

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。

A screenshot of a forum post from a user named Skiddy. The user's profile is on the left, showing a red and black avatar, the name "Skiddy", a "Premium" badge, and statistics: Joined Oct 2, 2018, 339 messages, 607 reaction score, 108 points, and a Telegram link. The post itself is dated "Oct 2, 2018" and is marked as a "Thread starter". The text of the post describes a service for "fresh dumps" of websites, claiming to be personally dumped by the team and not using aggregated lists. It also mentions uploading new dumps weekly (around 100 per week) and providing site information to verify honesty and responsibility.

Oct 2, 2018 Thread starter #1

Skiddy
Premium
Joined: Oct 2, 2018
Messages: 339
Reaction score: 607
Points: 108
Telegram: @ishher

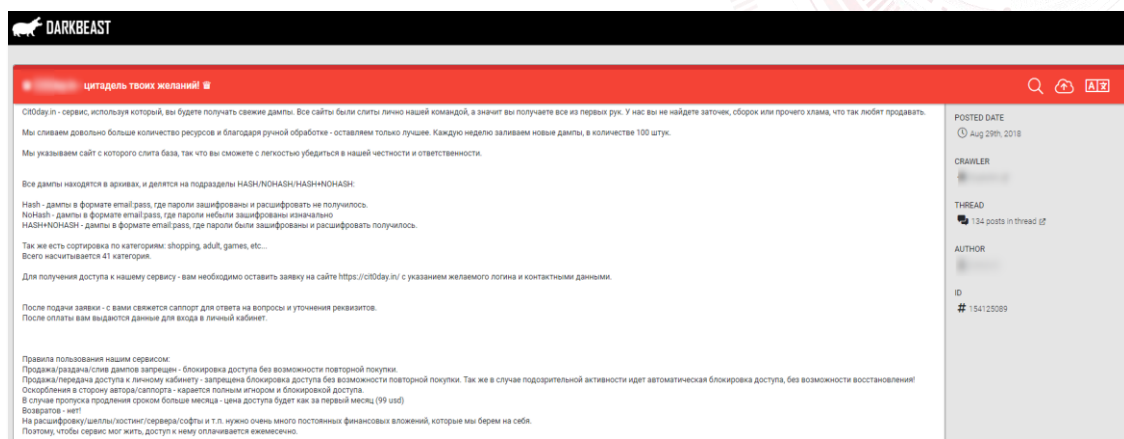
[REDACTED] - a service using which you will receive fresh dumps. All sites were dumped personally by our team, meaning that you get everything first hand. With us you will not find used combo lists, aggregated lists or other trash that they love to sell.

We are dumping a large amount of resources and thanks to manual processing - leave only the best. We upload new dumps each week - in the amount of a 100 dumps a week.

We also indicate the site from which the database was dumped, so that you can easily verify our honesty and responsibility.

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。

Name Dump	Date	Category	Number of lines	Country	Actions
onlybr.com	2018-08-26 21:36	Pornography	88381	Get Traffic Info	
veracbr	2018-08-26 21:36	Business	3558	Get Traffic Info	
worldnet	2018-08-26 21:36	Business	22310	Get Traffic Info	
www2th	2018-08-26 21:36	Business	3818	Get Traffic Info	
nurse.com	2018-08-26 21:36	Medicine	6430	Get Traffic Info	
2017.org	2018-08-26 21:36	Business	6438	Get Traffic Info	
designsfr	2018-08-26 21:36	NoCategory	1866	Get Traffic Info	
nian.com	2018-08-26 21:36	Sports	2335	Get Traffic Info	
de	2018-08-26 21:36	Social	2565	Get Traffic Info	
deosite.com	2018-08-26 21:36	NoCategory	1011	Get Traffic Info	

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パイ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。