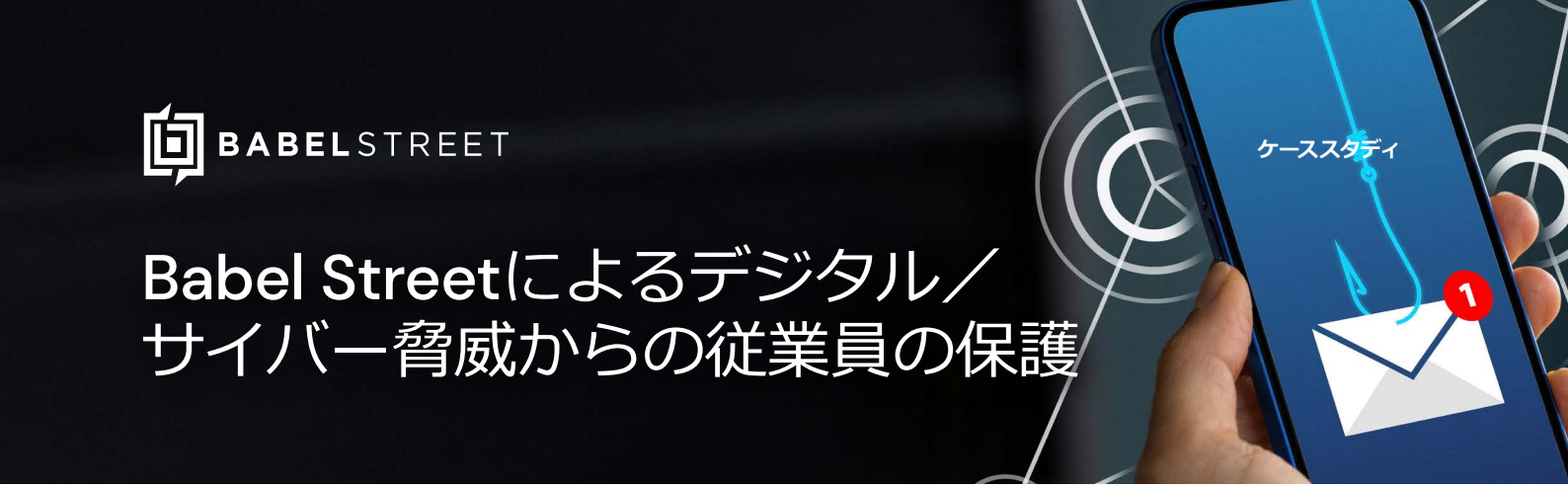

Babel Streetによるデジタル／サイバー脅威からの従業員の保護

これまで企業のセキュリティ部門は、役員、従業員、そして企業そのものを物理的な危害から守る役割を担ってきました。しかし、従業員がもはやたんなる被害者とは呼べず、犯罪者によって専有データや機密データを盗むために利用される無自覚な武器になってしまっているとしたら、企業のセキュリティチームには何ができるでしょうか。

サイバー攻撃者は、高度なテクニックとソーシャルエンジニアリングを駆使して、幹部や従業員を騙して個人情報や認証情報を暴露させ、その情報を使って企業データを盗んだり、身代金を要求したりします。

BEC、スピアフィッシングなど

企業のセキュリティチームは、さまざまなデジタル犯罪を阻止するための包括的な戦略を必要としています。このような攻撃には、犯罪者があたかも企業の重役から送られてきたかのように偽装した電子メール、IM、その他の通信を従業員に送信するビジネス電子メール詐欺（BEC）攻撃が含まれます。その目的は、従業員を強要して攻撃者に機密情報を提供させたり、攻撃者が企業システムへアクセスできるようにすることです。スピアフィッシング攻撃では、犯罪者は対象者のオンライン上の投稿やプロフィールを研究し、標的に接近する際の信頼性を高めます。ランサムウェア攻撃も大きな懸念事項です。

サイバー犯罪者を見分けるためにBabel Streetを利用する

Babel Streetのソリューションを利用することで、企業のセキュリティチームがデジタル脅威を発見し、軽減できるようになります。ここでは、Charming Kitten、PHOSPHORUS、Yello Garuda、APT35、APT42.1などのイランの支援を受けたハッキンググループによる持続的なサイバースパイを調査するために、セキュリティチームが取り得る手順を紹介します[1]。

フィッシング詐欺の調査

ハッカーは、ある機関の正当な人物になりすまして、目的のターゲットと信頼関係を築きます。図1のEメールにある「Join Us」リンクは、ハッカーが悪意のあるリンクを送る前にさらに情報を収集しようとする無害なサイトに飛ぶと思われます。しかし、どのようなフィッシングリンクも危険である可能性があります。サイバーセキュリティチームは、Babel Street Secure Accessを使用して、システムやネットワークをハッカーにさらすことなく、潜在的に悪意のあるリンクをテストするための隔離された仮想環境を構築することができます。

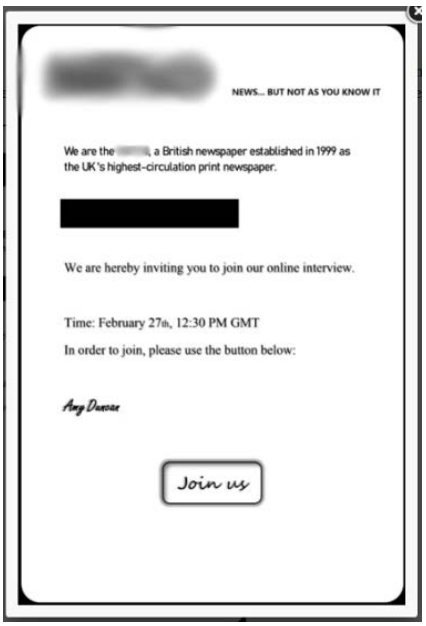

図 *1*：英国の有名メディアからの招待状を装ったフィッシングメール。

ハッカーのテクニックを研究

既知のハッキンググループの関与が疑われる場合、サイバーセキュリティチームはBabel Street Insightsを使用して検索を行えば、グループの手法をより深く理解できます。まず、チームはグループ名の亜種や他のグループとの潜在的なつながりを特定することができます。

そして、ソース、文書タイプ、日付範囲などのフィルターを使って検索を行うことで、ハッカーが以前に使用した戦術、テクニック、手順、ターゲットを明らかにします。

図3は、イランの支援を受けたハッキンググループAPT35とAPT42が、スピアフィッシング作戦で企業、学術機関、ジャーナリスト、NGO、個人の電子メールアカウントをどのように標的にしているかを示しています。

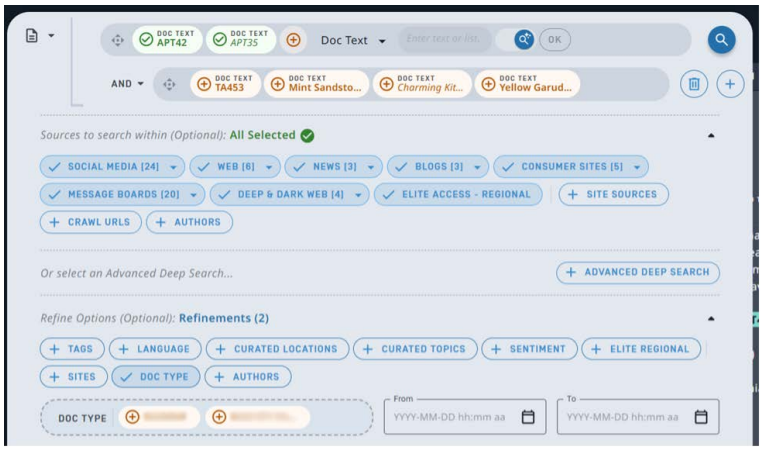

図 2：ハッカーグループの他のバリエーションを特定するための *Insights*ダークウェブ検索

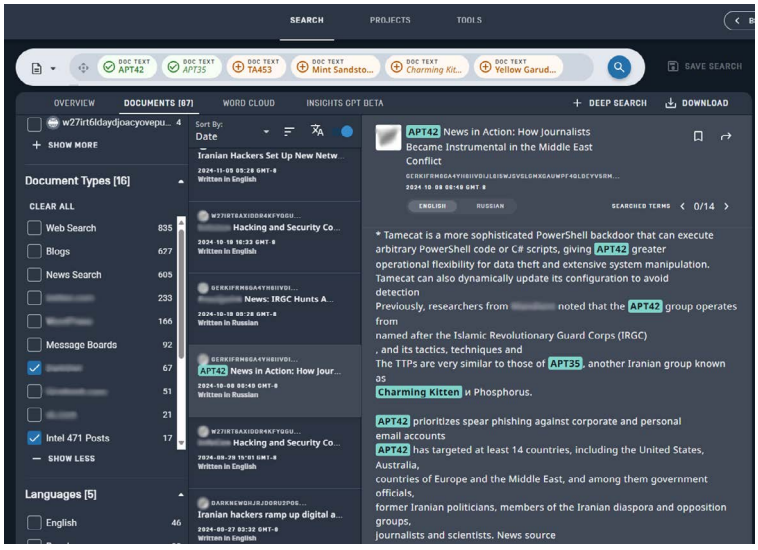

図 3：検索結果からハッカーのテクニックを知る

ハッキングの試みから従業員と知的財産を保護することに関しては、知識が力となります。この場合、サイバーセキュリティチームが国家の支援を受けたハッキングについて深く理解していれば、従業員に対してこうした攻撃に対抗する方法を十分に周知させることができます。

Endnotes

[1] Rozmann, Ofir; Koksal, Asli, et. al., “Uncharmed: Untangling Iran’s APT42 Operations” May 1, 2024, https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations