cpl.thalesgroup.com

THALES
Building a future we can all trust

保護されていないRDPを悪用したランサムウェア攻撃とその対処法

2020年前半、さまざまな業種の企業を標的としたランサムウェア攻撃が急増しました。サイバー犯罪者は、私たちのデジタル通信やリモートワークへの依存を、悪意のある目的で利用しています。ランサムウェアインシデントの大半は限られた数の侵入ベクトルに起因すると考えられ、その上位3つは、安全性の低いリモートデスクトッププロトコル（RDP）エンドポイント、電子メールフィッシング、ゼロデイVPNの脆弱性の悪用です。

Coveware, Emsisoft, Recorded Future のレポートでは、「RDPはランサムウェアの単一かつ最大の攻撃ベクトルと考えられ」、2020年のほとんどのランサムウェアインシデントの発生源であると強調されています。昨今の在宅ワークの導入によって、RDPがランサムウェアの最大の侵入ベクトルになったと思われるかもしれませんが、これは正しくありません。昨年以降、ランサムウェア攻撃者が消費者を標的にするのをやめ、代わりに企業や重要なインフラストラクチャを狙うようになり、RDPは最大の侵入ベクトルの1つとなりました。

根本原因は？

RDPは、リモートシステムに接続するための最も一般的な技術であり、通常、プライベートネットワーク内で使用する場合に安全かつ確実なツールと見なされています。ただし、RDPポートがインターネットに公開されたままの状態で、単純なパスワードでアクセス可能な場合、重大なセキュリティ上の問題が発生する可能性があります。パスワードは侵害を受けやすいため、保護されていないRDPを介した企業ネットワークへの悪意のある不正アクセスを容易に許してしまう危険性があります。RDPを介した不正アクセスにより、攻撃者は企業サーバーへのアクセスを取得し、ランサムウェア攻撃の発射台として利用できるようになります。

数百万台ものコンピュータのRDPポートが保護されずにオンラインに公開されており、RDPは、さまざまな悪意のあるサイバー活動や、ますます増加するランサムウェア攻撃への、巨大な攻撃ベクトルになっています。こうしたアクセスポイントを悪用しようとしている犯罪者は、「RDPマーケット」上でそれらを無料で見つけることができます。そこから先は、いつもどおりの仕事です。ブルートフォースやソーシャルエンジニアリングなどのよく知られた手法を利用して、脆弱なパスワードを探します。攻撃者はターゲットシステムへのアクセスを取得すると、ネットワークを可能な限り安全でない状態にすることに集中します。

セキュリティシステムが無効化され、ネットワークが保護されない状態になると、サイバー犯罪者は悪意のあるパッケージを自由に配信できるようになります。ランサムウェアのインストール、キーロガーの展開、侵害されたマシンを使用したスパムの拡散、機密データの窃取、今後の攻撃のためのバックドアのインストールなど、さまざまなものが考えられます。

RDP攻撃を軽減するためのベストプラクティス

上述のとおり、RDPは企業ネットワークの内部に侵入するためのアクセスポイントであるため、インターネット上にさらしたり、保護されていない状態で公開したりすべきではありません。ユーザーの利便性のためにリモートデスクトップを公開することは、組織がさらされる脅威の増大を正当化する理由にはなりません。

組織でRDPを使用する必要がある場合、アクセスポイントの強化に焦点を当てた次のベストプラクティスが、ブルートフォース攻撃からRDPを保護するために役立ちます。

- 原則として、保護されていないリモートデスクトップをインターネット上に公開しない。これが絶対必要な場合は、RDPアクセスポイントが多要素認証（MFA）によって確実に保護されるようにし、検証済みのユーザーのみがRDPにアクセスできるようにします。
- RDPゲートウェイを使用する。リモートデスクトップをリバースプロキシゲートウェイで保護し、標準のRDPポート3389を難読化する必要があります。RDPゲートウェイは、TLS暗号化プロトコルによって保護されたHTTPS接続（ポート443）を介してアクセスされます。
- RDPゲートウェイへのアクセスにMFAを適用する。最も強力なパスワードでさえ侵害される可能性があります。MFAは万能薬ではありませんが、RDPセッションにログインするためにユーザーが少なくとも2つの検証要素を提供する必要がある認証方法により、追加の保護レイヤーを提供します。
- ネットワークログオンにMFAを適用する。リモートデスクトップに入ったら、ネットワークログオンポイントにMFAを適用して、さらなるセキュリティレイヤーを実装します。

Thales SafeNet Trusted Accessを利用した攻撃の軽減方法

Thales SafeNet Trusted Accessは、RDPベースのランサムウェア攻撃からビジネス環境を保護するために役立ちます。SafeNet Trusted Accessにより、組織は、使用されているエンドポイントデバイスに関係なく、RDP、RDPゲートウェイ、追加のクラウドやレガシーアプリへのリモートアクセスを効果的に保護できます。SafeNet Trusted Accessは、以下を提供します。

- アダプティブ認証、ステップアップ認証、MFA、ハードウェアベースのトークンなど、多彩な認証オプションのサポート。
- すべてのOS（Windows/Mac/Linux）に対応する柔軟なアクセスポリシー – 実行しているOSに関係なく、単一のアクセス管理および認証サービスを使用して、クラウドベースのアプリとすべてのリモートデスクトップを保護できます。
- 単一のアクセス管理/MFAサービスによる、クラウドアプリとネットワークログオンの一元管理。

About Thalesタレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。

> cpl.thalesgroup.com <

お問い合わせ先 – cpl.jpsales@thalesgroup.com すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。