Quad Miners

概要

業界

- 金融

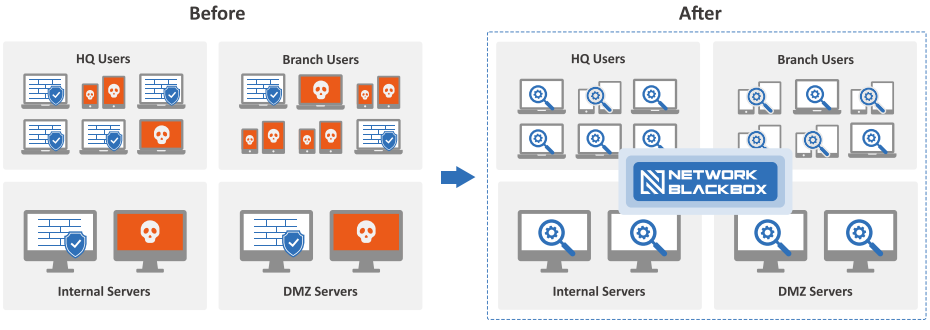
課題

- 悪性コードとランサムウェアに対応するためのセキュリティであるEPP/EDRの導入が必要
- エージェントがインストールされていない多くのデバイス、IOT、サーバで悪性コード感染の可能性
- 境界型セキュリティへの過集中

導入効果

- 死角のない悪性コード対応システムを構築
- ファイルハッシュとオリジンファイルの動的分析による全トラフィックの検査
- マルチAPTソリューション統合による悪性コードの分析と対応の体系化

悪意のあるコードを防止するため、ネットワークトラフィック調査システムを確立しています。 銀行のサーバは包括的に問題を抱えています。



今日のデジタル時代において、ランサムウェアは企業にとって非常に身近な脅威です。銀行のような金融機関にとっては、攻撃されてしまった場合、財務上の大きな損失が発生するだけでなく、その信用や顧客の信頼を損なう可能性があるため、特にリスクの高い脅威となります。
セキュリティベンダーのQuad Minersは最近、メガバンクと協力してランサムウェア攻撃に対処するための革新的なソリューションを実装しました。検疫システムを統合し、本社と支店のランサムウェアに対する穴を取り除くことにより、この増大する脅威に対する包括的なセキュリティを銀行に提供することができました。
このケーススタディでは、Quad Minersと銀行がどのように協力してこのソリューションを実装したのか、また達成した成果について説明します。

背景

主要な金融機関であるメガバンクは複数の場所とデータセンターにまたがる大規模なネットワークインフラを持っています。本社、支店、オフィス、データセンター、およびカスタマーサービスのネットワーク間で発生する多数のトランザクションにより、ネットワーク環境が複雑化しています。国立銀行のネットワークインフラは、顧客に対して信頼性が高く効率的なサービスの提供が必要不可欠です。
ネットワークインフラのセキュリティとして完全性を確保するため、韓国国内No.1のA銀行はQuad　Minersと提携しNDRソリューションを導入しました。NDRソリューションは高度な脅威検出および対応機能を提供するため、潜在的なセキュリティ脅威を事前に特定し、その脅威が被害をもたらす前に対応することができます。
A銀行はマルウェア感染やランサムウェア攻撃など、サイバー攻撃の脅威に絶えず直面しており、その攻撃は財政への莫大な被害や評価の失墜をもたらす恐れがあります。
これまでA銀行は、インターネット網を保護するために境界型セキュリティソリューションに依存してきましたが、常に進化する脅威においてこれらのソリューションでは不十分でした。

A銀行のネットワークインフラの複雑さを考慮すると、NDRソリューションはすべての場所とデータセンターのネットワークトラフィックの監視および分析が必要になります。そのためには、ネットワーク全体のさまざまなポイントにセンサーとプローブを配置し、トラフィックをリアルタイムでキャプチャおよび分析しなければいけません。

課題

A銀行が直面した主な課題の1つは、悪性コードとランサムウェア攻撃に対応するため、EPP/EDRセキュリティシステムを導入することでした。ランサムウェア攻撃は、フィッシング電子メール、ドライブバイダウンロード、ウォーターホール攻撃など、さまざまな形で発生する可能性があり、検出と防止が困難です。効果的なEPP/EDRシステムが導入されていないA銀行は、この種類の攻撃に対して脆弱でした。
また別の課題としてセキュリティの問題がありました。IoTデバイスやサーバなど、多くのデバイスにエージェントがインストールされていないため、悪性コードの感染リスクが高い状態にありました。それではセキュリティにギャップが生じてしまい、サイバー犯罪に利用される可能性があります。
最後に、境界型セキュリティソリューションに過度に集中していたため、内部のシステムとデータがサイバー攻撃に弱くなる恐れがありました。境界型セキュリティは重要ですが、高度なサイバー攻撃から完全に保護することはできません。多くのセキュリティソリューションを有しているA銀行では、Syslogまたはフロー分析データから取得した情報を利用していました。ただ、この情報だけでは脅威に対する具体的な証拠が不足しているため、分析と迅速な対応ができませんでした。この課題に対処するため、内部ネットワーク内の脅威を含むすべてのシステムとデバイスで脅威を検出し、対応できる包括的なセキュリティソリューションを必要としていました。

ソリューション

Quad MinersのNDRソリューションであるNetwork Black Boxには、ネットワークセキュリティ強化に役立ついくつかの主要な機能が含まれていました。まず、このソリューションはコアスイッチおよびバックボーンスイッチの南北・東西のトラフィックをミラーリングするように設計されています。これは潜在的なセキュリティの脅威を検出して対応するための重要な機能であり、これによりすべてのネットワークトラフィックを包括的に可視化することが可能です。
次に、トラフィックミラーリングを管理するためにNetwork Packet Brokers（NPBs）を活用してパケットの重複を排除したことで、セッションベースのミラーリングトラフィックを受信できるようになりました。これにより、ネットワークパフォーマンスに影響を与える可能性のあるボトルネックを回避することがきます。
また、このソリューションにはNetwork Black Boxも含まれています。Network Black Boxは、フルパケットキャプチャしたデータを用いてトラフィックを全数検知することにより、ネットワーク通信間のすべてのファイルを抽出することができます。この機能により、A銀行はファイルに対する脅威をリアルタイムでチェックできるようになり、悪意のあるアクティビティを迅速に特定し、対応することが可能となります。
最後に、統合検疫システムが組み込まれています。これもNetwork Blac Boxから実装されました。検疫システムは複数のAdvanced Persistent Threat（APT）ソリューションと統合しており、A銀行はAdvanced Threatに対する包括的なセキュリティを提供しています。これにより、既知/未知のマルウェアによる感染を複数のチェックで正確に判断できます。

導入効果

Network Black Boxの実装により、A銀行は南-北のトラフィックだけでなく東-西のトラフィックにも死角のない悪性コード対応システムを構築することができました。このソリューションは、ファイルハッシュとオリジンファイルの動的な分析により、すべてのトラフィックからすべてのファイルを徹底的に検査するように設計されました。
またマルチAPTソリューションを統合することで、悪性コードの分析と対応プロセスをシステム化することを可能にしました。これにより、A銀行は潜在的な脅威を迅速に特定、対応することができ、サイバー攻撃やデータ侵害のリスクを最小限に抑えることができました。
Network Black Boxを通じて実装された包括的な悪性コード対応システムは、非常に効果的であることが証明されました。また　A銀行は、システムの強固なセキュリティにより、顧客データを保護しながら業界の規則に準拠することができました。