

# リアルタイムのURL／マルウェア防御

今日の巧妙化する高度な攻撃を検知・防御 – 94%のマルウェアはメールによって持ち込まれている



94% of malware is delivered by email



本物そっくりの偽装されたフェイクログイン攻撃や認証情報を刈り取るクレデンシャルハーベスティング攻撃は、ますます巧妙になってきています。無防備なユーザーに対して定期的に攻撃を仕掛けてくるようになってきています。これまでのメールセキュリティテクノロジーでは、このような高度な攻撃に立ち向かうことは困難になってきています。

## SEGをすり抜けるメール脅威を検知

シグネチャベースの脅威はもう過去のもので、サイバー攻撃者は日々進化し、シグネチャベース検出を回避する複合型のポリモーフィック攻撃に移行しています。ポリモーフィック型亜種は動的に変態します。シグネチャベースの従来型ソリューションでは、ポリモーフィック型亜種から起こりうるすべての攻撃を特定することが不可能です。IRONSCALESのサービスは、メールボックスレベルで脅威を防御しています。サンドボックスや複数のウイルス対策エンジンによるスキャン、IRONSCALESのユーザーコミュニティが提供する独自のリアルタイム脅威インテリジェンスを組み合わせ、メールボックスレベルでの防御を実現しています。

警告バナー表示と直感的な自己管理は素晴らしい。これは、IRONSCALESが弊社を水際で防衛してくれている証しです。そして、弊社のメールセキュリティがセキュアであることを実証してくれます。

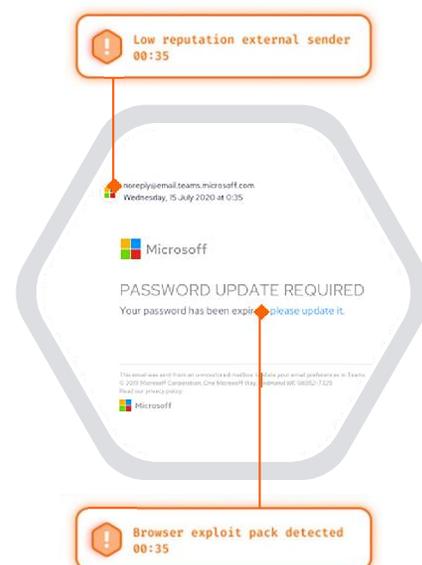
OrthoCarolina社テクノロジーサービス統括バイスプレジデント  
Neil Stein氏

## 課題

サイバー攻撃が大量化・巧妙化し続ける中、メールセキュリティは今、企業にとって最大の課題となっています。今日に巧妙化する脅威は、セキュアメールゲートウェイ(SEG)といった従来のテクノロジーソリューションを巧みにすり抜けるように作られています。今、サイバー攻撃者は進化し続けています。不正なリンクと偽のログインページを巧妙に組み合わせ、被害者を誘い込み、ユーザー認証情報やその他の個人情報を探取してしまうのです。

## ソリューション

1日に何千通ものメールを読み解き、新たな異常を発見することは、人の力だけでは不可能な仕事です。しかし、コンピューターなら可能です。今日の高度な脅威に対抗するには、メールセキュリティに新しいアプローチが必要なのです。IRONSCALESのメールボックスレベルでの防御。ここには、最新のAI/マシンラーニングのテクノロジーが活かされています。そして、サンドボックスや複数のウイルス対策エンジンによるスキャンに加えて、IRONSCALESのユーザーコミュニティが提供する独自のリアルタイム脅威インテリジェンスによって、瞬時にその脅威を分析します。



## 高度なURL攻撃を防御

IRONSCALESは、高度なディープラーニングアルゴリズム、ニューラルネットワーク、コンピュータービジョンなどの最新のAIテクノロジーソリューションを活用し、レイアウト、画像、ロゴなどの視覚的な乱れや逸脱をリアルタイムに検出し、ログインページが本物であるかどうかを判断します。

### IRONSCALESのURL／マルウェア防御テクノロジーの認証情報盗難／フィッシングマルウェア防御法

- 社内外の送信者のリアルタイムなIDプロファイリングとスコアリング
- コミュニケーションパターンの継続的な監視によって、未然に異常の発生を検出
- コンピュータービジョンとディープラーニングで偽ログインページをリアルタイムにブロック

## 協調型のマルウェア防御

IRONSCALESでは、複数のウイルス対策ソフト／サンドボックスを簡単に統合するためのアウトオブボックス型のオプションを提供しています。このインテグレーション機能によって、これまで活用してきた既存のマルウェア防御機能を組み込んだり、新しいエンジンと入れ替えたりすることが容易に可能です。

## プロアクティブなランサムウェア防御

ランサムウェアの攻撃は、防御をすり抜けるために常に変化しています。攻撃者は、攻撃の踏み台となるリンクを、即時ではなく、意図的に遅らせて実行したり、ネットワーク内に潜伏・待機させたりして、攻撃の機を窺うこともあります。そのため、メールボックスを継続的に監視することが、防御への唯一の対策となります。IRONSCALESは、行動分析と不審リンクや添付ファイルの継続的な自動検知を組み合わせることで、プロアクティブに攻撃を予測・防御します。

## なぜIRONSCALESなのか？

- 1 まず、第一に、IRONSCALESが選択されるのは、導入の早さと運用の容易さです。そして、BECやアカウント乗っ取りなどの高度な攻撃など、あらゆる種類のメール脅威を阻止する能力において、他に類を見ないサービスを提供していることです。
- 2 IRONSCALESは、メールボックスレベルで、攻撃のターゲットとなる可能性が最も高い部署から導入といったスモールスタートが可能。
- 3 また、IRONSCALESが「メールセキュリティ」と「ユーザーアウェアネス」を組み合わせた包括的なメールセキュリティプラットフォームであることも、IRONSCALESが選択される理由の1つです。

“1年半前にIRONSCALESを導入して以来、弊社のメールセキュリティシステムを通過するフィッシングメールの量は99%減少しました。

Apparo社テクノロジーエンゲージメント部門ディレクターStephanie McKee氏



IRONSCALESをさらに知りたい方は、[www.ironcales.jp](http://www.ironcales.jp)をアクセスしてください。

あらゆるタイプのフィッシング攻撃の予見、検知・防御から隔離・削除までの迅速かつシンプルなソリューションを今すぐ手に入れることができます。



Copyright 2022



販売代理店