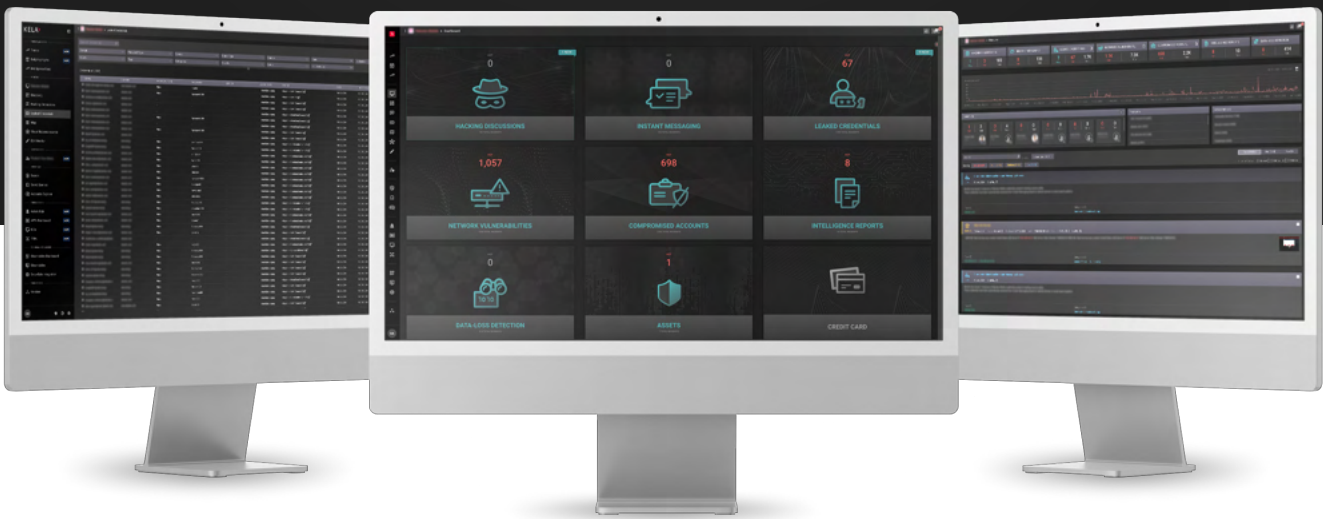


大手電気通信企業がKELAのOCR機能と広範な分析能力を活用し、ランサムウェア攻撃による二次被害を未然に阻止

概要

某大手日系電気通信企業もKELAのサービスを利用する顧客の一社だ。ある日KELAのOCRテクノロジーは、画像の中に同社の重要情報が含まれていることを検知した。

同社は、この画像がもたらしうる情報漏えいリスクを即時に検知し、スピーディな対応へつなげることによって、サイバー攻撃を未然に阻止し、インシデントがもたらしうる二次被害を最小限に抑えることに成功した。



インシデント

KELAの顧客である大手電気通信企業の主要サプライヤーが、ランサムウェア攻撃に見舞われた。その後、このインシデントで侵害されたデータの中に、同社（大手電気通信企業）の情報も含まれていたことが判明したが、この情報は機密保持契約書（NDA）を写した画像に含まれていたため、あやうく検知をすり抜けられる可能性があった。



業界
電気通信



国
日本

ソリューション

- リアルタイムな脅威の監視**

画像に含まれた脅威情報も見逃すことなく検知するKELAのテクノロジーが、サイバー犯罪プラットフォームで侵害の痕跡（IoC）をスキャン。各画像に含まれている文字情報を抽出し、コンテンツを監視する中で、大手電気通信企業のサプライヤーが被ったデータ侵害の証拠が公開されているスレッドを特定した。
- キーワードと組織名を検知**

KELAのテクノロジーに採用されている高度なアルゴリズムが、画像から抽出されたテキストの中に含まれた電気通信企業の名称を検知し、即時にレッドフラグを立ち上げた。
- スピーディなアラート送信&分析**

KELAの自動アラート機能が、電気通信企業のセキュリティチームへアラートを即時に送信。

その一方でKELAのアナリストが詳細な分析を行い、アラートの背景情報と脅威の重大度を評価して同社に報告した。
- 広範なインシデント分析**

さらに、サプライヤーが被ったインシデントによって流出した全ファイルをKELAのアナリストがダウンロードし、電気通信企業と関連のある情報が他に含まれていないかを入念にチェックした。
- 顧客企業の状況に合わせた対応策のアドバイス**

顧客である電気通信企業のデータが流出したことを確認後、KELAの専門家チームは同社に最善となる対応策について助言を行い、スピーディかつ効果的な対応をサポート。



結果

この電気通信企業の情報は、流出した画像に含まれており、検知をすり抜ける可能性もあった。しかし同社はKELAのMONITORモジュールの機能を活用することにより、データ侵害がもたらしうるダメージを最小限に抑えることに成功した。



メリット

このサクセス・ストーリーが示すとおり、KELAの高度な脅威インテリジェンスとインシデント分析能力、OCRを駆使した検知機能は、サイバー脅威に対抗する能動的な防御メカニズムの役割を果たす。つまり企業にとっては、潜在的な脅威の先を行くためのソリューションとして活用できるということだ。



KELAから皆様へ

KELAは、常に進化する脅威情勢の中で組織の皆様へ最高レベルの保護サービスをご利用いただけるよう、常にソリューションを改善・強化しています。

サイバー脅威に先回りした対策を取る手段として、ぜひKELAのサイバー脅威インテリジェンスをご活用ください。

KELAのソリューションの詳細や組織でのユースケースについては、本シートに記載の連絡先までお問い合わせください。