

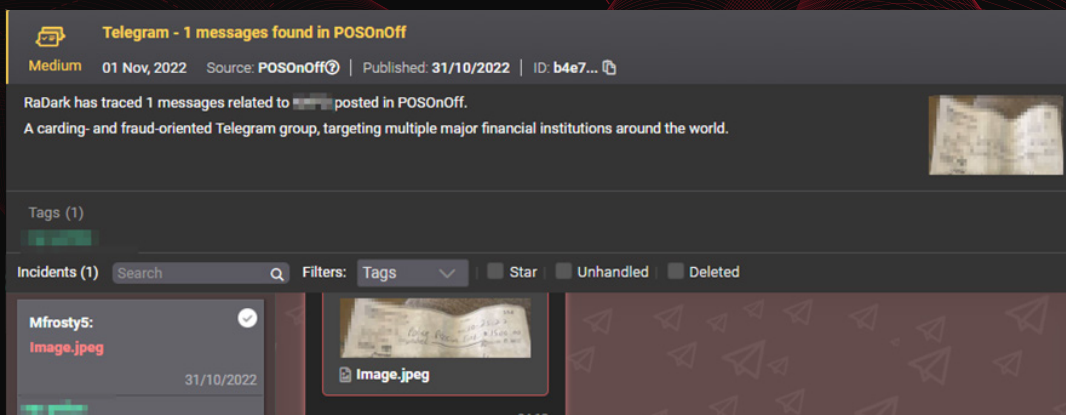
KELAのサイバー犯罪インテリジェンスプラットフォームで 詐欺を未然に阻止

背景

米国の法執行当局も、KELAのサイバー犯罪インテリジェンスプラットフォームを利用している。同プラットフォームには、サイバー犯罪に特化したアタックサーフェス自動監視機能が搭載されているが、この自動監視機能が、詐欺を専門とするTelegramのグループ内で小切手の画像を検知した。この小切手は当局に勤務する警察官から振り出されており、受取人の年金基金の名称には当局の名が含まれていた。当局の名を冠した組織も「監視対象資産」としてKELAのプラットフォームに登録していたため、プラットフォームのテキスト抽出機能が小切手に含まれた当局の名を検知したのだ。

警察官の個人的財務情報が犯罪者の手に わたって生じるリスク

銀行口座の詳細をはじめ、この警察官の個人識別情報（PII）は小切手を売りに出したサイバー犯罪者の手に渡っていた。犯罪者の中には、小切手と個人識別情報をベースに偽造小切手を作成できる者もいる。そういった人物にこの小切手を買取られた場合、偽造小切手を作成された挙句、銀行口座から金銭を引き出される可能性がある。アンダーグラウンドのサイバー犯罪コミュニティで、他の脅威アクターに小切手を売りつけて収益にされることも考えられる。KELAのサイバー犯罪インテリジェンスプラットフォームはこの事態を検知して当局へアラートを自動送信。アラートを受信した当局は、リスクの軽減に向けて直ちに行動を起こした。



さらなるインテリジェンスで調査を深化

01

通知を受けた当局は、問題の小切手を振り出した警察官を特定して直ちに連絡し、悪用されるリスクを回避することができた。

02

その後の調査で、この警察官が路上の郵便ポストに小切手を投函していたことが判明。郵便ポストに投函された小切手が犯罪者の手に渡り、写真を取られたのだ。

03

当局はUSPS（米国郵政公社）に今回の事件を報告した。

04

報告を受けたUSPSは、郵便ポストへの小切手投函について警告を出し、小切手を郵送する場合は直接USPSの支店から発送するよう市民に呼びかけた。

KELAのサイバー犯罪インテリジェンスプラットフォームで、詐欺を未然に阻止

- KELAのサイバー犯罪インテリジェンスプラットフォームに搭載されたリアルタイムな監視機能が、米国の法執行当局に紐づいた小切手を検知してアラートを送信
- 当局はアラートの情報をもとに、小切手を振り出した警察官を特定して悪用のリスクを回避
- 当局は警察官を犯罪から守るとともに、起こりうる詐欺を未然に阻止することに成功

