報道関係者各位

ウィズセキュア、サイバー犯罪のプロフェッショナル化に関する調査レポートを発表

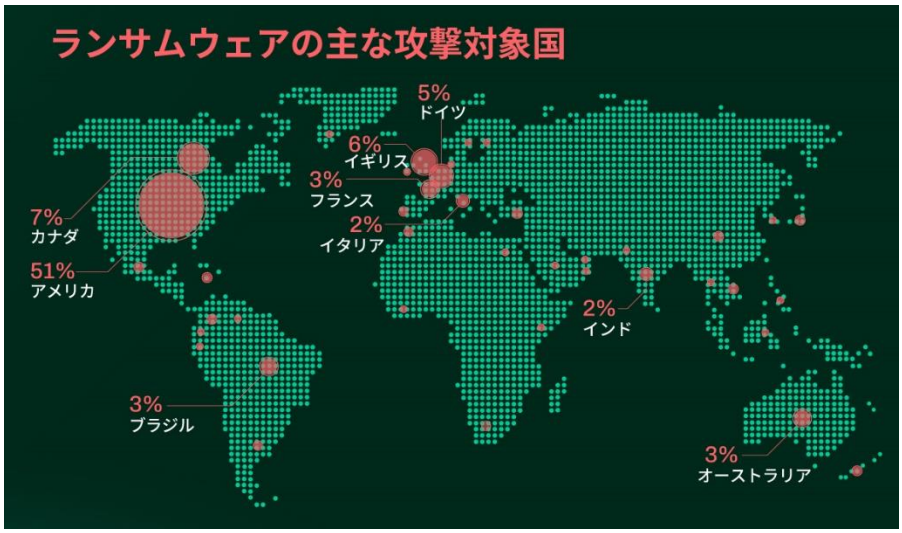
～ ランサムウェアの身代金支払いにより、サイバー犯罪グループはより多くのリソースを入手できるように ～

2023 年 5 月 26 日
ウィズセキュア株式会社

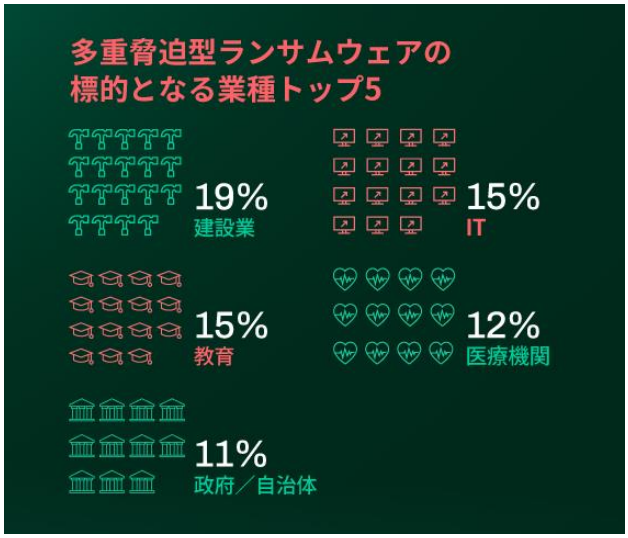
先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (旧社名: F-Secure、本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、ウィズセキュア) は、2022 年 1 月～12 月に観測したサイバー攻撃をもとに執筆した、サイバー犯罪に関する最新調査レポートを発表しました。レポートによると、ランサムウェアギャングの成功がサイバー犯罪者のプロ化というトレンドに拍車をかけ、様々なサイバー犯罪グループが専門的なサービスを開発し、それらを互いに提供し合っていることが明らかになりました。

ランサムウェアは数十年前から存在しています。防御側は長年にわたり対策を改善してきていますが、サイバー犯罪者はその都度そうした防御策に適応してきました。そうした中で注目すべきは、現在主流となっている多重脅迫型ランサムウェアグループで、その多くは、データの暗号化とそのデータの公開の両方の戦略を使用することで、被害者に身代金の支払いを促しています。

多重脅迫型ランサムウェアグループによる 3,000 件以上のデータ漏洩を分析したところ、これらの攻撃の被害者となった企業／団体は、国別ではアメリカが 51%と最も多く、次いでカナダ (7%)、イギリス (6%)、ドイツ (5%)、フランス (3%)、オーストラリア (3%)の順となっています。これら 6 ヶ国の被害者の数は、分析対象となったケースの 4 分の 3 を占めています。



業種別では建設業が最も影響を受けており、データ漏えいの 19%を占めています。2 番目に被害を受けたのは IT (15%) と教育 (15%)。そして医療機関 (12%)、政府／自治体 (11%) と続いています。ランサムウェア犯罪グループによって攻撃対象は様々で、必ずしも複数のグループが同じ業界を攻撃しているとは限りません。



ランサムウェアの脅威は様々な国や業界の組織に多大な被害や苦痛を与えており、サイバー犯罪業界におけるランサムウェアのインパクトは、誇張されても決してされ過ぎということはありません。

ランサムウェアが助長するサイバー犯罪の現状について、ウィズセキュアのシニア脅威インテリジェンスアナリストである Stephen Robinson (スティーヴン・ロビンソン) は次のように説明しています。
「ランサムウェアのグループは、ランサムウェア業界の莫大な収益の一部を得るために、オンライン犯罪の専門業者からツールやサービスを購入しています。これは、企業が利益を上げるために業務を外注するのとほぼ同じ方法です。このような能力と情報の供給は、低レベルの攻撃者から国家の支援を受ける APT (Advanced Persistent Threats = 高度かつ継続的な脅威) に至るまで、ますます多くのサイバー攻撃者に利用されるようになっています。ランサムウェアがサイバー犯罪そのものを生み出したわけではありませんが、火に油を注ぐことになったのは確かです。」

本調査レポートで取り上げている侵害のケースには、ある単一の企業が、それぞれ異なる目的やサービスを持つ次の 5 つの個々の脅威アクターによる攻撃を受けたものもありました:

- ランサムウェアグループ Monti
- Qakbot (マルウェア・アズ・ア・サービス)
- 8220 Gang (別名: ReturnedLibra) と呼ばれるクリプトジャッキング (暗号資産の不正マイニング) グループ
- イニシャルアクセスブローカー (サイバー攻撃において最初のステップである不正アクセスを実行する者)
- 北朝鮮の対外情報偵察総局に関連付けられる APT (高度持続的脅威) である Lazarus Group の下位集団

調査レポートによると、サイバー攻撃のプロ化の傾向により、企業や団体を攻撃するための専門知識とリソースが、低いスキルや少ないリソースしか持たない脅威アクターでも利用しやすくなっているとのことです。調査レポートはまた、今後数年間、攻撃者の数とサイバー犯罪産業の規模がともに拡大する可能性が高いと予測しています。

こうした傾向について、ウィズセキュアで脅威インテリジェンス部門の責任者を務める Tim West (ティム・ウェスト) は以下のように語っています。
「ランサムウェア攻撃が被害者に与える被害についてはよく話題に上っていますが、被害者が身代金を支払ってしまうことで攻撃者はより多くのリソースを得ることになり、それが本レポートで述べられているサイバー攻撃のプロ化という傾向を助長しているという事実は、あまり認識されていません。近い将来、このようなエコシステムの変化によって、防御側はより多様な種類の攻撃に直面することが予想されます。」

調査レポート「The Professionalization of Cyber Crime」(英語) の全文は以下のページをご覧ください:
https://www.withsecure.com/en/expertise/research-and-innovation/research/the-professionalization-of-cyber-crime

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、Twitter @WithSecure_JP でも情報の発信をおこなっています。