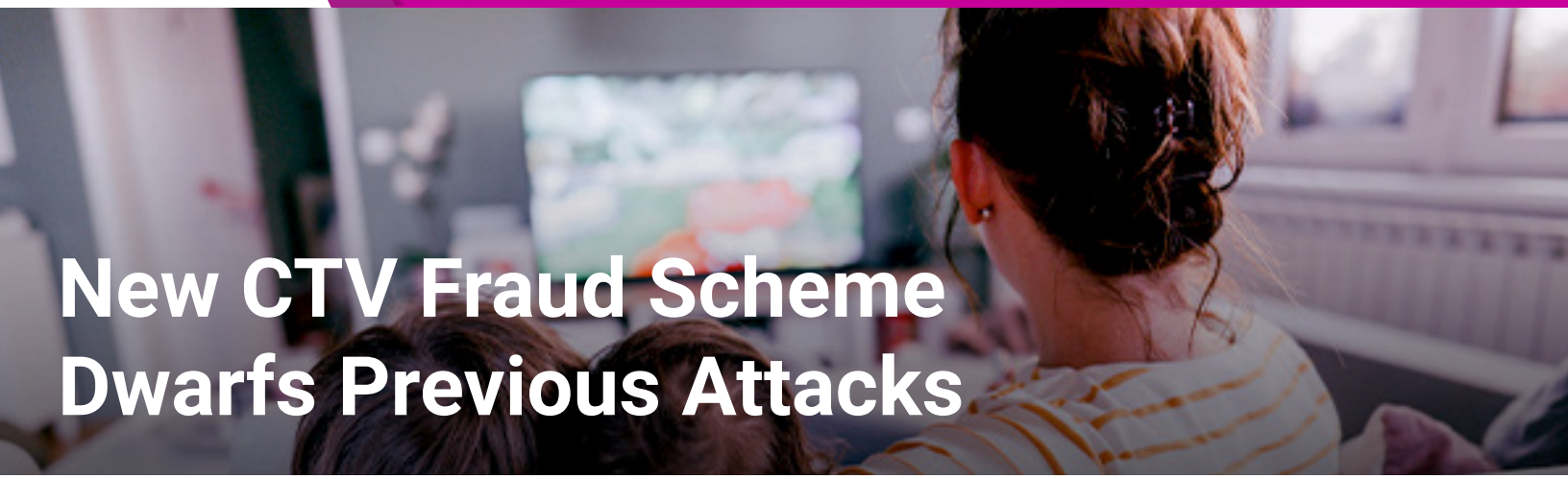
DoubleVerify

FRAUDLAB
FLASH REPORT



New CTV Fraud Scheme Dwarfs Previous Attacks

DV's Fraud Lab recently identified and blocked the biggest CTV fraud scheme to date, ParrotTerra. Before ParrotTerra, this title was held by LeoTerra, a similar server-side ad insertion (SSAI) scheme, which was first identified by DV in July 2020 and later resurged in December 2020, when other companies identified this same scheme using the name "StreamScam."

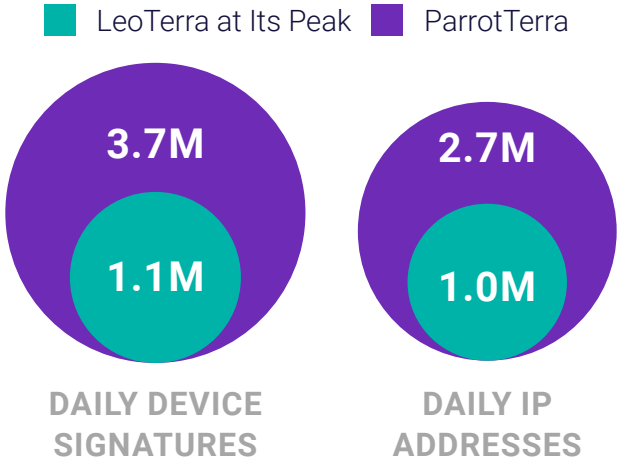
Both ParrotTerra and LeoTerra demonstrate how critical it is to continuously track and monitor emerging fraud threats. During the second half of 2020, LeoTerra exhibited three distinct phases, LeoTerra V1 (July), LeoTerra V2 (early December 2020) and LeoTerra V3 (mid-late December). In the first four weeks of the new year, DV identified two additional variations in LeoTerra (V4 and V5) followed by ParrotTerra — which outstripped any previous SSAI scheme in volume.

ParrotTerra Triples LeoTerra's Scale

ParrotTerra, like other SSAI schemes, worked by generating fake CTV inventory across countless apps, IPs and devices. But ParrotTerra dwarfed other SSAI schemes, including LeoTerra, which had previously spoofed more devices and IPs than any other SSAI scheme. Before DV detected and blocked ParrotTerra, it was scaling as many as 3.7 million device signatures each day and spoofing over 35% more apps than LeoTerra did at its peak.

Identifying and blocking fraud is critical to protecting ad dollars in any environment — but this becomes even more critical in CTV environments, where typical **CPMs are upwards of $20**, *eMarketer* estimates. Every time a scheme increases in size, fraudsters are getting more money for themselves and increasing the financial damage to the advertising ecosystem. Based on its size, ParrotTerra could have defrauded advertisers and publishers of millions of dollars if left undetected.

ParrotTerra Spoofs 3x More Devices and IPs than LeoTerra

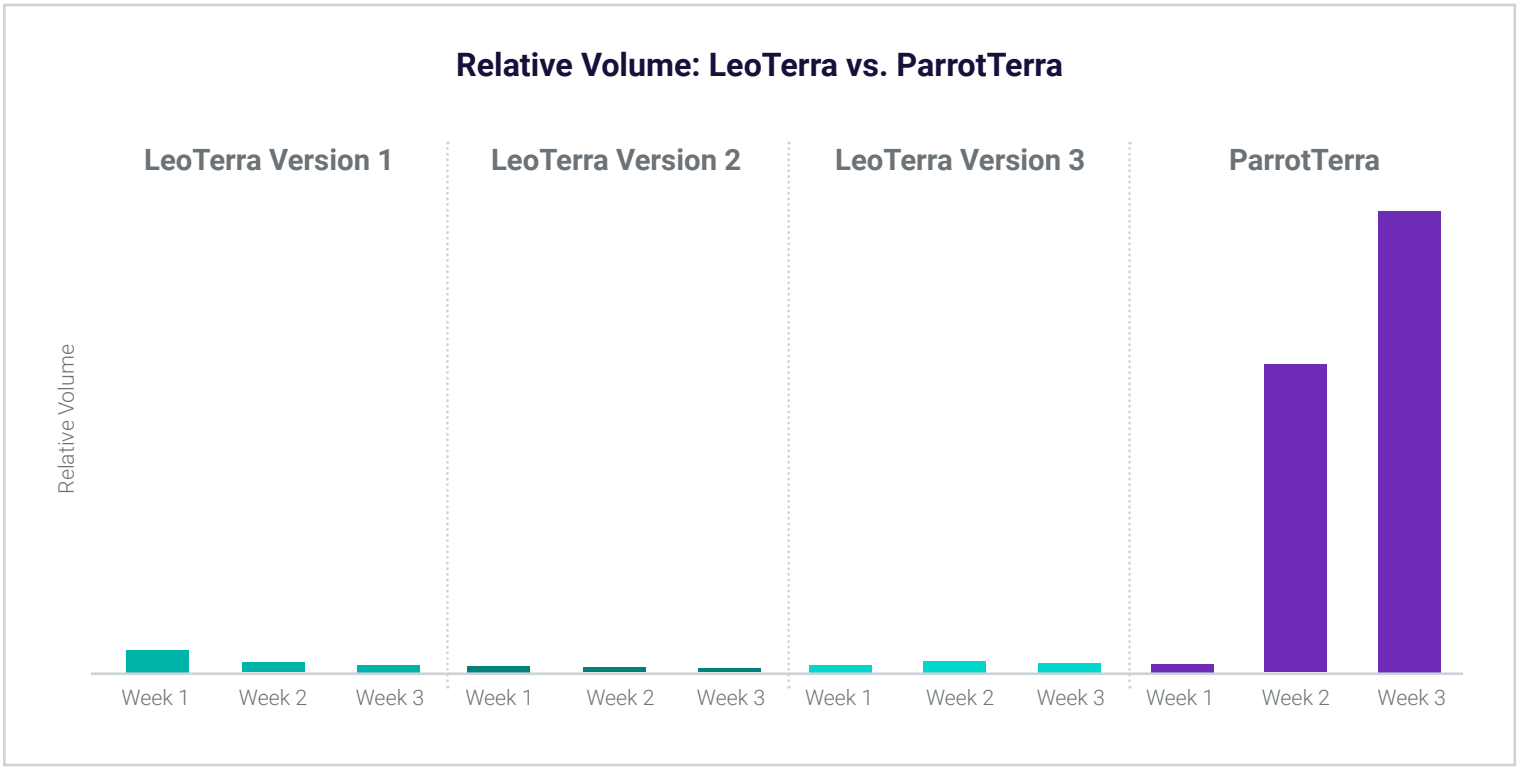


New Tactics in the ParrotTerra Scheme

Although ParrotTerra has many similarities to its predecessors, it also shows how fraudsters are evolving. Traditionally, SSAI schemes have generated impressions at a relatively slow and steady pace.

This trend is exemplified through **LeoTerra**, which underwent three phases in 2020. LeoTerra V1 began in July 2020 and targeted CTV devices only. In December 2020, LeoTerra mutated twice. LeoTerra V2 also targeted CTV but changed its underlying behavior in an attempt to evade detection. LeoTerra V3 shifted to mobile apps after being shut down twice by DV across CTV environments. Throughout each of these shifts, week-to-week, LeoTerra's overall impression volume remained relatively steady, which is typical of most SSAI schemes to date

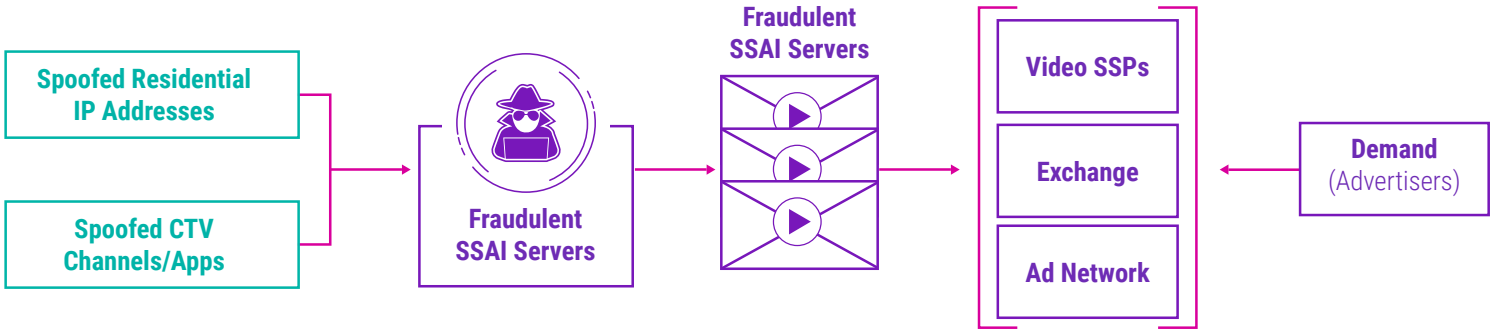
ParrotTerra, however, began by testing its manipulation on a smaller scale before rapidly progressing into high volumes. This is likely an attempt by the fraudsters to try and identify a path that DV would not detect, before they start to scale their operation.



This behavior suggests that SSAI schemes are now looking to act quickly before they're detected. Understanding how fraudsters behave helps the Fraud Lab more accurately predict what to anticipate in future attacks. This approach has paid off. Over the past year, DV has detected nearly 20 various types of schemes, roughly half of which were attempting to avoid detection by manipulating SSAI. DV's ability to track down fraud from its very early phases is a unique advantage.

How SSAI Schemes Work

SSAI fraud schemes, which tend to be an attractive target for fraudsters, typically involve the fraudster spoofing legitimate devices and apps that are not harmful on their own. These schemes take place in three phases. First, the fraudsters gather the details of legitimate users (i.e. the IP addresses or app bundle IDs). Next, they copy these details to mask their activity from being detected. Finally, they use the spoofed details of legitimate users to send fraudulent ad requests into the ecosystem.



DV's History with SSAI Fraud Detection: 2018-Present

DV has been safeguarding our clients against similar and, often more sophisticated, fraud schemes for over two years. At the end of 2018, we identified, flagged and took down the first large-scale SSAI ad fraud scheme, internally dubbed "Colorius." Colorius involved over 400 fake SSAI servers that generated millions of falsified impressions in a very similar manner to ParrotTerra.

Since first identifying Colorius in 2018, DV has uncovered at least eight different SSAI fraud schemes, including ParrotTerra and LeoTerra. While each of these schemes has behaved similarly, also previously noted, ParrotTerra generated over three times the volume of daily impressions.

To learn more about one of the most sophisticated SSAI fraud schemes we've detected recently, you can read the report on MultiTerra, a botnet that, if not caught, could have stolen over $1 million each month from unprotected publishers.

DV's History with CTV Fraud Detection

According to DV data, CTV fraud impressions have more than tripled in 2020 versus 2019 (~220% increase in fraudulent impressions). These figures are determined post-filtration, which includes DV's effective avoidance technology. Without our avoidance technology, these numbers would be exponentially higher.

DV has flagged thousands of CTV apps engaged in CTV ad impression fraud, and we detect over 500,000 individual fraudulent CTV devices every day. If left unchecked, these schemes would siphon off tens of millions of dollars a year — hurting advertisers and publishers alike.

DV Has You Covered

DV offers comprehensive fraud coverage across CTV. Here are the top five ways we keep our customers protected.

1. Sophisticated Tools and Algorithms

DV uses sophisticated tools and algorithms to accurately identify individual impressions that are infected by SSAI fraud. Once identified, DoubleVerify provides maximum brand protection throughout the media transaction — pre and post-bid, across all media channels and device types. We update our internal fraud database globally within 8 minutes and our partner platforms over 100 times per day. Customers can see SSAI fraud reflected in DV performance reporting as bot fraud activity.

2. Proactive Approach

DV has taken a proactive approach to ensure our clients can safely run in SSAI environments and that DV fraud detection appropriately delineates between valid SSAI traffic and fraudulent data center traffic. To do this, we use the following approach.

- DV is engaged with SSAI-related collaborative working groups to develop and implement standards around SSAI ad requests. In 2018, the IAB Tech Lab, with assistance from DV, released specifications for how SSAI ad calls must be made to ensure traffic avoids being categorized as fraudulent data center traffic.
- DV is involved directly with SSAI partners across the industry to advocate for best practices and IAB standards for server-side ad requests.
- DV's advanced look-alike modeling accurately identifies when SSAI technologies are being used — even if the partners have not declared the use of SSAI. Similarly, DV has developed detections to identify when fraudulent actors try to mask activity as an SSAI partner.

3. Continuous Innovation

Recently, DV also released Video Filtering protection, which prevents ads from serving against fraudulent inventory in CTV, mobile and desktop environments. DV's Video Filtering collects data from an ad request, runs it through DV's advanced fraud brand safety and geo detection models and ensures that ads are not served on non-compliant impressions.

4. Trusted Partner Support

DV launched the industry's first CTV Certification for programmatic platforms, designed to protect advertisers from fraud and invalid traffic in the CTV space. With DoubleVerify's CTV Certification program, platforms can ensure that the proper data telemetry is correctly passed to provide optimal pre-bid avoidance and post-bid identification on fraudulent activity.

In order to be certified by DV for CTV targeting, a platform must demonstrate the ability to prevent fraud and IVT by applying DV's pre-bid app and device fraud protection for CTV inventory transactions. DV found that non-certified programmatic CTV saw a fraud rate over 11x higher than CTV transacted through DV-certified marketplaces and approximately 9x higher than publisher-direct buys.To date, certified partners include Amobee, Adelphic, MediaMath, SpotX, The Trade Desk, Verizon Media, VideoAmp and Xandr.

5. The DV Fraud Lab

DV's Fraud Lab employs a rigorous process to evaluate and identify ad fraud across all devices and environments. At any given time, we are monitoring hundreds of data points on every impression, analyzing traffic patterns and leveraging numerous human-tuned algorithms to identify anomalies across different devices and media types.

Let's Build a **Better Industry®**

Neutralizing emerging fraud schemes demonstrates our commitment to power the new standard of marketing performance across devices, formats and ad delivery platforms, offering digital advertisers clarity and confidence in their digital investment.

Should you have questions about this fraud scheme, please reach out to your DV account manager.