滋賀県警からのサイバーセキュリティに関するお知らせ

新しいランサムウェア攻撃に注意
「人手によるランサムウェア攻撃」と「二重の脅迫」

最近、従来のランサムウェア攻撃とは異なる、新たな攻撃方法による被害が確認されています。

① 人手によるランサムウェア攻撃（human-operated ransomware attacks）

② 二重の脅迫（double extortion）

攻撃者は、企業・組織を標的としてこれらの攻撃方法を用いて、事業継続のため金銭を支払わざるを得ない状況を作り上げ、より確実に、かつ高額な身代金を得ようとしています。従来のランサムウェアに加え新たなランサムウェア攻撃にも注意が必要です。

ランサムウェアとは、パソコン等の端末及びネットワーク接続された共有フォルダ等に保管されたファイルを、利用者の意図に沿わず暗号化して使用不能にする、または画面ロック等により操作不可とするウイルスの総称です。

このウイルスは、使用不能な状況を復旧することと引き換えに、金銭を要求することから「身代金要求型ウイルス」とも呼ばれています。なおランサムウェアは「ransom」（身代金）と「malware」（マルウェア）を組み合わせ造語です。

従来のランサムウェア攻撃は、ウイルスを添付したメールをばらまき、ウイルス感染した端末に対して身代金を要求する手法です。つまり、攻撃対象は不特定で、運悪く感染した被害者から身代金を得ようという戦略です。

人手によるランサムウェア攻撃

「人手によるランサムウェア攻撃」とは、標的型攻撃と同様、攻撃者が様々な攻撃手法を駆使して、企業・組織のネットワークに侵入します。その後、事業継続に関わるシステムや機微情報が保存されている端末やサーバ等を探し出してランサムウェアに感染させたり、ドメインコントローラのような管理サーバを乗っ取って、企業・組織内の端末を一斉に感染させたりする攻撃です。

データやシステムの復旧を阻害するため、バックアップ等も同時に狙われることがあります。

二重の脅迫

「二重の脅迫」とは、ランサムウェアにより暗号化したデータを復旧するための身代金要求に加え、暗号化する前にデータを窃取しておき、「支払わなければデータを公開する」などと二重に脅迫する攻撃方法です。

従来のランサムウェア攻撃への対策として、データのバックアップを行う防御策を進めてきましたが、攻撃者は、この防御策の更なる対抗策として、データの窃取と公開による脅迫という、新たな攻撃方法を取り入れたとみられています。

«新たなランサムウェア攻撃の対策»

新たなランサムウェア攻撃の特徴は、企業や組織のネットワークに侵入すること、そして情報を窃取することです。 侵入には、パスワード解読による不正アクセス、システムの脆弱性をついた攻撃、メール送付によるウイルス感染等があります。したがって、侵入されないことが特に重要です。

侵入対策としては、

- 公開するサーバやネットワーク機器及びアクセス可能なサービスを最低限にする
- 外部からのアクセス制限と強固な認証方式の導入
- OS 及びソフトウェア、ネットワーク機器のファームウェア等の脆弱性の解消（最新の状態にする）
- メールに対するセキュリティ装置の導入や従業員の研修
- 侵入時の早期検知と侵害範囲拡大の防御のための、内部ネットワークの監視

などがあります。

詳しくは、IPA「【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について」（https://www.ipa.go.jp/security/announce/2020-ransom.html）をご覧ください。

[お知らせ] セキュリティに関する情報は、関係企業・組織と共有することも重要です。

滋賀県警察本部サイバー犯罪対策課 （代表）077-522-1231