Abnormal
Customer Case Study

人手だけではメール攻撃はもう防げない
ユーザベースが選んだ自律型AIという答え

人の判断やルール設定では追いつかなくなったメール攻撃。ユーザベースは、行動分析に基づく自律型AIで、検知から対処までを自動化した。

UZABASE

株式会社ユーザベース

本社：東京都千代田区丸の内2-5-2

業種：情報・通信業、メディア

事業概要：企業活動の意思決定を支える
ビジネス情報インフラの提供

保護対象メールボックス：2000

経済情報プラットフォームを運営するユーザベースでは、メールセキュリティのさらなる強化を図るべくAbnormal AIを導入。正規ドメイン／サービスの利用や実在の人物へのなりすましといった悪質な攻撃を高精度に検知できる環境を整備すると同時に、メールセキュリティにまつわる運用負担も大幅に軽減している。

攻撃の起点となるメールの安全をどう守るか

経済情報プラットフォーム「Speeda」やソーシャル経済メディア「NewsPicks」の運営会社であるユーザベース。同社では、情報セキュリティ対策の一環としてメールセキュリティの強化に取り組んでいる。同社でCIO／CISOを務める王 佳一氏は「昨今のランサムウェア被害において、フィッシングメールを起点とした初期侵入はまだまだ主要な侵入経路の一つです。」と話す。

これまで同社では、Google Workspaceの迷惑メールフィルタを一次防御に用いてきた。しかし最近は、これをすり抜ける標的型攻撃メールも増加し、対応負荷が拡大していたという。「たとえば、ユーザーがうっかり不正なリンクをクリックしてしまうと、その後の調査やパスワードリセットなどの対応をすべて人手で行わなくてはなりません。そういった対応に加えて、当社のセキュリティチームでも国内の多くの企業と同様に、アンコントローラブルな外部からのフィッシングメール攻撃キャンペーンの対応に追われてきました」と同社の当真 彰吾氏は話す。

高精度×低運用負荷が採用の決め手に

このような課題を解消すべく、同社では新たなメールセキュリティソリューションの導入に着手。その要件としては、まず検知精度の高さが挙げられる。いくら多くの脅威を検知できても、過検知・誤検知が多ければ実運用に耐えない。新ソリューションには、高精度な脅威検知能力が求められた。

課題

・Google Workspaceの迷惑メールフィルタ（フィッシング・不正なソフトウェア対策含む）をすり抜ける標的型攻撃メールが急激に増加

・標的型攻撃メールの内容が巧妙化しユーザーが見抜くことが困難になっている

・不審なメールの確認やユーザーの問い合わせ対応が担当者の負担となっている

・フィッシングメールによるランサムウェア等の深刻な被害を引き起こす可能性を危惧

効果

・Google Workspaceの迷惑メールフィルタをすり抜けた、標的型攻撃メールを月間約3,000件ブロック

・高精度な検知と自動修復機能によりユーザーへの攻撃メール到達とメール開封を大幅に削減

・ルールレス＆AIによる自動運用で担当者の不審メール対応工数が激減

・SIEMとの連携などさらなるセキュリティ対策強化も視野に

攻撃の主要な起点となるメールセキュリティは、企業にとって最優先で守るべきポイントです。Abnormal AIによる高精度な検知と自動修復機能を活用することで、セキュリティ担当者の運用管理負担を軽減しつつ、標的型攻撃メールなどの脅威からビジネスの安心・安全を守れるようになりました。

株式会社ユーザベース　上席執行役員　CIO/CISO
王　佳一氏

もう一つのポイントが、運用負荷を最小限に抑えられるという点だ。ルールやシグネチャのカスタマイズに手間が掛かるようだと、それ自体が大きな負荷を生んでしまう。さらに最後のポイントが、検知後の隔離・修復作業を自動化できることである。従来は人手と時間を費やしていただけに、これを自動化できることも必須条件だった。

そして、これらを満たせるソリューションとして選ばれたのがAbnormal AIである。「Abnormal AIは、AIによる行動解析で不審なメールをチェックしますので、正規のドメイン／サービスを用いた攻撃やなりすましも高精度に検知できます。事前に行ったPoCでは、複数ツールの中でも、過検知・誤検知の少なさも際立っていました。また、AIが自律的に学習・判断を行うため、ルール設定や例外登録などの作業を人が行う必要もありません。自動修復についても問題なく行えることが確認できました」と当真氏は話す。

これに加えて、API型のソリューションであったことも採用を大きく後押しした。「ゲートウェイ型のソリューションだと、既存のメール環境を改修しなくてはなりません。その点、Abnormal AIは、既存のGoogle Workspace環境へシームレスに統合できるため、導入が容易な点も良かったですね」(当真氏)。

人手での対応を大幅に削減することに成功

Abnormal AIを導入したことで、同社の環境にも大きな改善効果が生まれている。まず、Google Workspaceの迷惑メールフィルタをすり抜けていた攻撃メールを、月平均約3,000件追加でブロック。また約4カ月間で、約30,000件の攻撃メールやフィッシングメールなどを検知し、ユーザーに届いてしまったメールもほぼユーザーが開封する前に自動修復したという。

「メール受信後、AIが脅威を判定し、隔離・削除などの対処を完了するまでの時間は、メールが届いてからユーザーが内容を確認し、開封・クリックに至るまでの時間を大きく下回ります。実質的に、ユーザーの目に触れる前に攻撃の芽を摘み取っているため、脅威が顕在化することはありません」と当真氏は話す。

加えて見逃せないのが、こうした攻撃メールへの対応作業を、ほぼ人手をかけずに済むようになった点だ。検知も修復もすべてAbnormal AIが自動対応するため、担当者もより付加価値の高い業務に専念できるようになった。

「メールに関する問い合わせはヘルプデスクでも対応していますが、Abnormal AI導入後は問い合わせ件数が大幅に減少しました。元々、ヘルプデスクのメンバーは全員がセキュリティに詳しいわけではありません。従来は人による対応の差異も生じがちでしたが、こうした属人性の課題も解消できました」と王氏。リスクをデータで可視化できるようになったことも、非常に大きなメリットだという。

SIEMとの連携などさらなる対策強化も視野に

このように大きな成果を上げた今回の取り組みだが、同社では今後もさらなるセキュリティ強化を進めていく考えだ。「たとえばその一つが、SIEMとの連携です。SIEMの相関分析情報とAbnormal AIのデータを突き合わせることで、脅威の挙動をより詳細に把握できるようにしていきたい」と当真氏は話す。

続けて王氏も「メールセキュリティは最優先の課題です。とはいえ社員が集中すべきは、あくまでもビジネスの本業です。その点、Abnormal AIは、人が意識することなく安全を保つことができる。これが一番の良さですね」と語る。躍進する同社のビジネスの根幹を、今後もAbnormal AIがセキュリティで守り続けていくことになるだろう。

株式会社ユーザベース
上席執行役員　CIO/CISO
王　佳一氏

株式会社ユーザベース
IT本部 Security Division
リードエンジニア
当真　彰吾氏

導入ソリューション

- Inbound Email Security
- AI Security Mailbox
- AI Phishing Coach

abnormal.ai ›

Abnormal