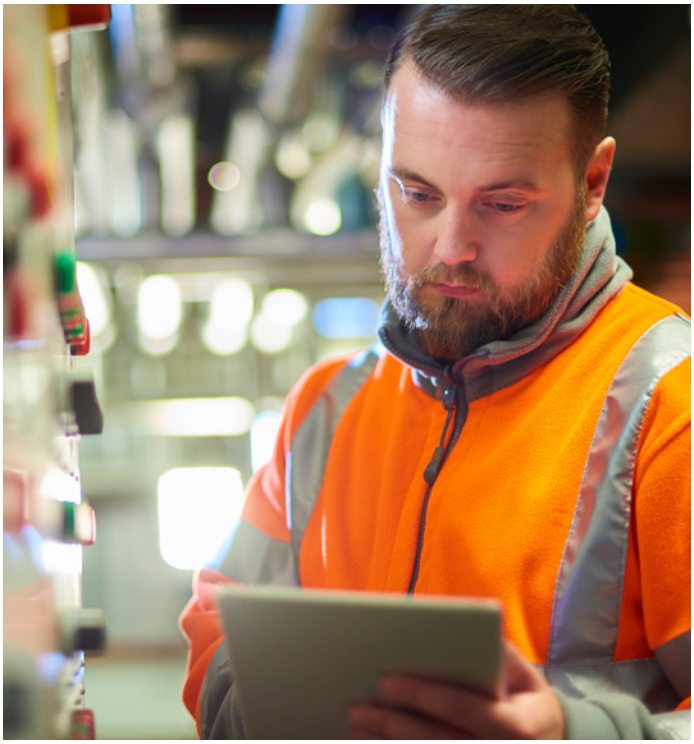
REAQTA
an IBM Company

IBM

お客様事例：
重要なインフラストラクチャー

水管理設備に対する極めて巧妙な
サプライチェーン攻撃を追跡



事例

国外の攻撃者は、サプライヤーを通して水管理施設を標的にします。オペレーターが疑わしい動きに気付いても、外部のセキュリティー・サービス・プロバイダーが保守作業を行っているだけだと考えてしまいます。アクセスの権限入手に成功した攻撃者は、ラテラル・ムーブメントの手法でオペレーターのネットワークに入り込みます。そして、ハイレベル・サーバーに侵入し、水管理施設に関する内部情報の持ち出しを企て、犯罪対策対抗型のランサムウェアを展開します。

課題

- 業務対象地域への配水管理を担当する重要なインフラストラクチャーとして、攻撃を受けやすい立場である
- ファイルレス脅威やラテラル・ムーブメント手法に対する検知機能および追跡機能がない
- ランサムウェアに対する防御機能がない
- エンドポイント・セキュリティーに割り当てられるリソースが限られている

ソリューション

- IBM® Security ReaQtaは、攻撃者から見えない設計となっているNanoOSを使用し、エンドポイントとインフラストラクチャー全体で優れた可視化を提供
- ラテラル・ムーブメントや異常なログイン活動を徹底的に追跡
- ランサムウェアによる攻撃から徹底的に防御
- 極めて複雑なインシデントの追跡と再現を可能とする強力な脅威追跡インターフェースを提供

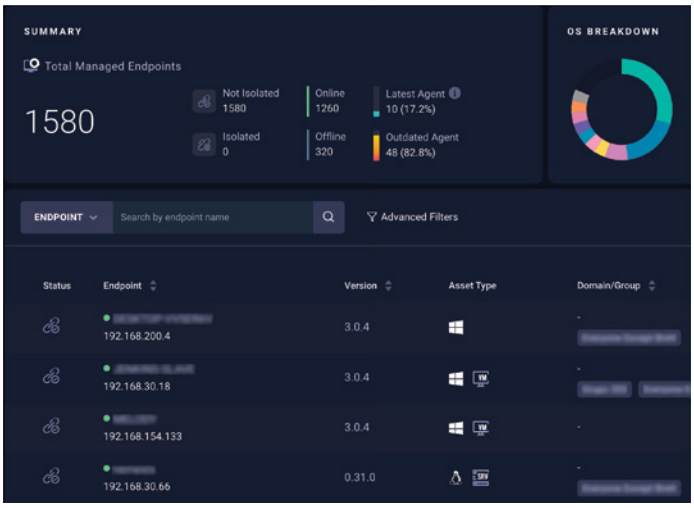
企業

ヨーロッパに拠点を構えるこの水管理施設は、約100万人分の水処理および配水業務を担っています。当施設は、極めて重要なインフラストラクチャーであり必要不可欠なサービスに分類されます。

セキュリティー上の課題

サイバー・リスクの複雑化が進み、攻撃者の手口が巧妙になってくることから、重要なインフラストラクチャー施設は、攻撃への対策を継続的に実行しなければなりません。重要なインフラストラクチャー施設で管理されるリソースの特徴として、大きな影響を与え、極めて機密性の高いデータを持ち出すことが可能になるため、これらの施設は攻撃者の格好の標的です。

この水管理施設には従来のネットワーク分析ツールだけで、エンドポイントのモニタリングは設置されておらず、攻撃に対応できる機能がありませでした。ラテラル・ムーブメントなど、エンドポイントをまたぐ攻撃を追跡することはできなかったのです。また、ITリソースが全体的に不足しており、Eメール、DNS、VPNやファイアウォールなどの重要なサービスを管理する際に、オペレーターは外部のプロバイダーを雇っていました。複数のプロバイダーが業務を実施しているため、ますます複雑化が進んでしまったのです。



独自のハイパーバイザー型アプローチであるNanoOSは、オペレーティング・システム外で機能するため、エンドポイントで実行されるプロセスとアプリケーションで優れた可視性を発揮します。

プロセス

IBMの関連会社であるReaQta社は、施設内のすべてのサーバー、デスクトップおよびノートPCにおいて、継続的にあらゆる資産をモニタリングしながら、潜在的なセキュリティー・ブリーチ（抜け穴）を迅速に追跡および検知できるソリューションを設置してほしいという依頼を受けました。内蔵型デュアルAIエンジンと詳細な行動分析を使用するReaQta NanoOSテクノロジーにより、インフラストラクチャー全体が最大限に可視化されました。このため、リアルタイムでエンドポイントにおけるクエリーを実行し、侵害の痕跡（IOC）や不正な行動の痕跡（IOB）を広範囲で検知するとともに、潜伏した脅威の発見に向けた高度なデータ・マイニングも実行することができました。

導入から6カ月後、エージェントが最初の異常なアクティビティーを検知し、特定のデータ群にアクセスしようと試みていた攻撃者を追跡しました。今まで使用していたアンチウイルスや侵入検知システム（IDS）などのソリューションでは、攻撃が最終段階に至るまで、不審なアクティビティーがまったく検知されませんでした。もしReaQtaを導入していなかったら、攻撃者はデータにアクセスして持ち出し、インフラストラクチャーのどこにもその痕跡を残さないことに成功していたでしょう。

サプライチェーン攻撃
最初の攻撃があった日、ReaQtaによりVPNサーバーから非特権ネットワーク・セグメント内のエンドポイントに向けて、疑わしいログインにフラグが立てられます。セキュリティー・チームは、このログインが社外のセキュリティー・プロバイダーによる保守業務のためだと考え、インシデントの優先度を低と設定します。攻撃者は、特権ネットワークへ直接つながるパスを見つけるため、主にネットワーク・セグメントのマッピングに使う最初のマルウェアを展開させます。そのようなパスが存在しないと分かると、攻撃者はメモリー内に第2のマルウェアを展開し、資格情報を取得して、後のラテラル・ムーブメントに再利用しようとします。目当ての資格情報を入手すると、攻撃者はドメイン・コントローラーへ侵入し、その直後、内部文書が収められているファイル・サーバーへ侵入します。攻撃の最終段階で、攻撃者は痕跡を隠蔽するため、インフラストラクチャー全体にランサムウェアを展開します。

根本原因分析
最初の不正ログインは、サーバーとのやり取りは多いものの、ワークステーションとはやり取りしないエンドポイントにおいて、シフト時間外に発生しました。VPNチャネルの管理者は、VPNの他にEメール・サーバーやファイアウォールの維持も担当している社外プロバイダーでした。権限の性質上、あらゆる操作を追跡するためにアラートはアクティブな状態に保たれていました。しかし、社内セキュリティー・チームは当時、社外プロバイダーがインフラストラクチャーの保守作業を行っていると考え、このインシデントの優先度を低に設定しました。

翌日、ReaQtaにより内部ネットワークがスキャンされた際に、軽度マルウェアによるアクティビティーが検知され、2回目のアラートが出されました。その後間もなく、キーロギングおよび資格情報取得機能を持つメモリー内ベクトルの存在を警告する別のアラートが出されました。この時点でセキュリティー・チームは、ラテラル・ムーブメント手法によりドメイン・コントローラーの1つにアクセスしようとしたサイバー攻撃インシデントであると考え、脅威検知を開始しました。セキュリティー・チームは、攻撃者に見えないNanoOSテクノロジーを活かし、攻撃者の手口と目的を探るため、可能な限り追跡を継続しました。

攻撃者が、極めて機密性の高い情報が保管されているファイル・サーバーへ侵入しようとした時、チームはこれを阻止するための排除計画を開始しました。さまざまなデバイスが修正され、攻撃者はハイレベルの権限を取得したにも関わらず、目当ての情報にアクセスできないことに気付きました。見つかったと判断した攻撃者は、痕跡を隠すため、インフラストラクチャー全体にランサムウェアを展開しました。

攻撃と再現
攻撃の動機が明らかになると、オペレーターはインフラストラクチャー内の弱点を強化するため、攻撃の全体像を理解する必要がありました。ランサムウェアの展開前の段階（フェーズ1）で攻撃されたデバイスは12台、展開後の段階（フェーズ2）では数千台のデバイスが攻撃されていました。

攻撃者は、VPNとメール・サーバーへのアクセス権限を入手しており、これらの権限を内部ネットワークへの最初のエントリー・ポイントとして使用しました。プロバイダーの資格情報を再使用してデバイス間を移動していた攻撃者は、最終的にある特定のワークステーションに落ちつきました。攻撃者はこの時点で、一連のツールを使って内部ネットワークをスキャンし、ラテラル・ムーブメントの標的を特定しました。最終段階では、ドメイン・コントローラー自体を使用して、全てのデバイスをランサムウェアに感染させました。

対応および修復
VPNアクセスが保護され、脅威検知が行われて、攻撃者がアクセスに成功したデバイスが全て特定されました。ReaQtaの修復モジュールにより、クリーンアップ・プロセスが自動的に実行され、セグメントのクリーンアップが数秒で終わりました。偵察およびラテラル・ムーブメントの段階で使用されたツールがすべて取得され、IOCおよび不正な行動への対処を含むポリシーが、即座にインフラストラクチャー全体に反映されました。ポリシーの展開後、危険なホストの侵入は確認されていません。すべてのユーザーの資格情報は即座にリセットされ、重要な情報の損失や通常のアクティビティーの中断を防止するReaQtaのアンチランサムウェア機能がすべてのデバイスで有効化されたため、ランサムウェア攻撃は、それ以上進みませんでした。

このインシデントは、データの損失、必須サービスの中断またはエンドポイントなどの被害を受けることなく、2日目に無事に終結しました。

結果

セキュリティー・チームがアクセスを遮断するまで、IBM Security ReaQtaにより、相手から見えないように攻撃者の動作が追跡されました。その後、ReaQtaソリューションが展開され、侵入された装置はクリーンアップされ、ダウンタイムもありませんでした。ReaQtaを導入していなければ、機密性の高い情報が攻撃者により確実に持ち出され、長期間サーバー内で不正なアクティビティーが続き、最後にはランサムウェア攻撃によってインフラストラクチャー全体が破壊されてしまったかもしれません。このような壊滅的な攻撃が発生すると、対象地域の市民に継続的に必要なサービスを提供する施設の機能に甚大な影響を与え、施設の機能がストップしてしまったでしょう。サプライチェーン攻撃を特定することは非常に難しいため、漏洩の根本原因を特定するための犯罪科学情報を利用していなかった場合、施設は同じようなチャネルを通じて情報漏洩の被害に遭っていたかもしれません。

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

2022年5月