報道関係者各位

ウィズセキュア、データ侵害のリスクを軽減する予測分析に関するリサーチを発表

～ サイバー攻撃のプロフェッショナル化により攻撃者／ツールの特定が困難になるなか、予測がより重要に ～

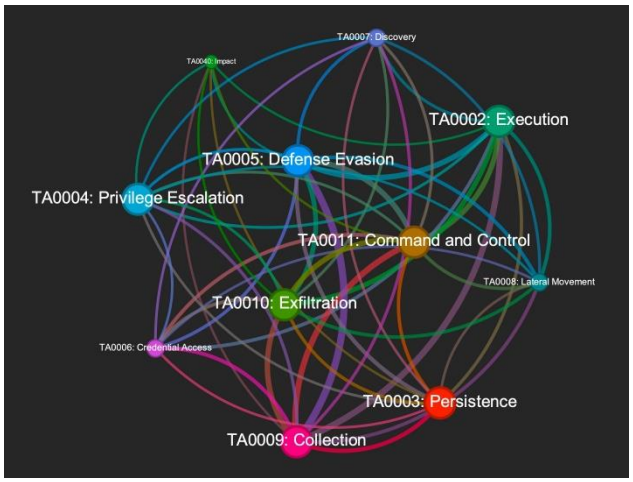
2023 年 10 月 12 日
ウィズセキュア株式会社

近年、サイバー犯罪のプロフェッショナル化により、セキュリティアナリストにとっては、使用される特定の TTP (戦術、技術、手順) に基づいて攻撃者や脅威を特定することがますます難しくなっています。そうしたなか、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、このような課題に対処するため、攻撃がどのように展開されるかを予測する代替モデルを実証する、新しいリサーチの結果を発表しました。

サイバー攻撃グループは自分たちのために企業／個人への攻撃を実行するだけでなく、自らが開発したツールの販売／レンタルやランサムウェア攻撃の請け負いを相互に行うなど、攻撃のプロフェッショナル化、そしてそしてサービス指向を強めています。[*1] そのため、「このツールを使った犯行はどのグループによるもの」という推測が必ずしも正解とは言えなくなってきています。

ウィズセキュアのリサーチ部門である WithSecure Intelligence でシニアリサーチャーを務める Neeraj Singh (ニーラジ・シン) は、サイバー攻撃の専門化という傾向はさらに悪化する可能性が高いと述べています。
「私たちはまず、攻撃者は常に新しい攻撃手法を開発し、ツールキットをはじめとするリソースを増やしていることを考慮する必要があります。このような変化により、特定の TTP やツールセットと関連付けることで特定のタイプの攻撃を理解・予測する従来のプロファイリング技術は、もはや有効であるとは言えなくなっています」。

そうした中、データ侵害における一般的な手法とツールセットに関するウィズセキュアの新しいリサーチは、サイバー攻撃がどのように展開されるかを予測する、別のアプローチを示しています。

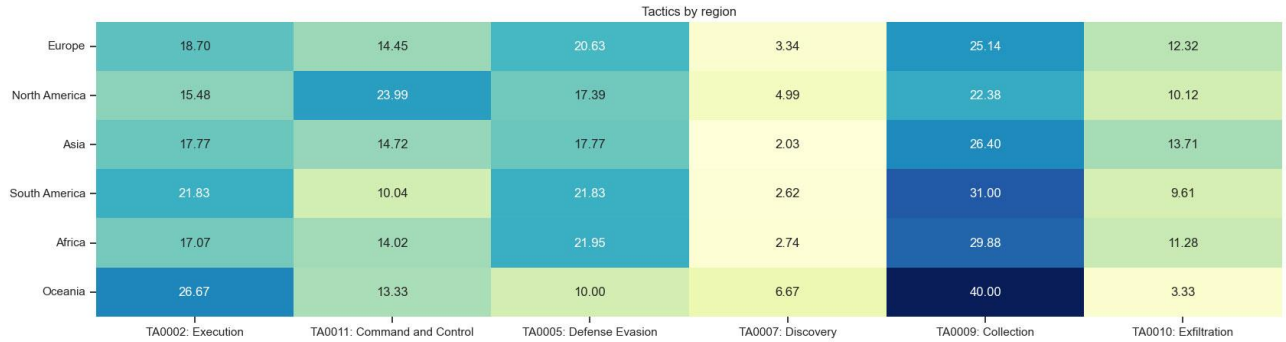


(過去 1 年間に ウィズセキュアのテレメトリーが観測した戦術をグラフ化)

2023 年にウィズセキュアが観測したサイバー攻撃から収集したデータに基づき、リサーチャーたちは攻撃で使用された戦術／ツールセットを相関させることができました。例えば、一般的に流出と C&C (コマンド・アンド・コントロー

ル) 戦術につながることがわかり、この可視化によって、攻撃者がその目的を達成するためにさまざまな攻撃チェーンで採用しているさまざまな戦術の相互関連性が明確に示されます。

Singh はまた、様々な攻撃経路についてさらなる予測を行ううえで、こうした相関関係が根拠となると語っています。「マシンラーニングは従来のデータ分析技術に基づき、異なるターゲットに対して異なる戦術やツールセットが使用される可能性を判断できる予測モデルを訓練することができます。これこそが、攻撃者が企業に対して特定のアプローチを使用するリスクを軽減するために、企業自身が取ることができる対策なのです」。



(2023 年に WithSecure Elements EDR テレメトリーで観測されたインシデントに見られる、地域ごとの MITRE ATT&CK 戦術)

レポートでは、攻撃におけるツール／戦術の相関関係の予測において、以下の項目を挙げています。

- ツールパターンの識別
- 防御に用いるツールの推奨
- 脅威インテリジェンスの強化
- 予測モデルの構築
- 新たな脅威への対応

ウィズセキュアによるリサーチ『Unveiling the Arsenal: Exploring Attacker Toolsets and Tactics』(英語) には、2023 年中に攻撃で観測された最も一般的な戦術とツールセットに関する情報、ウィズセキュアが調査した様々なセキュリティインシデントの解説、そして企業へのセキュリティアドバイスが含まれています。本リサーチの全文は以下のページでご覧いただけます:
https://www.withsecure.com/en/expertise/research-and-innovation/research/unveiling-the-arsenal-exploring-attacker-toolsets-and-tactics

*1:
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。