



DataVisor Empowers Global Social Platform to Stop ATO and Spam Before Damage Occurs

CLIENT A leading global social commerce platform with over 250 million monthly active users.

CHALLENGE Fraudsters were taking over user accounts in bulk and spamming legitimate users, thereby damaging the client's brand and accelerating their customer churn rate. The client's existing tools could not catch up with new and evolving account takeover (ATO) techniques or detect large groups of coordinated ATO. When fraudsters used legitimate accounts to spam good users, their solutions were not effective at capturing those events—the coverage was limited and the fraud alerts triggered weeks later.

RESULTS



of all spammers captured



of spammers stopped at sign-up

7x

increase in overall detection rates

FRAUD PATTERNS DETECTED

- ▶ Fraudsters took over inactive accounts and edited profile descriptions to include spam domains. They used these accounts to follow large number of users, and gained new followers who would then visit the spam links in their profiles.

Large-scale friend requests with spam links in the profile

Friend Request from Alex

Message

Follow

80 followers, 900 following

Followed a large number of users expecting them to see the profile

About me:

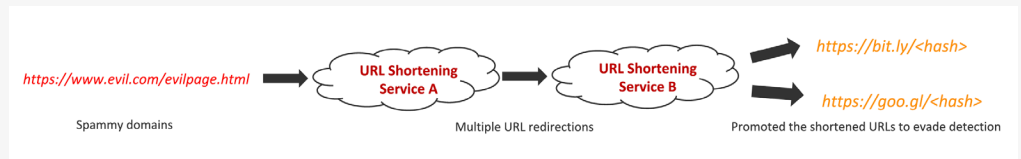
[https://bit.ly/\[hash\]](https://bit.ly/[hash])

Spammy links in the profile descriptions

The link has steal more of my sex photos and videos

- ▶ Attackers disguised spam domains with shortened URLs to avoid blacklisting and used multiple URL redirections to further evade detection.

URL shortener and multiple URL redirections to evade detection



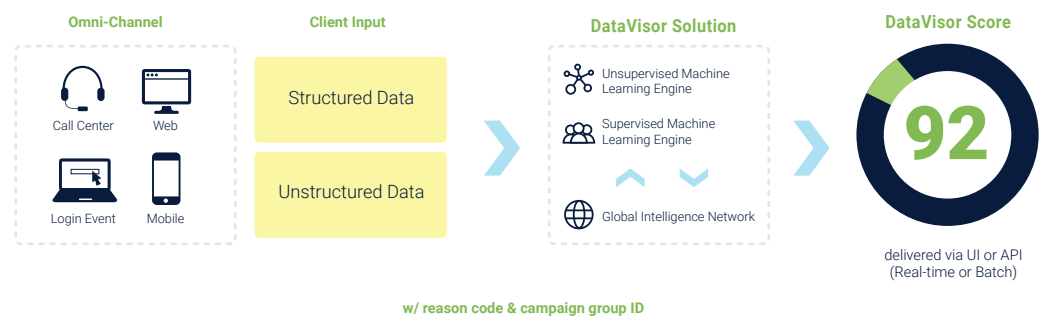
- ▶ Fraudsters used VPN or cloud hosting sites to hide their true locations.
- ▶ Attackers used scripted bots to automate high-frequency events: 90% of observed inter-event intervals were 1-3 seconds.

HOW DATAVISOR HELPED

Using machine learning models to analyze user histories, behavior changes, and suspicious patterns, DataVisor's solutions captured sophisticated, large-scale, coordinated ATO attacks before damage could occur, and prevented spambot attacks by identifying correlations of digital patterns.

HOW DATAVISOR DETECTION WORKS

The DataVisor approach enables proactive fraud protection. While conventional rules or model-based solutions require “pre-knowledge” of how attacks work to be effective, DataVisor’s systems are architected to detect fraud attacks without any historic labels, large datasets, or training time. Drawing on a proprietary UML engine, DataVisor’s solutions accelerate detection by analyzing all accounts and events simultaneously and identifying suspicious clusters of malicious activity—even at the point of account registration. This approach is ideal for finding new and unknown attacks because it does not require historical data and constant retuning.



To enhance detection efforts and enrich decision-making, DataVisor also leverages its Global Intelligence Network (GIN), which is comprised of anonymized non-PII data from over 4 billion protected accounts and 800 billion events across the globe. The GIN contains rich information on digital data such as IP address subnets, prefixes, proxies and data centers, user agent strings, device types and OS, email address domains, and more. Information from the GIN feeds into machine learning algorithms to further improve overall detection.

CONTACT US

If you are interested in learning how DataVisor can help bring your fraud detection to the next level or wish to start a trial to assess your current fraud exposure level, please contact us at: info@datavisor.com or visit us at www.datavisor.com

DATAVISOR

967 N. Shoreline Blvd.
Mountain View | CA 94043