習という 2 種類の人工知能が使用されています。エキスパートルールシステムは、セキュリティ専門家の意思決定能力を模倣して、偽装の可能性を示す特徴を推論します。この推論は、送信者情報や送信経路などの攻撃の特徴と、操作の要求、金銭請求の含み、あるいは切迫感の演出といったメールの意図の特徴の両面で行われます。さらに「高プロファイルユーザ」機能が精密な調査を行い、偽装された送信者 (多くは会社役員) と、標的となる組織内の実際のメールアドレスを関連付けます。

一方の機械学習モデルは、各特徴の重み付けを決定し、それを何百万もの安全または不正なメールと比較して BEC 攻撃かどうかを正確に識別します。機械学習モデルは自ら学習を行い、継続的に結果の精度を向上させていきます。

トレンドマイクロのスパムメール検索エンジンには、この高度な BEC 対策技術が使用されています。それでは、このホワイトペーパーに記載した偽装手法からユーザを保護する方法について詳しく見ていきましょう。

「エンベロープ From」の偽装からの保護

「エンベロープ From」の偽装攻撃は、社内 (受信者と同じドメイン) の送信者、世間一般によく知られたサービスプロバイダやインターネットドメイン、あるいは偽装だと明確には判断できない送信元からメールが送信されたかのように SMTP メールの From アドレスを装います。この攻撃に対処すべく開発されたのが、SPF (Sender Policy Framework) や DKIM (DomainKeys Identified Mail) のような SMTP 認証技術またはメール検証技術です。これらの技術は世界中の多くの組織で導入されています。

SPF では、インターネットにメールを送信することができる IP アドレスを組織が管理します。これにより、そのドメインを偽ったメールの受信を組織側で拒否できるようになります。

一方 DKIM では、送信側がメールに電子署名を施し、受信側のメールサーバが電子署名を照合して、メールが指定したメールアドレスから送信されているかどうかを確認します。この技術でも、「エンベロープ From」の偽装されたメールアドレスを回避することができます。

HES には、SPF と DKIM の両方の技術が採用されており、「エンベロープ From」の偽装攻撃への対応をより高い精度で行うことができます。HES では、未知または解決不能なドメインから送信されたメールも拒否されます。登録が公開されておらず MX レコードのないドメインは受け入れられません。

HES には、メール認証の最新技術である DMARC（Domain-based Message Authentication, Reporting & Conformance）も導入されています。

「メッセージ From」の偽装からの保護

「メッセージ From」の偽装攻撃は、受信者に表示される「送信者」のメールアドレスを、社内または信頼される人物のアドレスと同じになるように装います。今ではこれが **BEC** 攻撃で広く利用されている手口です。

HES には、この種の攻撃に対応する独自の **BEC 検索条件**があります。BEC 対策技術で提供される機械学習やエキスパートルールをベースとした検出手法に加え、この新しい機能を使用すれば、管理者は、標的となる組織の役員など高プロファイルユーザを識別した上で、さらに HES の詐欺メール確認条件を適用して偽装メッセージを特定できるようになります。これにより、この種の攻撃に対処するより堅牢なセキュリティ保護が実現されます。

CAS でこの攻撃に対応するには、BEC 対策技術を含む**高度なスパムメール対策**を使用します。

類似ドメインの悪用からの保護

「類似ドメインの悪用が成功する確率は、「メッセージ From」の偽装攻撃と組み合わせなければそれほど高いものではありません。偽装攻撃を組み合わせたとしても、今度は HES の BEC 対策技術によって検出されるので、この攻撃が成功する確率はかなり低くなります。

さらにフロントエンドには、HES が使用するトレンドマイクロのスパムメール検索エンジンが配置され、感染報告のあるスパムメールを 96.83%* を超える確率でフィルタします。頻繁に更新されるスパムメール対策のヒューリスティックルールを組み合わせることで、ほとんどの類似ドメイン攻撃はこのスパムメール検索エンジンで検出されます。

HES の **IP レピュテーション**機能も潜在的な類似ドメイン攻撃の検出およびブロックに役立ちます。Trend Micro Email Reputation Services のスタンダード IP レピュテーションデータベースと (リアルタイムで更新される) 高度なダイナミック IP レピュテーションデータベースを使用して、新しいスパムメールや未知の脅威の送信元に迅速に対応し、それらを接続の段階でブロックします。

送信先ドメインによく似た存在しないドメインを使用して攻撃が行われた場合は、HES がブロックします。パブリック DNS レコードがないドメインから送信されるメールは、すべて HES で拒否されます。

CAS でこの攻撃を阻止するには、**高度なスパムメール対策**を「**高プロファイルユーザ**」を設定して使用します。

* 出典 : Opus One, Comparative Performance of Anti-Spam Gateways
* テスト実施時期 : 2014 年 7 月に行われたスパムメールテスト結果
* テスト対象製品 : InterScan Messaging Security Virtual Appliance ™ 8.2
（Trend Micro Hosted Email Security は、InterScan Messaging Security Virtual Appliance と同じエンジンを使用しています）
* 記載の内容は、2014 年 7 月時点の情報をもとに作成したものです。

無料メールアカウントの悪用からの保護

無料メールアカウントの悪用は、なりすまし攻撃や BEC 攻撃で行われることがあります。攻撃者は、偽装する送信者の名前を無料メールアカウントの表示名に設定することで、社内ユーザ (一般に会社役員) を装います。無料メールアカウントを使用することを除き、この手法は「メッセージ From」の偽装攻撃によく似ています。

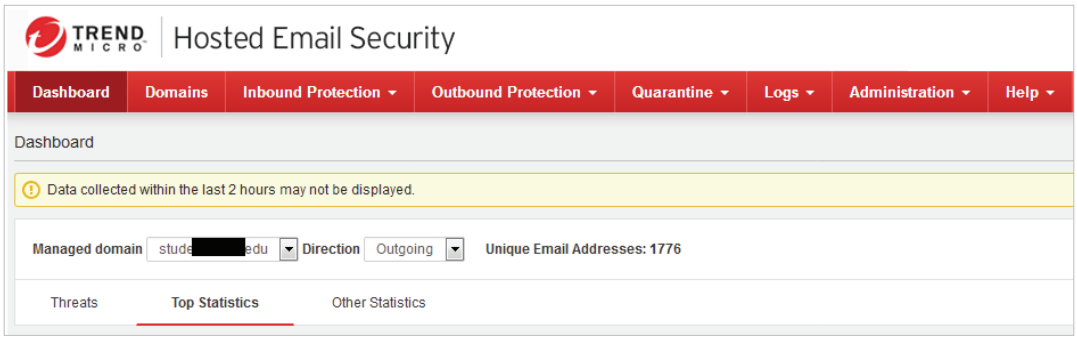
そのため HES では、この種の攻撃も機械学習の **BEC 検出機能**で検出およびブロックすることができます。高プロファイルユーザの名前をリストすることによって、それらのユーザから送信されたメールをより積極的に検索できます。

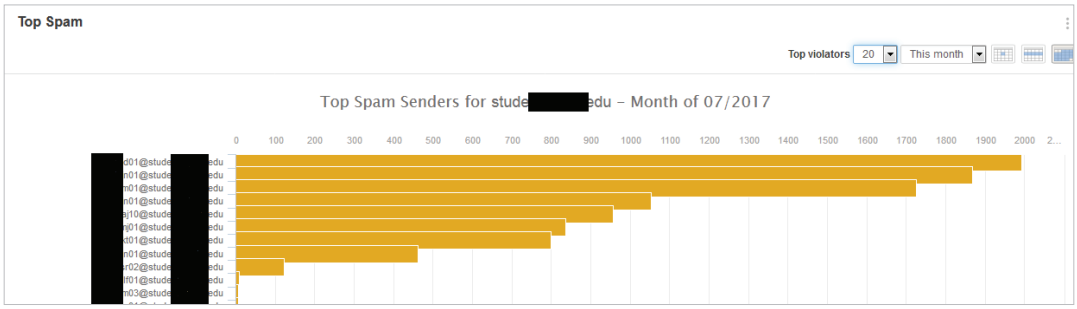
同様に、CAS でも、**高度なスパムメール対策**を**高プロファイルユーザ**機能とともに使用することで無料メールアカウントの悪用を阻止できます。この場合は、高度なスパムメール対策を有効にするメッセージ範囲に「**すべてのメッセージ**」を、検出レベルに「**中**」または「**高**」を選択することをお勧めします。

メールアカウントの侵害からの保護

メールアカウントの侵害攻撃は 2 つの異なる方向から行われ、1 つは社内アカウントを、もう 1 つは外部アカウントを乗っ取ることで実行されます。

社内アカウントが乗っ取られると、そのアカウントを使用してインターネット上の膨大な標的にスパムメールやフィッシングメールが送信されます。HES の**送信メール検索機能**を使用すれば、このようなスパムメールの送信を検出してログに記録できます。**ダッシュボードの [スパムメール送受信者 (上位)] の表**を利用することで、メールに関連したユーザの動作に基づく潜在的な侵害を管理者に警告できます。以下に例を示します。





外部からの攻撃については、HES のスパムメール対策フィルタでヒューリスティック検索を使用し、さらに Trend Micro Smart Protection Network を統合することで、ブロックすることができます。スパムメールやフィッシングメールに含まれる不正な URL については、**Web レピュテーション**検索の**Time-of-Click プロテクション機能**が有効です。

CAS では、社内アカウントから送信される BEC 攻撃を検出できます。メールアカウントの侵害攻撃を阻止するには、「**高度なスパムメール対策**」、「**高プロファイルユーザ**」、および「**全てのメッセージに対する検索**」を有効にすることをお勧めします。

参照情報

Trend Micro Hosted Email Security™

なりすましメールをゲートウェイレベルでブロックするには、次の設定を有効にすることを強くお勧めします。

- **受信および送信ポリシー**の両方でスパムメールおよびフィッシングメールのポリシーを有効にして、スパムメール、BEC、フィッシングメール、Web レピュテーション、およびソーシャルエンジニアリングの攻撃を検索するように設定します。ポリシーは個別に作成することもできます。
- **Web レピュテーション**で **Time-of-Click プロテクション**を有効にして、[トレンドマイクロでテストされていない URL に適用] オプションをオンにします (推奨)。
- **ソーシャルエンジニアリング**フィルタの仮想アナライザオプションを有効にします。
- BEC フィルタ用に**高プロファイルユーザ**を特定し、そのメール表示名を高プロファイルユーザのリストに追加します。
- HES の **IP レピュテーション**を有効にします。
- SPF (Sender Policy Framework) を有効にして、**適切な SPF レコードを DNS で公開します**。
- HES の **DKIM 検証**および **DKIM 署名**を有効にします。

HES には情報漏えい対策機能も導入されています。情報漏えい対策により、なりすましメール攻撃がアカウント侵害または無防備なユーザを利用して組織外に送信する機密情報を検出できます。

Trend Micro Cloud App Security™

Exchange Online のメールボックスレベルでなりすましメールをブロックするには、次の設定を有効にする必要があります。

- **高度な脅威対策**の設定で**高度なスパムメール対策**を有効にして、BEC、ランサムウェア、高度なフィッシング、および他の頻繁に見られる攻撃から Exchange Online ユーザを保護します。この対策を有効にするメッセージ範囲には [**すべてのメッセージ**] を選択します。
- すべての**内部ドメイン**を定義して、内部から送信されたメールメッセージと偽装されたメールメッセージを識別します。
- **高プロファイルユーザ**を特定し、より厳密な方法で BEC 攻撃を検出します。
- リアルタイムの **Web レピュテーション**を有効にして、メールに含まれる URL の信頼性を確認します。これは [**すべてのメッセージ**] に適用するように設定します。
- **情報漏えい対策**機能を使用して、なりすましメール攻撃により機密情報が漏えいしないよう阻止します。

TREND MICRO™
Securing Your Journey to the Cloud

1988 年の創業以来、トレンドマイクロは、個人およびあらゆる規模の組織に受賞歴のあるセキュリティソフトウェア、ハードウェア、およびサービスを提供してきました。本社を日本の東京に置き、30 か国以上に拠点を持つトレンドマイクロのソリューションは、付加価値再販業者やサービスプロバイダを介して世界中で販売されています。トレンドマイクロの製品やサービスの詳細、および体験版のダウンロードについては、弊社の Web サイト www.trendmicro.com を参照してください。

TREND MICRO INC.
フリーダイヤル（米国内）: +1 800.228.5651
電話 : +1 408.257.1500
FAX: +1 408.257.2003