DATAVISOR

FRAUDONOMICS:

TIMELY LESSONS ABOUT HOW FRAUD WORKS

This brief takes a look at digital fraud through a new lens. It covers the markets that function in illegality and enable professional fraud rings with the aim of helping you to gain a better knowledge of your adversaries in the fight against fraud.

In the United States, the average data leak costs companies $3.86 million, including an estimated $1.52 million in lost business and the average time for a company to identify and contain an attack is 280 days.

These attacks are staggering, and they represent the supply for an entire economic system that operates in the background of financial crime. The demand, on the other hand, mostly consists of cartels of attackers that purchase leaked information and use it to steal from people, merchants, banks, and more.

Did you know that your social security number might be for sale for less than what you'd pay for a Starbucks cup of coffee?

Welcome to Fraudonomics: The Hidden Side of Online Fraud.

What Are Synthetic and False Identities?

First things first. If the supply consists of sensitive information (e.g. social security numbers, digital or physical IDs, and credit card data) and the demand is a set of attackers willing to buy those items, then the products they generate from it are false identities. Fake identities can either be synthetic or traditional.

- **Synthetic identities** are a combination of authentic and made-up credentials to create a single identity. They are a mix-and-match of personal information components that do not belong to a single person entirely. For example, a synthetic identity might use a valid social security number but with a different first and last name.

- **A traditional false identity** is one in which a single person's entire informational profile is compromised. For example, a data breach can yield a person's name, address, date of birth, SSN, and employer information. The attacker who procures this information might be able to impersonate the victim in various ways.

How Much Do Fake Identities Cost on the Dark Web?

Atlas VPN investigated and found that the going rate for a stolen social security number is just $4. That's a little less than a venti Starbucks latte!

For banking and financial data, the price is a little steeper. For example, a bank account number with a high account balance might cost $25 or so. Credit score may also increase the price, as banks treat customers with a good credit score with more trust. This makes it easier for fraudsters to carry out fraudulent transactions and malicious activity.

How Much Do Credit Card Numbers Cost on the Dark Web?

Like synthetic identities, credit card fraud runs rampant on the dark web. A full credit card number can be purchased for $5 to $110 (debit cards run about the same price).

Interesting fact: Credit numbers with CVV typically cost just $5 more.

Prices can vary widely depending on several factors. For starters, credit cards with higher balances tend to cost less than those with lower balances. Spending limits and credit scores may also influence the price of a credit card number on the dark web.

Unsettling fact: For $600 would-be hackers can enroll in online classes in identity theft.

How Much Do Fraud Attacks Yield?

For most of us, getting such sensitive details might seem like a tremendous feat — one that would certainly be worthy of more than a few bucks.

But hackers are professional fraudsters and steal their data in bulk, so it's not uncommon for just one cyberattack to net millions of records. A large supply helps to keep the cost per record low.

Hackers steal identities for a variety of purposes, from credit card fraud to taking out loans and even intercepting tax refunds. Just how much they can gain from stealing your identity depends on how they intend to use it; however, in the end it's a numbers game for them. If they purchase personal information by the thousands and then start automated or serial attacks, they stand to gain a lot of money in the aggregate.

What Can Fraud Practitioners and Their Teams Learn from These Economic Dynamics?

The best offense against online fraud is a good defense. As companies and their customers learn more about the mindset of a cybercriminal, they can take better steps to protect their data and finances.

1

LESSON ONE:

Online fraud is an organized criminal activity.

Long gone are the days of the solo hacker; instead, today's fraudsters are major cross-border syndicates that engage in fraud at scale.

Legacy fraud prevention tools are insufficient to thwart these fraud attempts because they are unable to look past individual transactions and make sense of batches of events (e.g., applications, payments, and account openings) to detect connections between them and stop at-scale attacks coordinated by fraud rings.

DataVisor's machine learning algorithm stops fraud rings because it uncovers connections between seemingly unrelated events that are invisible to the naked eye. To picture this, imagine being able to get an in-depth view of every attribute that makes up an identity and its relationship to other events and profiles in your database.

2

LESSON TWO:

Identity data is no longer enough to prevent fraud.

Given the vast number of compromised accounts and identities, businesses can no longer rely solely on verifying the identity of their users through their personal information.

Identity data is still relevant and useful in evaluating the risk profile of a potential customer; however, businesses also need to verify that the actual beneficiary of a transaction is the person whose identity they have before them. In other words, third-party fraud (which occurs when a person's identity is used to someone else's benefit) is a clear threat, and advanced fraud systems are required to stop it.

Old-school fraud strategies that only focus on identity verification leave behind large quantities of data created by criminal rings as a byproduct of their activities. For example, when cultivating synthetic IDs, criminals spend up to three years building up fake profiles and nurturing their credit scores. In this process, they leave behind a data trail consisting of hundreds of events (logins, payments, account updates, etc.) that DataVisor leverages by detecting unusual patterns through its patented machine learning technology to stop fraud before these synthetic identities are used to commit attacks.

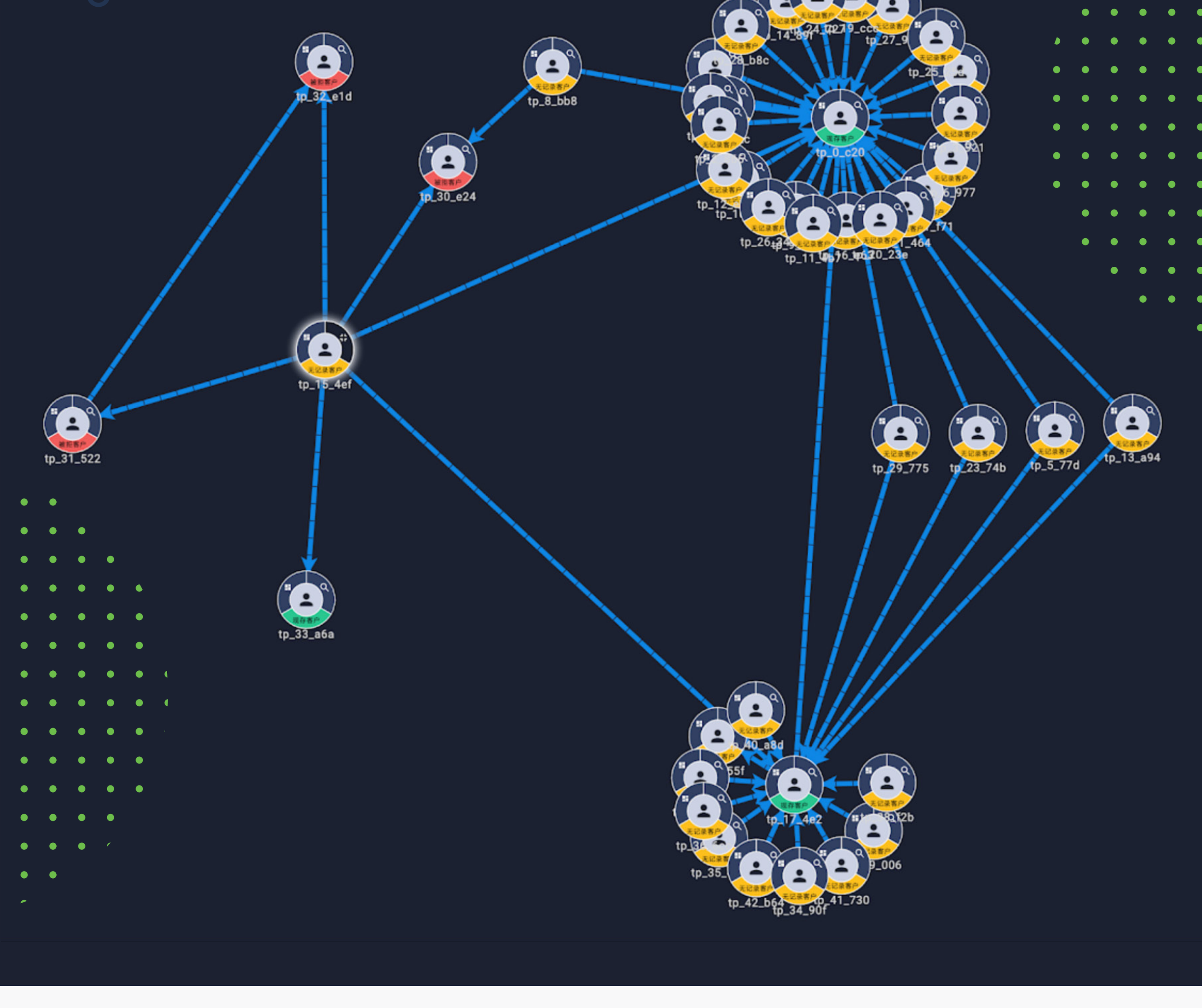
3

LESSON THREE:

It's hard to hit a moving target.

Fraudsters keep evolving and nowadays have access to resources that allow them to innovate in their nefarious ways. This means that businesses need to be able to respond to coordinated attacks in real time.

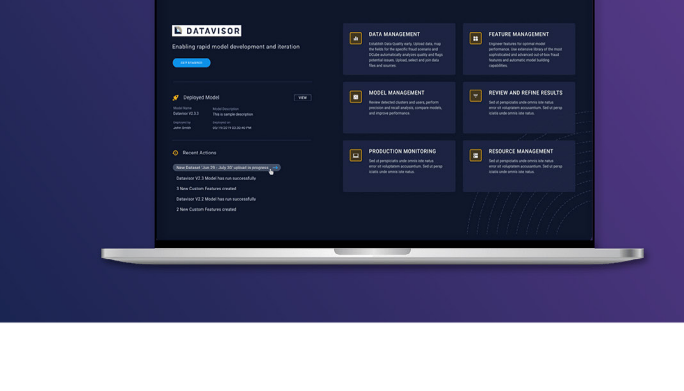
With traditional rules-based systems, it takes fraud teams months to react to a new fraud pattern. Fraud specialists must detect an attack pattern, train models and rules to defeat it, implement them (with the deployment and governance issues that this may bring), and test them in the hope of being effective. By this time, the losses could amount to tens of thousands of dollars, if not more.



Final Thoughts

DataVisor's unsupervised machine learning detects fraud in real time before it happens because it can analyze vast amounts of behavioral data that could not be processed by people and create clusters of users in high-dimensional feature space. This allows our customers to visualize fraud attacks in seconds and react to them on the spot. We even have a One-Click Feature to resolve cases that can save your team hours per incident.

To learn how DataVisor fights against data leaks at scale, request a demo and experience proactive AI-powered fraud prevention today.



Sources:

https://www.usatoday.com/story/news/nation/2014/09/03/stolen-credit-cards-fenced-on-the-dark-web/15020053/, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/, https://www.prnewswire.com/news-releases/people-are-worth-1-285-on-the-dark-web-new-study-by-privacy-affairs-finds-301078215.html, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/01/21/the-economics-of-credit-card-security/

https://www.aarp.org/money/scams-fraud/info-2020/international-fraud.html

https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=3d260b9813f1

https://atlasvpn.com/blog/your-ssn-costs-less-than-a-starbucks-coffee-on-the-dark-web, https://

www.degruyter.com/document/doi/10.1515/rle-2015-0035/html

https://atlasvpn.com/blog/your-ssn-costs-less-than-a-starbucks-coffee-on-the-dark-web,

https://www.techrepublic.com/article/interview-with-a-hacker-gh0s7-leader-of-shad0ws3c/

About DataVisor

DataVisor is the leading fraud and risk management platform powered by transformational AI technology. Using proprietary machine learning algorithms, it restores trust by enabling organizations to stay ahead of even the most sophisticated forms of fraud. DataVisor protects clients across financial services and digital commerce against economic losses and reputational damage by combining advanced analytics and an intuitive SaaS interface with terabytes of data enriched by an extensive partnership network of identity providers.

For more information on DataVisor:

info@datavisor.com

www.datavisor.com

967 N. Shoreline Blvd. | Mountain View | CA 94043

DATAVISOR