報道関係者各位

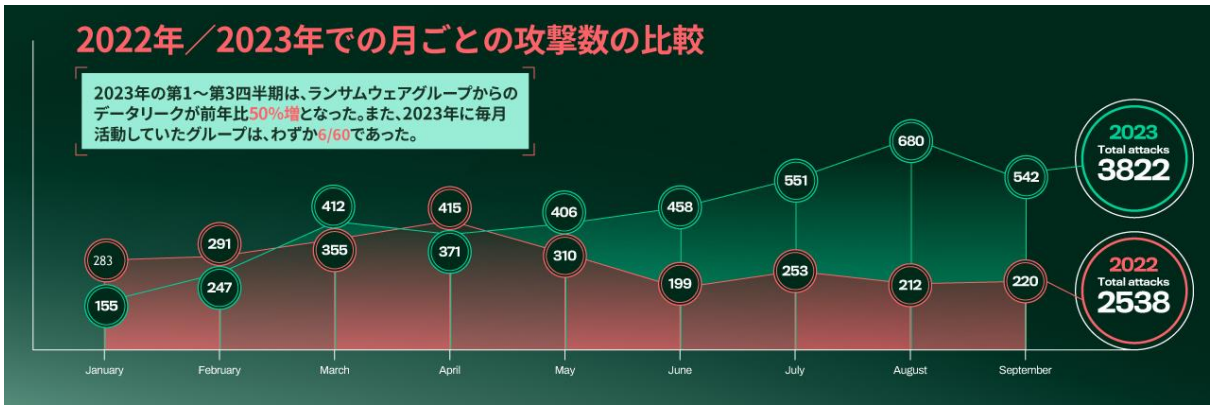
ウィズセキュア、2023 年第 1～第 3 四半期のランサムウェアリサーチ結果を発表

～ 前年比で攻撃数は増加しているものの、既存のプレイブックの焼き直しも多数観測 ～

2023 年 11 月 16 日
ウィズセキュア株式会社

マシンやデータの制御を奪う悪意のあるソフトウェア (マルウェア) の一種であるランサムウェアは、長年にわたりセキュリティ上の重要な問題となっています。その大きな理由の 1 つはランサムウェアを使用する攻撃グループの自己改変能力にあります。先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (旧社名: F-Secure、本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、ウィズセキュア) は同社のリサーチチームによる 2023 年第 1～第 3 四半期のランサムウェア攻撃の傾向をまとめたリサーチの結果を発表し、ランサムウェアの急増および変化について注意喚起をしています。

企業／団体や政府組織さえをもターゲットとするランサムウェアは攻撃グループにとっての大きな収入源となっており、この数年間猛威をふるっています。そして、それらのランサムウェアを取り巻く環境は変化しています。ランサムウェアギャングは、ターゲットのデータを暗号化して脅迫するだけでなく、データに含まれる個人をも脅迫するなどの複数の方法で身代金を要求する、いわゆる『多重脅迫型』の攻撃を仕掛けるようになってきています。多くの場合、身代金が支払われなければリークサイトでデータを公開すると脅迫しています。

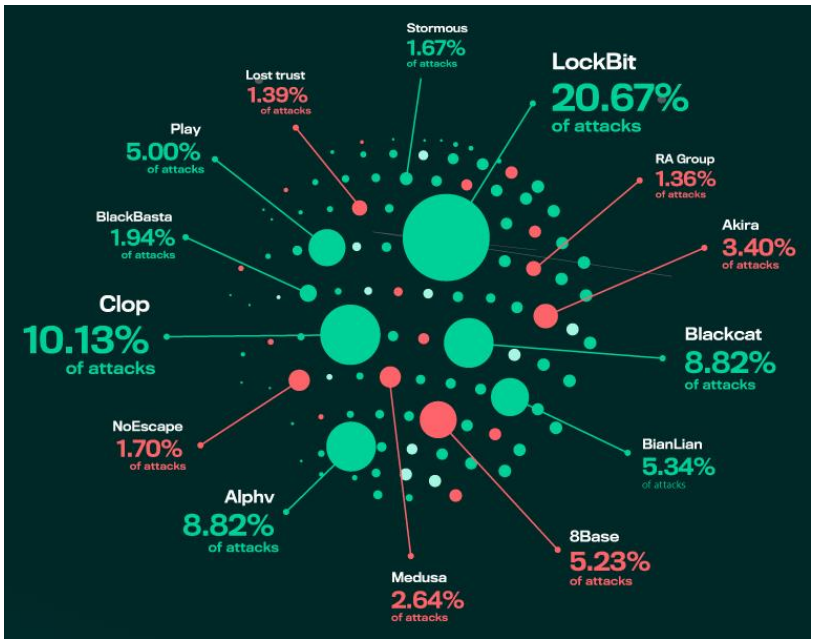


攻撃グループが運営するリークサイトに掲載されたデータをもとにウィズセキュアがおこなったランサムウェアリサーチによると、2023 年第 1～第 3 四半期において多くの新規のランサムウェアグループが活動を開始したことがわかりました。

ウィズセキュアで脅威インテリジェンスアナリストを務める Ziggy Davies (ジギー・デイヴィース) は、新たな攻撃グループの手法は既存のグループによる「既に確立された」プレイブックの焼き直しであるものの、その攻撃数を考慮すると、企業側も防御の手を緩めてはいけないものであると語っています。
「グループの名称が変更されたりメンバーが新規グループに移籍しても、ある程度は同じリソースや手法を再利用しているケースが多いのです。実際、今年私たちが目にした新しい攻撃グループの多くは、既知のランサムウェア攻撃キャンペーンにルーツを持つと考えるべきものが多く見受けられます。例えば、『Akira』をはじめとする複数のグループは、今はなき『Conti』と多くの共通点を持ち、『Conti』の元アフィリエイトが立ち上げたグループである可能性が高いです。」

以下は今回のリサーチから得られた、多重脅迫型ランサムウェア攻撃に関するインサイトの一例です:

- 2023 年第 1～3 四半期において、ランサムウェアグループからのデータリークは前年同期比で 50%増加した。
- LockBit がリークの最大のシェア (約 21%) を占めた。
- リークが多かった 5 つのグループ (8Base、Alphv/BlackCat、Clop、LockBit、Play) が全体の 50%以上を占めた。
- 分析の対象となったデータリークの約 25%は、2023 年になってから活動を開始した新規のランサムウェアグループによるものだった。
- 29 の新規ランサムウェアグループのうち、14 はすでに消滅または活動を停止している。
- 2023 年 1 月～9 月のすべての月に活動が観測されたのは、60 グループ中わずか 6 グループだけだった。



サイバー犯罪グループは以前にも増してランサムウェアの使用を推し進めているようですが、これらのグループが互いにプレイブックを再利用する現象が見られるため、防御側にはいくつかのアドバンテージがあります。Davies はその点について次のように述べています。
「サイバー犯罪者にとって、ランサムウェアは引き続き効果的な金儲けの手段であるため、これまでにない全く新しい手法や防御側が予想もできないことを考え出すのではなく、同じようなプレイブックに依存しています。そのため、サイバー犯罪グループによる攻撃はある程度予測可能であり、防御側にとっては、何を相手にすればいいのかがわかっているので好都合だとも言えます。とは言え、防御側は決して楽観的になってはならないのです。」

本リサーチに関するブログは以下のページにてご覧いただけます:
https://www.withsecure.com/jp-ja/expertise/blog-posts/2023-ransomware-rookies-are-a-remix-of-conti-and-other-classics (日本語)
https://www.withsecure.com/en/expertise/blog-posts/2023-ransomware-rookies-are-a-remix-of-conti-and-other-classics (英語)

ウィズセキュア Web サイト:
https://www.withsecure.com/jp-ja/
ウィズセキュアプレスページ:
https://www.withsecure.com/jp-ja/whats-new/pressroom

WithSecure について
ウィズセキュアは、IT サービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちは AI を活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を検出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は 30 年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。
1988 年に設立されたウィズセキュアは本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。
詳細は www.withsecure.com をご覧ください。また、X (旧 Twitter) アカウント @WithSecure_JP でも情報の発信をおこなっています。

※　以下、メディア関係者限定の特記情報です。個人の SNS 等での情報公開はご遠慮ください。

【本件に関する報道関係者からのお問合せ先】
ウィズセキュア株式会社
広報部　　秦　和哉
TEL：080-6842-8222 (モバイル)　／　03-4578-7745 (直通)
press-jp@withsecure.com