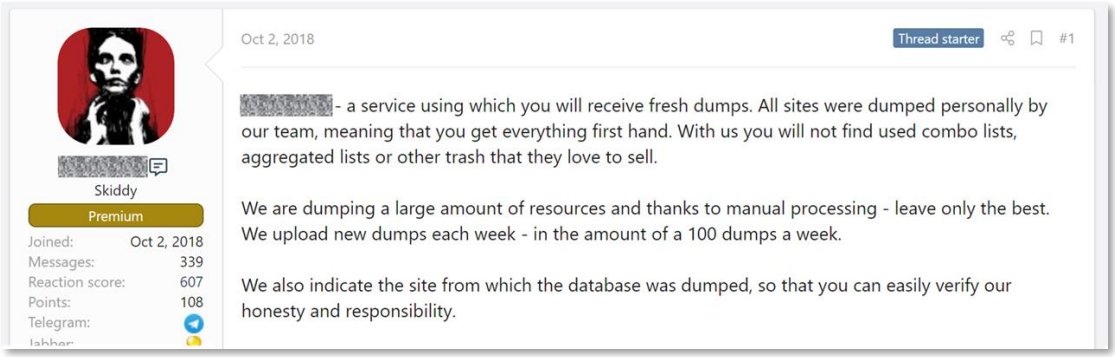
KELA UPDATE

新たな流出データベースをサービスに追加

KELA では、様々なソースを利用してサイバー犯罪者や脅威アクター達の間で交換される情報や会話を監視しております。そしてこの度、**アンダーグラウンドのアクター達（以後「プロバイダー」）がサービスとして提供している流出データベース**を、新たなソースとして追加いたしました。

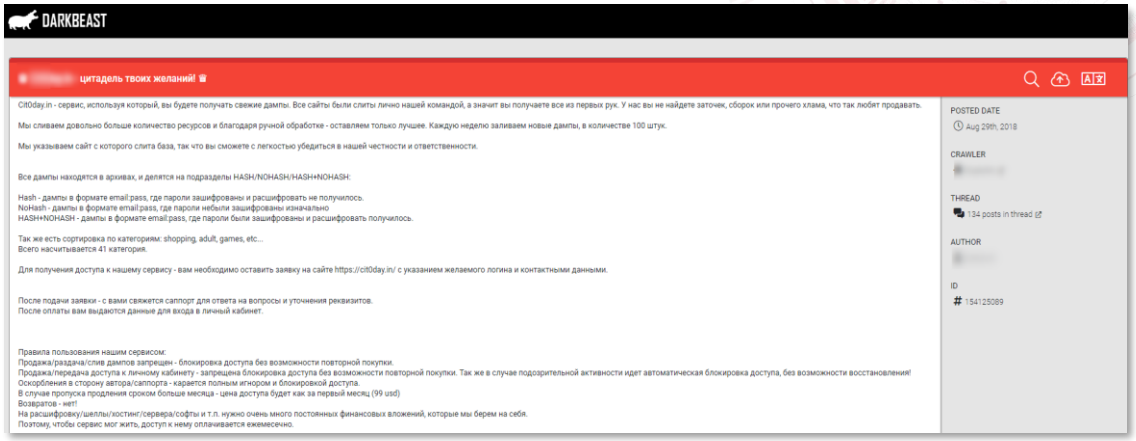
こういったサービスは、脅威アクター達にとっては、労力を使わずスケーラブルに第三者のデータベースを入手できる手段となっています。そして過去 3 年間にわたり、サイバー犯罪のアンダーグラウンドで同サービスを提供している某主要プロバイダーは、ここ最近さらに好調な売り上げを達成しています。現在彼らが販売しているデータサービスには、自らが**侵入したウェブサイト 2 万 3000 件のリストとそこから窃取した認証情報 5 億件が掲載されています。**

脅威アクター達は月額制でこのサービスを購入し、このプロバイダーが日々ウェブサイトを侵害して窃取、処理、解読したデータベースにアクセスしていると考えられます。また、これまでは窃取したデータベースをフォーラムやマーケットで、人手を介して取引する方法が主流でしたが、今回取り上げているサービスモデルでは、絶え間なく増え続ける大量のデータを簡単に取引することが可能になります。こういったサービスを提供するプロバイダーの多くは、他者から入手したデータベースを転売しているのではなく、自らがウェブサイトに侵入して窃取したデータベースを販売していることを謳い文句にする等、自らの商品の独自性をアピールしています。

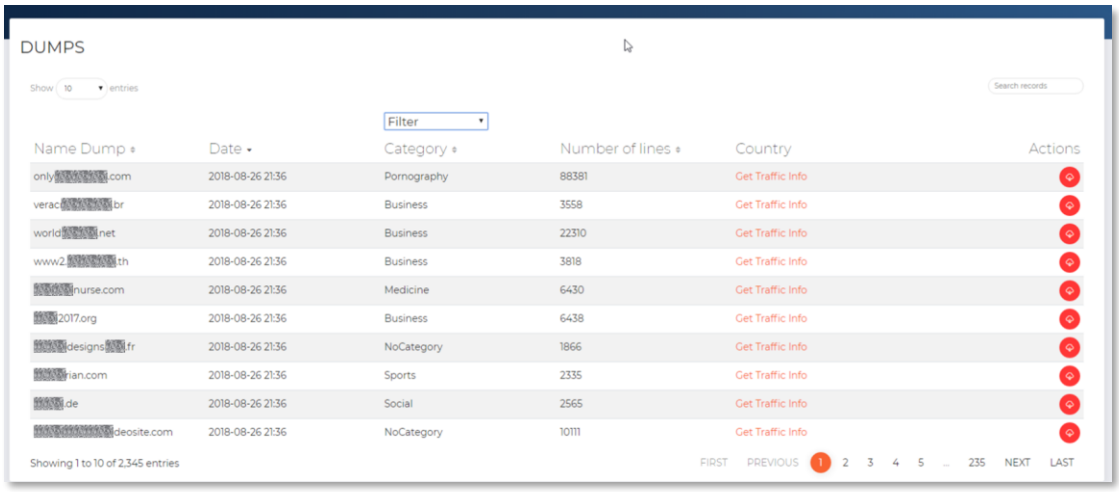


KELA UPDATE

新たな流出データベースをサービスに追加



*流出データベースをサービスとして販売する主要プロバイダーが、サイバー犯罪のアンダーグラウンドフォーラムに掲載した投稿。プロバイダーがフォーラムに掲載した投稿（上図）を、**DARKBEAST** で閲覧して頂けます（下図）。また、オリジナルの投稿はロシア語表記ですが、**DARKBEAST** にてご希望の言語で表示したり、この投稿の全スレッドを閲覧して頂くことも可能です。この投稿を **DARKBEAST** でご覧になる場合は、こちらをクリックしてください。*



上記投稿に記載されていたプラットフォームの実際のスクリーンショット

脅威アクター達は、上述のサービスを活用することで、人手を介さず簡単かつスケーラブルに流出データベースを利用することが可能となります。その結果、様々な戦術を使って認証情報を現金化しようと目論む脅威アクター達が、消費者の認証情報窃取を狙ったアカウントの乗っ取りから、業務上の電子メールの窃取、企業をターゲットとするスピアフィッシングに至るまで、流出情報を様々な攻撃に悪用する恐れがあります。

KELA UPDATE

新たな流出データベースをサービスに追加

この度 KELA は、高度なオートメーション機能と柔軟なウェブ情報収集機能を組み合わせ、アンダーグラウンドのプロバイダーが提供する流出データベースや認証情報に完全自動でアクセスできるサービスのご提供を開始致しました。当社のテクノロジーを脅威アクター達のポータルと統合し、ありとあらゆるデータベースをリアルタイムで自動ダウンロードして当社内のデータベースに保存しております。お客様には、**RADARK および DARKBEAST の両方でこの潤沢なデータベースをご利用いただけます。**

ご質問等がございましたら、info@ke-la.com までお気軽にご連絡くださいませ。