Cofense Intelligence™

人が吟味した、phishing 固有の脅威インテリジェンス。

Cofense Research によると、2016年に発生したすべての phishing メールの97%以上がランサムウェアだったことが判明しました。非常に警戒を抱かせる数字です。企業がこの統計に含まれないようにするにはどうすればいいでしょうか？ Cofense Intelligence は、正確でタイムリーな警告を発して、進行中の phishing 攻撃を組織が迅速に特定し対応する能力を強化します。

ソリューション

Cofense Intelligence は、危険なマルウェアや phishing 攻撃を企業が阻止するのを支援するために設計された、先進的なサイバー・セキュリティ・サービスです。当社は独自の手法を使用して、企業への最大の脅威を自動的に特定する専有の方法を使用し、逐次実行可能なインテリジェンス、ツール、およびコーチングを提供して、従来検出されないような攻撃にも対応します。

電子メール攻撃は、直接的または間接的にマルウェアを企業に展開するための主要なメカニズムです。悪意のある添付ファイルやリンクを含んだ phishing メールは、引き続き大多数の組織のセキュリティ層をすり抜けて、エンドユーザーにまで達することが可能なままです。

ほとんどのセキュリティベンダーが脅威を分析して悪意があると宣言するのは、脅威があなたの目の前に迫ってきてからです。通常、顧客の一定数が不審ファイルを報告するまで、あるいはエンドポイントシステムが情報をベンダーに返すまで待つことになります。したがって、攻撃の開始時点から、企業がそれについて最終的に信頼できる情報を取得するまでの間に遅延が生じます。それぞれの脅威は個別に調査されるため、すべての脅威は、攻撃またはそれに関連する攻撃についての前後関係なしに、対等に報告されます。

この方式の結果として、セキュリティ専門家は、攻撃を中断させたり脅威への対応に優先順位を付けるだけの脅威インテリジェンスを持ちません。

Cofense は、会社のネットワークが攻撃を受ける前に、日々出現する脅威を特定するため、根本的に異なるアプローチを採用しています。

当社は広範囲な情報源から毎日100万件以上のメッセージを受信します。攻撃を自動的に解読し、その間にある関係を判断します。当社独自開発のクラスタリング・アルゴリズムは、さまざまな要因に基づいて悪意のある電子メールを分類し、危険なリンクや添付ファイルを含む電子メールの形で新たに出現する脅威を監視します。新たな脅威クラスタが特定されると、その特性は当社の脅威リポジトリに記録され、更新されます。

確認された各 phishing キャンペーンのペイロードが独自方式を使用して分析され、各脅威の性質を判断します。この情報はその後、キャンペーンや時間枠を超えた追加分析のために当社に蓄積されたデータに更新されます。この分析から得られた脅威インテリジェンスは、セキュリティチームとセキュリティ・インフラストラクチャが十分に認識され適切に対応するために、複数の形式で公開されます。

先を見越した積極的な脅威分析アプローチにより、既存のセキュリティ・インフラストラクチャを利用して、これらの潜在的に悪意のある攻撃を中断させることができます。ネットワークに侵入するために使用された攻撃の手口も、phishing キャンペーンと脆弱性指標（Indicators of Compromise=IOC）との関係と共に露呈されます。実行可能な脅威インテリジェンスと共に、phishing 攻撃およびその動機付けとの相関関係を理解することは、チームの優先順位付け、調査、対応に役立ちます。

主な利点

- ✓ タイムリーで正確、すぐに実行可能な Phishing 脅威インテリジェンス
- ✓ 使用可能な Phishing 脅威インテリジェンス
- ✓ 脅威インテリジェンスの運用とガイダンスの提供に役立つ専門的脅威アナリスト
- ✓ 情報に基づく迅速な意思決定を支援する攻撃分析と関連情報

Cofense　独自のセキュリティ・インテリジェンスは、日々企業を襲う脅威を特定し、阻止し、調査するために必要な武器を提供します。この正確な情報は、会社チームがネットワークへの積極的攻撃に対して準備し対応するために、複数の形式で利用できます。

- **人が読める脅威インテリジェンス・レポートは、最大の脅威に対するディープダイブ分析およびトレンド分析を提供します。このレポートには、当社専門家による攻撃手口の分析が含まれています。**
- **機械可読型脅威インテリジェンス（MRTI）は、セキュリティデバイスや脅威リポジトリに直接供給できます。ファイアウォール、IDS/IPS、SIEM は、新たに発生した脅威を攻撃の最も初期段階で検出しブロックすることができます。**
- **phishing およびマルウェア攻撃を調査するための SaaS 調査アプリケーション。これらのオンデマンド・ツールは、どの攻撃が関連しているか、どのように攻撃されているかについて最新の見解を提供します。**
- **企業チームがベストプラクティスを導入してネットワークに対する脅威を軽減するのに役立つ、Cofense の世界一級セキュリティチームによる専門的指導**

> 私達は PhishMe レポートをまず最初に処理します。なぜなら、Cofense が報告しているなら、それは対処しないと被害が発生することを知っているからです。Cofense Intelligenceは、私達が受信する最も正確な phishing 脅威情報であり、簡単に使用できます。
>
> **大手金融機関の脅威アナリスト**

Cofense Intelligence サービスがすぐに実施可能である理由：

使える	Cofense Intelligence は、脅威インテリジェンスを複数の形態で提供します。機械可読脅威インテリジェンス（MRTI）は、既存セキュリティデバイスとの迅速な統合のための業界標準に準拠しています。PDFおよびHTML形式の分析レポートは、脅威アナリストやインシデント対応チーム向けに最適化されています。
信頼できる	Cofense　Intelligenceは、当社の熟練したアナリストが審査した確認済みの脅威についてのみお客様に通知し、信頼性の高いインテリジェンスをもたらします。
タイムリー	新たな攻撃が確認されると、MRTIはその都度発行されます。戦略的分析報告は毎週発表されます。調査アプリは24時間365日利用可能です。
フレッシュ	Cofense Intelligence サービスは、毎日危険なペイロードを従業員に配信するために使用される悪意のあるさまざまな電子メールやスパムのソースから、脅威インテリジェンスを抽出します。
文脈的	Cofense　Intelligenceは、攻撃の個々の要素がどのように関連しているかを示す、また、一見異種と見られる攻撃間の関係を示す脅威インテリジェンスを公開します。
使いやすい	当社は、サービスの運用を支援し、サービスが最大限に活用されていることを確実にするため継続的なサポートを提供いたします。

Cofense(旧PhishMe)は、人間主導型のフィッシング防御ソリューションを全世界的に提供する大手プロバイダーです。私たちは、能動的な電子メールの脅威に対する組織を挙げた取り組みを可能にすることで、サイバーセキュリティに対する協調して対応するアプローチを提供します。

当社の集合的防御スイートは、最上級のインシデント対応技術を、従業員からもたらされたタイムリーな攻撃情報と組み合わせます。Cofenseのソリューションは、スピアフィッシング、ランサムウェア、マルウェア、および業務電子メール漏洩の影響を素早く軽減します。今やこれは、国際的組織、企業にとってすべて現実となっています。　より詳しくは、www.cofense.comをご覧ください。

COFENSE

W: cofense.com/contact **T:** 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175