



KELA

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 —先進的な意思決定にむけて—

2021年に確認されたサイバー攻撃の振り返り

社外秘

本プレゼンテーション及び本資料に記載されている内容はKELA株式会社に専属的に帰属するものであり、その全てまたは一部を第三者に公開したり、記載されている以外の目的で使用することを禁じます。本プレゼンテーションをご覧の皆様が、事前に書面にてKELA株式会社の許可を得ることなく、本資料に記載されている情報を電子媒体や紙媒体に複製、配布、再送、修正することを禁じます。また、本資料に掲載されている情報は、弊社にて予告なく更新、修正、補足、改訂されることがあります。

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。



2021年に確認されたサイバー攻撃の振り返り



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、アンダーグラウ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



ランサムウェアのインストール & 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

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

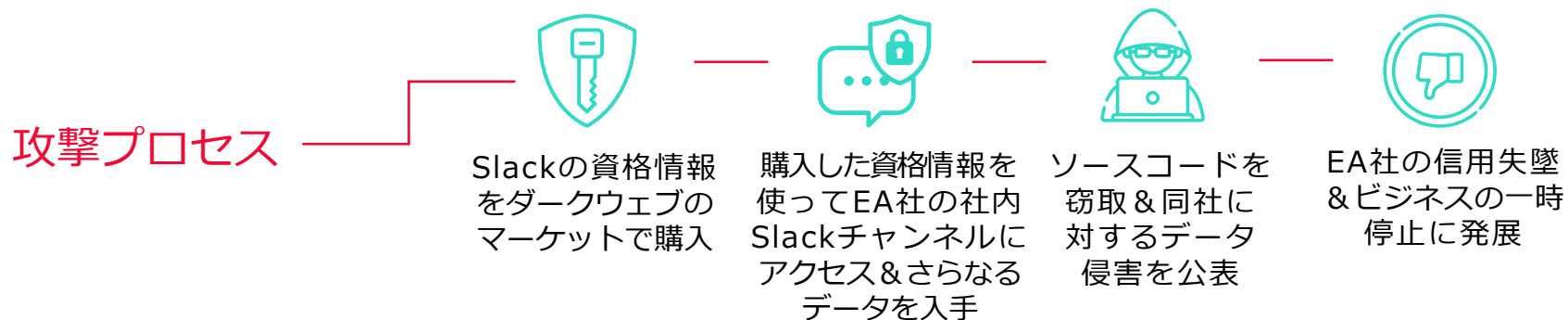


ハッカーらが、EA社から窃取されたクッキーをダークウェブにて10ドルで購入。

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。



ジャイロデータ社へのランサムウェア攻撃

インシデントの概要

ジャイロデータ社がDarkSideによるランサムウェ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、その後ランサムウェ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ェアに感染するに至った。



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ェアをインストール



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

Latest Intelligence

Insights from the dark web at your fingertips.

EXPLORE OUR SOLUTIONS →

Select Categories

- Random Event
- Network Access
- Database Leak
- Threat Update

Clear all

All Geographics

All Sectors

November 15, 2021

Source Type: Hacking Forum

Threat actor korada/nel sells access to a France-based private school of osteopathy

On November 15, 2021, KELA observed the threat actor korada/nel selling access to a France-based private school of osteopathy, with USD5 million in revenue. The actor claimed the access is provided through VPN and RDP and enables to log in to an adminprivileged machine. The actor offered to sell the access for USD400.

Network Access

- Education
- France

November 15, 2021

Source Type: Hacking Forum

Threat actor korada/nel sells access to a Venezuela-based insurance company

On November 15, 2021, KELA observed the threat actor korada/nel selling access to a Venezuela-based insurance company, with USD10 million in revenue. The actor claimed the access is provided through VPN and RDP and enables to log in to an adminprivileged machine. The actor offered to sell the access for USD700.

Network Access

- Financial Services
- Venezuela, Bolivarian Republic Of

November 15, 2021

Source Type: Hacking Forum

Threat actor Alexand7 sells access to a Spain-based company

On November 15, 2021, KELA observed the threat actor Alexand7 selling access to a Spain-based company with over 4000 employees. The actor claimed the access is provided through VPN and enables to log in to a user privileged machine. The actor offered to sell the access for USD15000.

Network Access

- Spain

November 15, 2021

Source Type: Hacking Forum

Threat actor korada/nel sells access to a US-based business consulting firm

On November 15, 2021, KELA observed the threat actor korada/nel selling access to a US-based business consulting firm, with more than USD6 million in revenue. The actor claimed the access is provided through VPN and RDP and enables to log in to an adminprivileged machine. The actor offered to sell the access for USD400.

Network Access

- Professional Services
- United States of America

November 14, 2021

Source Type: Hacking Forum

Threat actor "Alexand7" sells access to a Spain-based company

On November 13, 2021, KELA observed the threat actor "Alexand7" selling access to a Spain-based company with USD150 million in revenue. The actor claimed the access is provided through VPN and enables to log in to a domain adminprivileged machine. The actor offered to sell the access in an auction form, starting with a bid of USD10000.

Network Access

- Spain
- 1 Row Intelligence

November 14, 2021

Source Type: Hacking Forum

Threat actor "Alexand7" sells access to a US-based manufacturing & industrial products company

On November 13, 2021, KELA observed the threat actor "Alexand7" selling access to a US-based company from the manufacturing & industrial

Network Access

- Manufacturing & Industrial Products
- United States of America

Events

3271
ALL TIMES

Locations



mapbox

United States of ...	42%	<div style="width: 42%;"></div>
France	5%	<div style="width: 5%;"></div>
United Kingdom ...	4%	<div style="width: 4%;"></div>
Canada	4%	<div style="width: 4%;"></div>
Germany	4%	<div style="width: 4%;"></div>

Common Sectors

Manufacturing ...	15%	<div style="width: 15%;"></div>
Professional Ser...	15%	<div style="width: 15%;"></div>
Technology	10%	<div style="width: 10%;"></div>
Consumer & Retail	8%	<div style="width: 8%;"></div>
Engineering & C...	7%	<div style="width: 7%;"></div>

サブスクリプションのお申込み

