2023 年 9 月 22 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai 脅威レポート：ゼロデイおよびワンデイ脆弱性の悪用がまん延、ランサムウェアの被害数は 143%増加

ランサムウェアグループの戦術が進化し、ファイル盗難が脅迫理由の首位になっていることが判明

※本リリースは 2023 年 8 月 7 日 (現地時間) マサチューセッツ州ケンブリッジで発表されたプレスリリースの抄訳版です。

オンラインライフの力となり、守るクラウド企業の Akamai Technologies, Inc. （NASDAQ：AKAM）は、進化するランサムウェアの状況に焦点を当てた最新の脅威レポート「インターネットの現状 | 猛威を振るうランサムウェア：進化する悪用手法と執拗なゼロデイの利用」（英文）を発表し、レポートのハイライトをまとめたブログを公開しました。

本レポートでは、ゼロデイおよびワンデイ脆弱性の悪用により、2022 年第 1 四半期から 2023 年第 1 四半期にかけて、ランサムウェアの被害総数が 143% 増加したことが指摘されています。また、ランサムウェアグループがファイル盗難を標的にする傾向が高まっており、機微な情報の不正な抽出または転送が脅迫理由の首位になっているという事実も明らかになっています。この新しい戦術の登場は、ファイルのバックアップ・ソリューションがもはやランサムウェアに対する十分な保護戦略ではないことを示唆しています。

レポートによると、攻撃者は手法や技法をフィッシングからさらに進化させており、脆弱性の悪用に重きを置くようになっています。攻撃者の戦術が変化するこの状況で、ランサムウェア界を席巻しているのが日本国内でも被害を出した LockBit です。2021 年第 4 四半期から 2023 年第 2 四半期には、被害総数の実に 39% を占めています。これは第 2 位となったランサムウェアグループの被害数の 3 倍以上の数字です。さらに解析を進めた結果、CL0P ランサムウェアグループはゼロデイ脆弱性を積極的に悪用しており、その被害数は前年比 9 倍に増加しています。

業界別に被害総数を見ると、製造業は 2021 年第 4 四半期から 2022 年第 4 四半期にかけて 42% 増となり、世界中のサプライチェーンに対する潜在的な脅威を示唆しています。LockBit は、製造業全体の攻撃のうち、41% を占めていました。ヘルスケア業界は、同期間の被害数が 39% 増となり、主に ALPHV（または BlackCat）と LockBit のランサムウェアグループの標的となっています。

「猛威を振るうランサムウェア：進化する悪用手法と執拗なゼロデイの利用」では、他にも以下のことが明らかになりました。

- 年間収益が 5,000 万ドル以下の組織は標的になるリスクが最も高く（65%）、同 5 億ドル以上の組織は被害総数の 12% にとどまります。
- ランサムウェア攻撃の被害者は複数回の攻撃を受けるリスクが高く、最初の攻撃の 3 か月以内に 2 回目の攻撃を受ける可能性が 6 倍以上となっています。
- 金融サービス組織は、被害を受けた組織の総数が前年比 50% 増となりました。小売業は業種別のランサムウェア被害数の第 3 位となり、9% 増となっています。

Akamai の Enterprise Security 担当 Senior Vice President 兼 General Manager である Pavel Gurvich は「ランサムウェア攻撃を仕掛ける攻撃者は、その手法と戦略を絶えず進化させており、組織の重要かつ機微な情報を盗み出すことで甚大な被害を与えています。組織は重要な資産を守り、ブランドの信頼を保ち、事業継続性を確保するために、攻撃者が用いる手法とツールを理解することが重要です」と、述べています。

詳細な情報については、Akamai セキュリティハブにアクセスするとともに、Twitter で @Akamai_Research をフォローしてください。Akamai の脅威リサーチャーと交流し、貴重な知見を得ることができます。

手法

このレポートで使用しているランサムウェアのデータは、約 90 のさまざまなランサムウェアグループのリークサイトから収集したものです。一般に、こうしたグループは、タイムスタンプ、被害者名、被害者のドメインなど、自らの攻撃の詳細を公表しています。注意が必要なのは、こうした公表は、ランサムウェアグループが自らの犯行を世に示したいという欲求の現れだということです。報告されているこうした攻撃の成否は、この調査の対象ではありません。

この調査では、報告された被害者に焦点を当てています。それぞれの解析では、各グループ内で固有の被害者数を測定しました。この被害者データを ZoomInfo から取得したデータと照合することで、各被害者の所在地、収益範囲、業種などの詳細を明らかにしています。すべてのデータは、2021 年 10 月 1 日から 2023 年 5 月 31 日までの 20 か月間に収集されたものです。

Akamai について：

Akamai はオンラインライフの力となり、守っています。世界中の先進企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、世界中の人々の生活、仕事、娯楽をサポートしています。超分散型のエッジおよびクラウドプラットフォームである Akamai Connected Cloud は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。