2023年第1四半期のランサムウエア被害組織とネットワークアクセスの販売状況

KELA

2023 年第 1 四半期のランサムウエア被害組織とネットワークアクセスの販売状況

KELA サイバー犯罪インテリジェンスセンター

目次

エグゼクティブサマリー

2023 年初旬、数千台もの ESXi サーバーを標的とする大規模なランサムウエアキャンペーンが発生し、ランサムウエアグループやデータリークグループが世界中の組織に危険をもたらし続けているという現状が浮き彫りとなりました[1]。さらに KELA でも、2023 年第 1 四半期（2023 年 1-3 月期）に発生したランサムウエア攻撃やデータリーク攻撃、売り出されたネットワークアクセスの件数が前年同期比で増加していることを確認しました（ネットワークアクセスは、ランサムウエアグループのサプライチェーンの中で重要な役割を果たしています）。今期我々がランサムウエアグループ、データリークグループ、初期アクセスブローカーの活動を監視して得た洞察の要点は、以下のとおりです。

- 2023 年第 1 四半期に発生したランサムウエア攻撃及びデータリーク攻撃の件数は、前年同期比（2022 年第 1 四半期比）で増加し、被害組織の数は約 900 に上りました。
- 今期、攻撃件数でトップ 5 にランクインしたランサムウエアグループ及びデータリークグループは、「LockBit」、「Clop」、「Alphv」、「Royal」、「Black Basta」となりました。今回初めてランクインした Clop は、Fortra 社製ファイル転送管理ソリューション「GoAnywhere MFT」のゼロディ脆弱性（CVE-2023-0669）を悪用しており、同グループの標的となった組織の数は 130 に上りました（Clop の主張に基づく）。
- 今期、ランサムウエアグループ及びデータリークグループの標的となった業界の 1 位は製造・工業製品であり、同業界に対する攻撃の 50%以上は LockBit、Royal、Alphv による犯行でした。
- 今期、ランサムウエアグループ及びデータリークグループの標的となった国の 1 位はこれまでと同じく米国であり、被害組織の 45%が米国の企業や組織でした。2 位は英国、3 位はカナダ、4 位はドイツ及びフランスとなりました。
- 2022 年に攻撃件数上位にランクインしていた Hive のオペレーションは、今期で活動を止しました。

[1]弊社プラットフォームで「ESXiargs Ransomware Campaign」に関するレポートをご覧いただけます。プラットフォームは、無料トライアル でアカウントを作成後ご利用いただけます。

- 今期新たに登場したランサムウエアブログ・データリークサイトは Vendetta、Medusa、Dark Power、Abyss、Money Message です。
- 今期 KELA が追跡調査を行ったネットワークアクセスの数は 600 件を超え、その希望販売価格の合計は約 58 万米ドルとなりました。
- 2023 年第 1 四半期に売り出されたネットワークアクセスの平均価格は約 1,100 米ドル、中央価格は 400 米ドルとなりました。

2023 年第 1 四半期におけるランサムウエア攻撃・データリーク攻撃の被害組織

2023 年第 1 四半期、我々は監視対象とするソース（ランサムウエアグループのブログや交渉ポータルサイト、データリークサイト、報道やその他公表されている報告など）で約 900 の被害組織を確認しました。この数字は前年同期比で 30%増となります。また我々が確認した被害組織数をひと月あたりの平均数で見ると、前年同期は約 230 組織であったのに対し、今期は約 300 組織となっています。

攻撃件数上位のランサムウエアグループ

2023 年第 1 四半期に攻撃件数で上位に挙がったランサムウエアグループ及びデータリークグループは、LockBit、Clop、Alphv（別名 BlackCat）、Royal、Black Basta であり、各グループが公表した被害組織の数は 45～270 に上りました。LockBit は 265 を超える被害組織を公開し、引き続き 1 位のポジションを維持しました。なお、この 265 という数字は 2 位の Clop が公表した被害組織の約 2.5 倍に相当します。しかしその Clop も 2023 年 3 月に攻撃のペースを上げて 100 の被害組織を公開し、同月に公表した被害組織数では LockBit を追い抜きました。

攻撃件数で 3 位となった Alphv は、先日フォーラム「RAMP」でランサムウエアの新バージョン「"BlackCat 2.0: Sphynx」のリリースを発表しました。

なお、Clop と Royal は今期初めて攻撃件数トップ 5 にランクインしたグループです。両グループは 2022 年にはランクインしていなかったものの、トップグループの 1 つであった Hive のオペレーションが米連邦捜査局（FBI）にテイクダウンされた恩恵を受けて、それぞれ 2 位と 4 位の座を獲得できたようです。