REAQTA
an IBM Company

IBM

お客様事例: 主要国際空港

エアギャップ・ネットワーク
内部のマルウェアの追跡

事例

世界最大級の空港の 1 つでは、セキュリティーから物流まで、内部業務を管理するエアギャップ・ネットワークを運営しています。空港という隔離された環境にも関わらず、いくつかのデバイスがマルウェアに感染し、ローカルの情報が不正に搾取され、保存されていることが判明しました。

課題
- 重要なインフラストラクチャーであるためダウンタイムが許されない
- ネットワーク内のセキュリティー対策が不十分である
- エアギャップ・ネットワーク内で、高いセキュリティー・レベルと低いセキュリティー・レベルのデバイスが混在している
- エアギャップ内のデバイスに可視性がない

解決策
- IBM® Security ReaQta は、NanoOS テクノロジーを使用して、エンドポイントとインフラストラクチャー全体に優れた可視性を提供するように設計されています。
- ReaQta 動作分析は、分離されたネットワーク上で劣化することなく動作します。
- ReaQta は、インシデントの再構築と侵害後の分析を可能にする強力な脅威追跡機能を提供します。

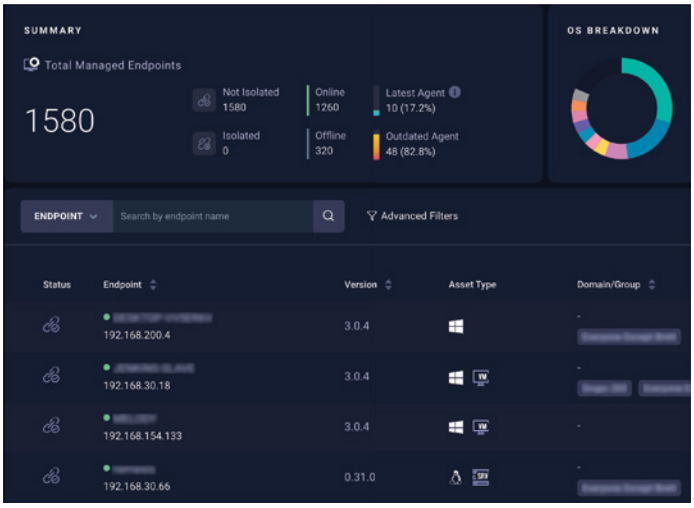
会社

この主要な国際空港は、世界最大の交通ハブの 1 つです。1 日あたり 1,000 便以上のフライトがあり、年間 7,000 万人の乗客が利用するこの施設は、重要なインフラストラクチャーとして認識されています。

セキュリティーの課題

空港では非常に優れたセキュリティー・プロトコルが全体に採用されていました。完全に分離されたネットワークでいくつもの重要なサービスを採用し、インターネットからの感染を防いでいました。しかし、エアギャップ・ネットワークであることで、誤った安心感が生まれてしまったのです。エアギャップ内の全デバイスはインターネットに接続されていないものの、内部の全ネットワーク・セグメントは、トラフィック制御なしで相互に接続されていました。

さらに、エアギャップ・ネットワークには、インフォメーション・キオスクなど、一般の人々が物理的にアクセスできるデバイスが含まれており、重要なサービスが潜在的な攻撃にさらされていました。また、外部からの情報を内部に取り込む唯一の手段として USB ドライブを使用していたため、空港従業員によって無意識のうちにマルウェアが持ち込まれる可能性があり、エンドポイントが脆弱になっていました。



プロセス

一部のエンドポイントで速度が低下したような兆候が見られたため、ReaQta (IBM) による、エアギャップ・ネットワークの検疫チェックを提案しました。ReaQta が最初のセグメントに実装されると、対応エンジンにより、いくつかのデバイスで潜在的な不正アクティビティが検出されました。最初の分析では、一般人のアクセスが可能なインフォメーション・キオスクが最初のエントリー・ポイントとして指摘され、次の分析では、チェックイン・エリアのデバイスが 2 番目のエントリー・ポイントであることが判明しました。これら 2 つの攻撃ベクトルは、異なるネットワーク・セグメントに接触する限られた数のデバイスに拡散させようとしていました。

ReaQta プラットフォームによって可視性が提供されたことにより、空港のビジネス継続を中断することなく、インシデントの初期段階で再構築が可能になり、感染後でも安全にシステムを修復することができました。

根本原因分析
導入後初期の段階で、いくつかの動作に対して異常フラグが立てられました。アプリケーションにより、既定ブラウザーに隠しインスタンスを挿入する方法で、メモリ内にキーロガーがインストールされました。その後、別のスレッドにより、Microsoft Word ファイル、PDF ファイル、クッキー、ブラウザー・データベースを探すディスクに対しスクラブを実行しました。これらの情報は、隠しフォルダ内で収集され、コマンド＆コントロール (C2) サーバーに定期的に送信する動作が見られましたが、ネットワークが外部から完全に隔離されていたため失敗に終わっています。

攻撃ベクトルをより詳しく調べると、興味深い結果が得られました。攻撃ベクトルは異常なほど大きく、ローカル・アンチウイルスだけでなくサンドボックス分析もバイパスするような一連のメカニズムが含まれていました。そのような攻撃システムは通常、バイナリー全体の小さなチャンクをエミュレートするため、攻撃ベクトルを大きくすることで、ウイルス対策エミュレーション・エンジンを回避する意図があると思われます。

最終的に、公共のインフォメーション・キオスクに設置された攻撃ベクトルと、チェックイン管理ネットワークセンサーの一部であるデバイスにインストールされた攻撃ベクトルという、2 つの異なるベクトルが特定されました。2 つの攻撃ベクトルは異なっているように見えましたが (主に、検出を回避するために使用される大量のジャンク命令)、マルウェアは同じ種類のようでした。いずれの場合も、同じ C2 サーバーに接続しようとしており、同じように動作していました。

攻撃再構成
ReaQta は侵害後のみに適用され、すべての情報が利用できないため、ネイティブ・インフラストラクチャーでは最小限のオペレーティング・システム・レベルのログ記録のみが使用されます。最小限の情報であったにも関わらず、フォローアップ分析によると、感染は 5 か月前に発生しており、2 つのエンドポイントで、2 つの異なる USB ドライブから数日の間に感染していたことが判明しました。その他のエンドポイントでは、接続可能な全デバイスでマルウェアによるランダムな照合が行われてしまい、パスワードが簡単だったことが原因で、攻撃ベクトルの 1 つから感染してしまったのです。このマルウェアは、継続的に情報を搾取することは可能であるものの、情報の保持や管理、また独自のストレージに制限を適用したりすることは不可能のようでした。8 時間ごとに C2 への接続が行われましたが、エアギャップ・ネットワークのために成功しませんでした。

最終的な分析によると、マルウェアには自己複製機能があり、外部 USB ドライブにストレージを自動でコピーできるものの、この機能は有効になっていませんでした。おそらく、情報搾取は手動で開始されることになっていたと思われます。

対応と修復
ReaQta の修復モジュールは、感染したデバイスをクリーンアップし、識別されたストレージ・フォルダーをクリアにして、データ漏洩を回避しました。脅威追跡インターフェイスは、すでにデバイスへの感染が検出されている場合を除き、インフラストラクチャー全体に同じ攻撃ベクトルがないことを確認するために必要不可欠であることが証明されました。不正な動作の検索が実行され、マルウェアのインスタンスが他のデバイスで検出されていないことも確認されました。インフラストラクチャー内に、その攻撃ベクトルと変異型ベクトルが存在しないことが確認されるまで、特定されたすべての不正な動作、永続的な脅威、およびデータ収集方法が追跡されました。

最後に、ローカル・セキュリティチームは、内部トラフィック制御に対して、より厳格な各ルールを設定しました。ネットワークの公開部分は運用から分離され、ローカル・セキュリティチームにより、継続的なエンドポイント監視と定期的な脅威追跡などの対応が行われました。

結果

エアギャップ・ネットワークのセキュリティー・レベルは強力であると言えますが、実装が緻密かつ慎重でないと、セキュリティーに対して誤った安心感が生まれてしまう可能性があります。攻撃の動機は不明であり、データが搾取されたものの、漏洩することはありませんでした。攻撃者は、情報を漏洩させるのみでなく、空港の運営に大きな損害を与えるために、インフラストラクチャーへ侵入しようとした、と断定されました。チェックイン・エリアで発生した単純なランサムウェア感染により、避けられない遅延が発生してしまいました。セキュリティー・エリアで同じような攻撃が行われたら、フライト停止に追い込まれ、深刻な状況が引き起こされたおそれがあります。

詳しくは、以下をご覧ください:
ibm.com/jp-ja/products/reaqta

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町19-21

米国で制作

2022 年 4 月