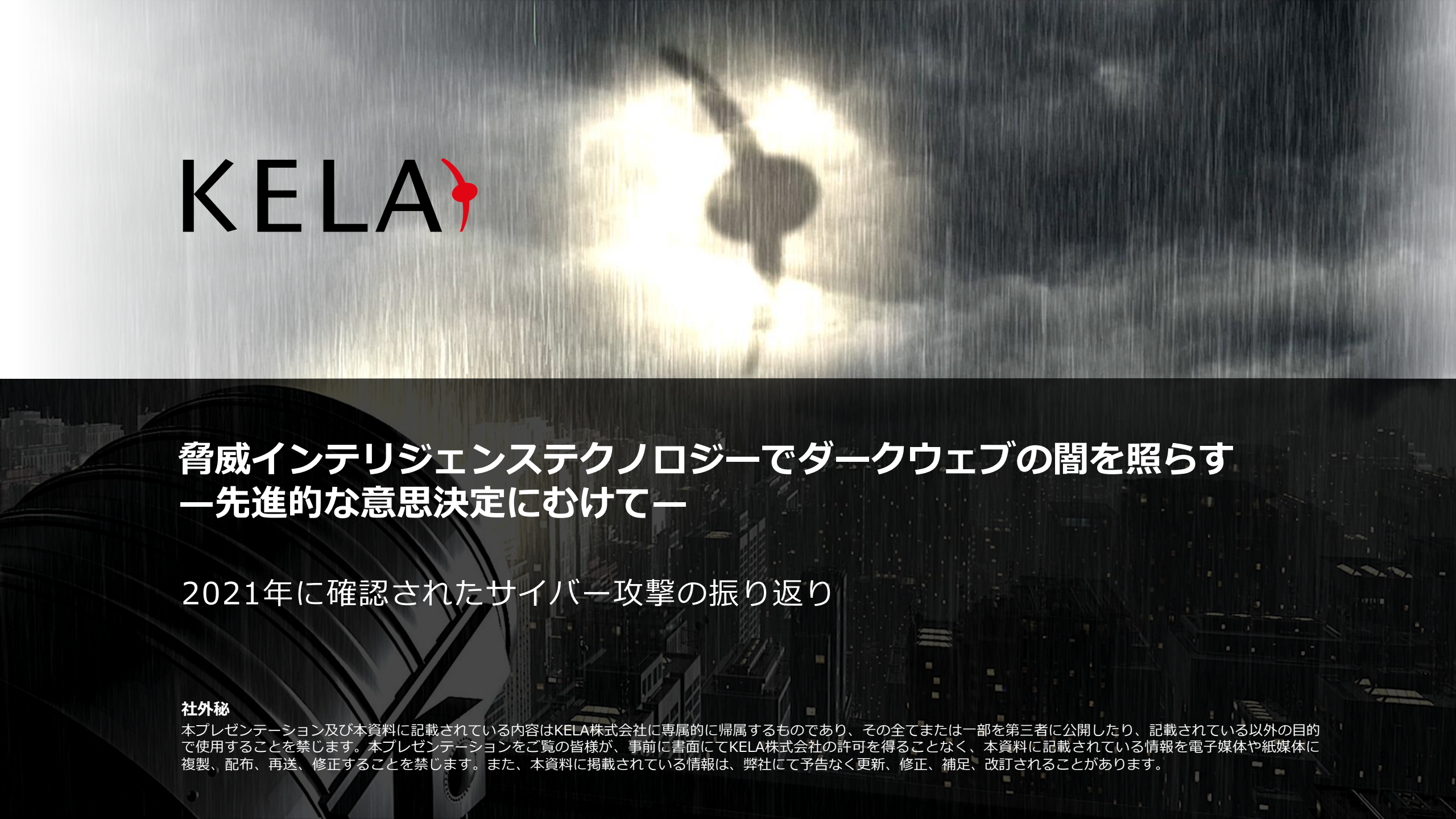


脅威インテリジェンステクノロジーでダークウェブの闇を照らす
ー先進的な意思決定にむけてー

2021年に確認されたサイバー攻撃の振り返り

KELA について

ミッション

あらゆる盲点をカバーする実用的な自動インテリジェンスソリューションをご提供し、アンダーグラウンドのサイバー犯罪社会から「お客様を狙いうる脅威」を無力化できるようお手伝いします。

業界の専門知識

弊社は、ダークウェブに特化した脅威インテリジェンスソリューション＆サービスのプロバイダーとして、厚い信頼と高い評価を受けています。

顧客基盤

世界中の大手企業や名だたる組織、法執行機関をはじめとするお客様に、弊社ソリューションをご利用いただいています。

グローバルな事業展開

イスラエルに本社を置き、米国、日本、英国、シンガポール、その他の国々に拠点を展開しています。

ダークウェブを照らし出すKELAの強み

業界トップのテクノロジー

自動化されたスケーラブルなプラットフォームは、セキュリティ＆インテリジェンス分野に携わる世界中のトップ・プロフェッショナルの日常業務でも活用されており、高い操作性が証明されています。

世界中からの高い信頼

KELAは、自動脅威インテリジェンスソリューションのサプライヤーとして、世界中から高い信頼を受けています。

最高品質のインテリジェンス

アンダーグラウンドのサイバー犯罪社会でお客様を狙う脅威を特定し、攻撃を回避できるようサポートします。

比類なき独自のデータレイク

比類なき過去データを保存したKELAのデータレイクは、EDRやDRP、脆弱性管理、ブランド保護、サプライチェーンの監視、その他様々なサイバーセキュリティ業務を支援する広範かつ包括的なインテリジェンスで構成されています。

深い専門知識

KELAのソリューションとサービスは、イスラエル国防軍諜報部隊と熟練したインテリジェンス専門家の深い専門知識をもとに設計されています。

包括的なサービス

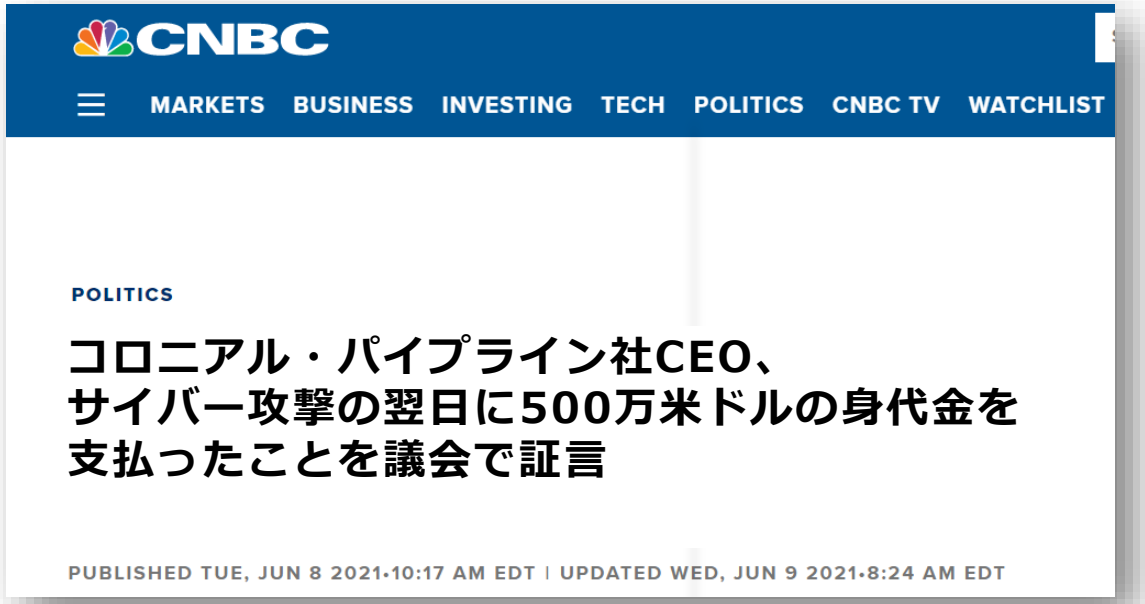
KELAのサイバーインテリジェンスセンター（CIC）が、お客様専用のSWATチームとして活動します。

KELA

2021年に確認されたサイバー攻撃の振り返り

コロニアル・パイプライン社へのサイバー攻撃

インシデントの概要


CNBC

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV WATCHLIST

POLITICS

コロニアル・パイプライン社CEO、サイバー攻撃の翌日に500万米ドルの身代金を支払ったことを議会で証言

PUBLISHED TUE, JUN 8 2021•10:17 AM EDT | UPDATED WED, JUN 9 2021•8:24 AM EDT

DarkSideが、コロニアル・パイプライン社で不使用となっていたVPNアカウントのパスワードを入手。

このVPNアカウントの資格情報を利用して、同社のシステムへリモートでアクセス＆サイバー攻撃に成功。

攻撃者は、アンダーグランドのサイバー犯罪コミュニティで回覧されていた同社VPNアカウントのパスワードを悪用することで、社内ネットワークへの侵入に成功。

攻撃プロセス

ダークウェブでパスワードが流通

資格情報を利用してコロニアル社のシステムにリモートでアクセス

ランサムウエアのインストール＆攻撃開始

コロニアル社が身代金約500万ドルをDarkSideに支払い

KELA

エレクトロニック・アーツ（EA）社への不正アクセス

インシデントの概要

CNN BUSINESS

ハッカーがエレクトロニック・アーツ社に不正アクセス、ゲーム用ソースコードとツールを窃取

By Brian Fung, CNN Business

Updated 1938 GMT (0338 HKT) June 10, 2021

攻撃プロセス

- Slackの資格情報をダークウェブのマーケットで購入
- 購入した資格情報を使ってEA社の社内Slackチャンネルにアクセス＆さらなるデータを入手
- ソースコードを窃取＆同社に対するデータ侵害を公表
- EA社の信用失墜＆ビジネスの一時停止に発展

ハッカーらが、EA社から窃取されたクッキーをダークウェブにて10ドルで購入。

その後このクッキーを利用して、EA社が使用するSlackチャンネルにアクセス。

さらにハッカーらは、Slack上でEA社の従業員を騙してログイントークンを入手し、同社から多数のゲーム用ソースコードを窃取。

このインシデントでは、EA社がゲーム用ソースコードや関連ツールを使用・管理するネットワークへの侵入も行われた。

KELA

ジャイロデータ社へのランサムウエア攻撃

インシデントの概要

攻撃プロセス

- ジャイロデータ社のシステムへのアクセスを入手
- アクターが同社システム内を水平移動して権限を昇格
- ハッカーらが同社システムにランサムウエアをインストール
- 深刻な業務停止に追い込まれたうえ、従業員の個人情報や財務情報にも被害が発生

ジャイロデータ社がDarkSideによるランサムウエア攻撃の被害者となる。

調査の結果、今回の攻撃は某アクターが同社の一部システムに不正アクセスしたことから始まったことが判明。

この不正アクセスで使用された資格情報が、その後ランサムウエアアクターらに売り渡され、ジャイロデータ社のシステムがランサムウエアに感染するに至った。

LUMINT
BY KELA

サブスクリプションのお申込み