DoubleVerify

**FRAUD**LAB

VIPERBOT

# New Fraud Scheme Redirects Verification Tags to Siphon CTV and Mobile Video Ad Spend

**DV Fraud Lab Researchers:** Arik Nagornov, Yuval Rubin, Lia Bader

DoubleVerify's Fraud Lab recently identified a new fraud scheme, ViperBot, that is attempting to steal over $8M from advertisers each month. The scheme works by stripping and redirecting verification tags, which allows fraudsters to evade detection and spoof premium video inventory on both CTV and mobile apps.

Although ViperBot is presently active, its peak activity occurred over the busy holiday season between Q4 2021 and Q1 2022. During this time, there were spikes when ViperBot spoofed up to 85 million requests a day.

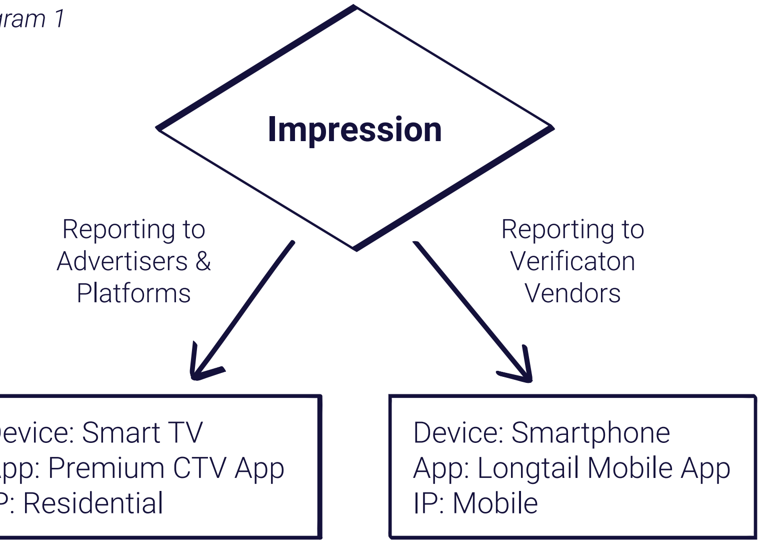
## How ViberBot Operates: A New Level of Sophistication

When an impression renders, an ad tracking pixel fires reporting to an ad server while a verification pixel fires reporting to verification vendors. Fraudsters use "verification stripping" to remove verification tags and interrupt network calls between an ad server and measurement provider.

This method, however, typically results in reporting discrepancies between the ad server and verification provider. With ViperBot, fraudsters have introduced a new layer of sophistication in an effort to evade detection. Rather than removing verification tags entirely, the fraudsters built an elaborate system that redirects verification calls through real devices.

As a result, verification providers and advertisers are getting different data, as shown in *Diagram 1*. Advertisers receive spoofed information while verification providers see data about a real app/device – making that data appear legitimate.

*Diagram 1*



## The ViperBot Workflow

The fraudsters behind ViperBot execute their scheme in three steps:

1. The scheme begins with spoofing CTV and mobile inventory by generating falsified ad requests through counterfeit server-side ad insertion (SSAI) servers.
2. Then the fraudsters strip out verification tags.
3. Finally, they reinsert the stripped tags inside cheap ad slots running on real devices in an attempt to hide the scheme.

Because the ad calls in ViperBot come from real devices, verification vendors are more likely to treat the traffic as legitimate. Although ViperBot ultimately affected verification tags from DV, IAS, Pixalate, Oracle Moat and others, DV quickly detected and mitigated the scheme – ensuring protection for DV customers.

## From Verification Stripping to Redirecting: A Three Step Evolution

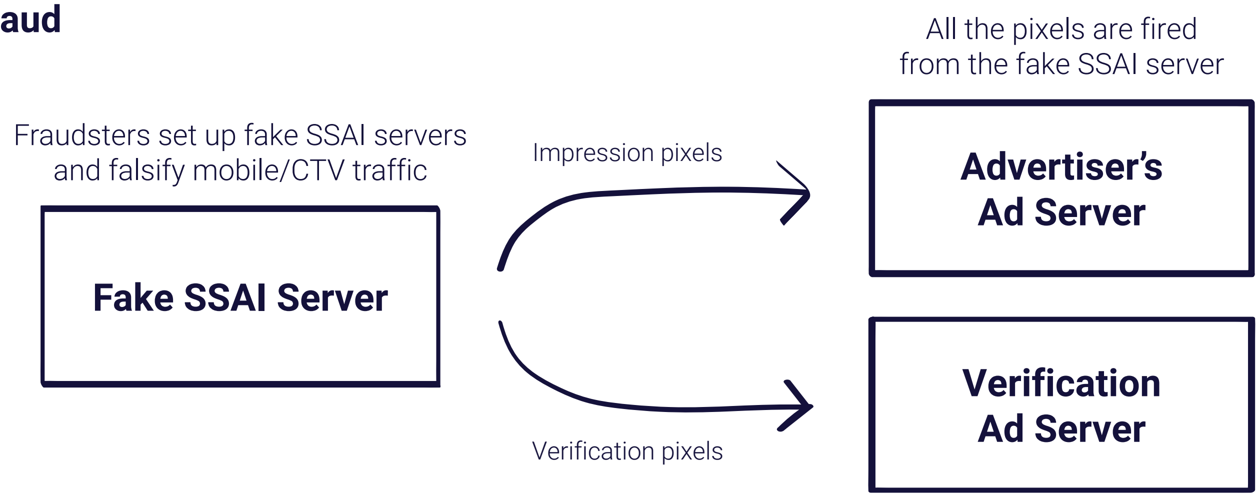
The three steps ViperBot uses to carry out their scheme are an evolution of verification stripping.

### Step 1, The Baseline: Spoofing Inventory Without Verification Stripping

A very common approach to CTV and mobile fraud includes **SSAI manipulation**. In these types of schemes, fraudsters set up counterfeit SSAI servers and falsify premium inventory across different apps, IPs and devices. Fake SSAI servers fire both impression pixels (i.e. the reporting to advertisers and platforms) and verification pixels (i.e. the reporting to verification vendors), as shown in *Diagram 2*. This makes it relatively easy for verification vendors to detect the spoofed inventory. In fact, DV has been protecting its clients against similar fraud schemes for years.

**SSAI Fraud**

*Diagram 2*

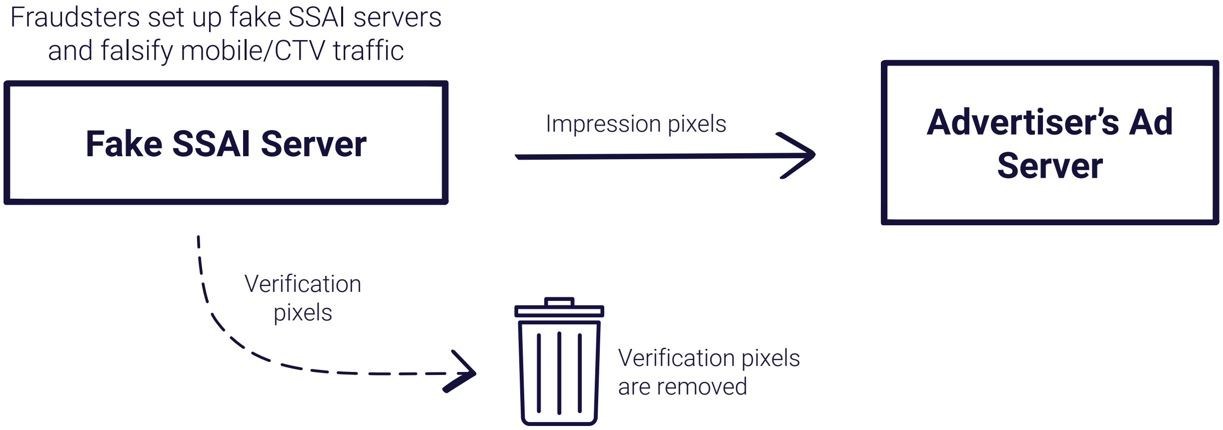


### Step 2, The Introduction of Verification Stripping: Hiding Malicious Activity

In order to hide their fraudulent activity, **fraudsters introduced verification stripping**, where they remove verification pixels to avoid monitoring and detection from verification vendors. The problem with this practice, though, is that it causes measurement discrepancies. Verification providers and ad servers measure a different number of impressions because the verification pixel is removed. *Diagram 3* illustrates this practice, which DV has also been protecting its clients against for over four years.

## Verification Stripping

*Diagram 3*

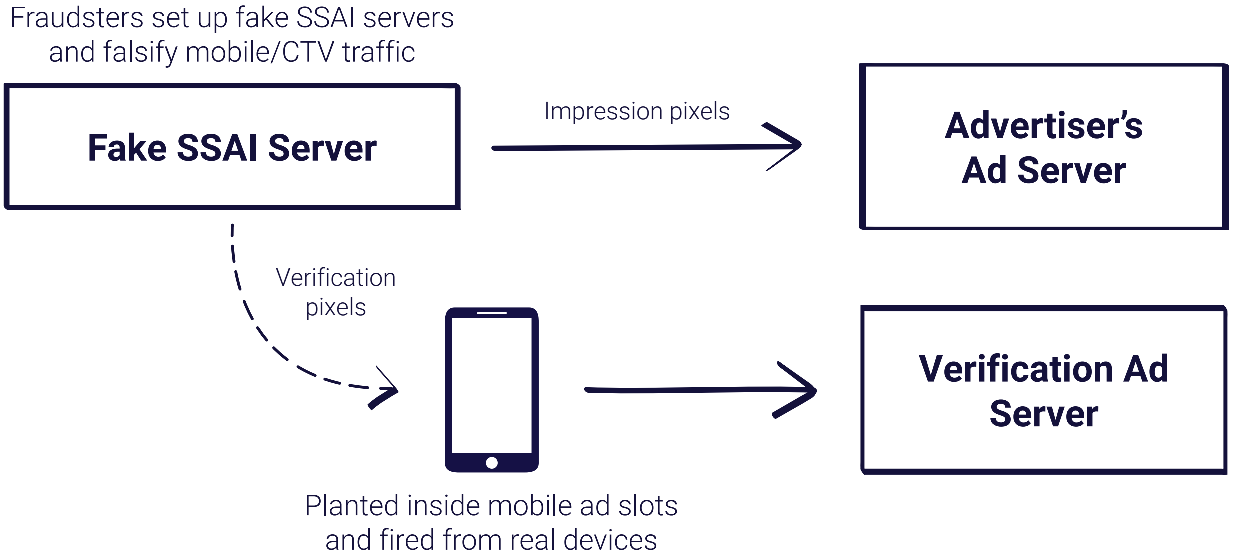

Fraudsters set up fake SSAI servers and falsify mobile/CTV traffic
Fake SSAI Server
Impression pixels
Advertiser's Ad Server
Verification pixels
Verification pixels are removed

### Step 3, The Next Level of Verification Stripping: Using Real Devices to Evade Detection

Because sophisticated verification providers, such as DV, can detect standard verification stripping, the ViperBot fraudsters were motivated to take their scheme to the next level. These fraudsters are not only removing verification tags from the ad being delivered, they're also reinserting the tags inside cheap ad slots – running on real devices – in an attempt to prevent detection. Because the ad call is coming from a real device, verification vendors are more likely to treat the traffic as legitimate. *Diagram 4* depicts the extra effort taken by the fraudsters to manipulate advertisers and verification companies.

## ViperBot

*Diagram 4*


Fraudsters set up fake SSAI servers and falsify mobile/CTV traffic
Fake SSAI Server
Impression pixels
Advertiser's Ad Server
Verification pixels
Verification Ad Server
Planted inside mobile ad slots and fired from real devices

## A Deep Dive Into ViperBot

The ViperBot fraudsters execute their verification redirection through a list of interchangeable domains that share the same SSL certificate (a digital certificate that authenticates a website's identity). During the third step of their scheme, they use these domains to redirect pixels through real devices so that the traffic appears legitimate.

Notably, one person owns several of the domains, based on publicly available information. *Image 1* depicts a partial list of ViperBot-involved domains identified by the DV Fraud Lab.

### Partial List of ViperBot-Involved Domains Identified by the DV Fraud Lab

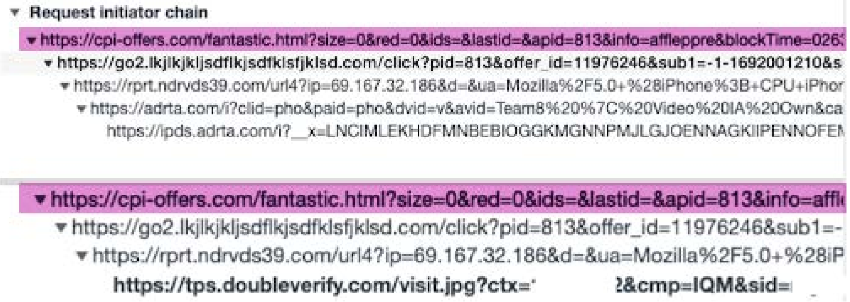
- **alitd**v2vserv.com
- **amity**v2vserv.com
- **germvid**v2vserv.com
- **vudha**v2vserv.com
- ctv.media
- ztvava.com
- junnya.com
- ndrvds.com
- ndrvds23.com
- ndrvds25.com
- ndrvds27.com
- ndrvds29.com
- ndrvds30.com
- ndrvds32.com
- ndrvds35.com
- ndrvds37.com
- cpi-offers.com
- lkjlkjkljsdflkjsdfklsfjklsd.com

*Image 1*

## How Verification Redirection Works on a Technical Level

The scenario below outlines an example of how verification redirection works.

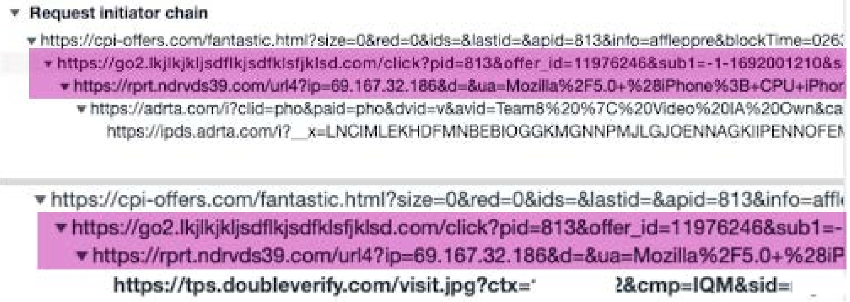
1. Telemetry collected by DV suggests the fraudsters gain access to mobile inventory facilitated by cpi-offers.com where they reinsert the misdirected verification pixels.



```
▼ Request initiator chain
  ▼ https://cpi-offers.com/fantastic.html?size=0&red=0&ids=&lastid=&apid=813&info=affleppre&blockTime=026:
    ▼ https://go2.lkjlkjkljsdflkjsdfklsfjklsd.com/click?pid=813&offer_id=11976246&sub1=-1-1692001210&s
      ▼ https://rprt.ndrvds39.com/url4?ip=69.167.32.186&d=&ua=Mozilla%2F5.0+%28iPhone%3B+CPU+iPhor
        ▼ https://adrta.com/i?clid=pho&paid=pho&dvid=v&avid=Team8%20%7C%20Video%20IA%20Own&ca
            https://ipds.adrta.com/i?__x=LNCIMLEKHDFMNBEBIOGGKMGNNPMJLGJOENNAGKIIPENNOFEN

  ▼ https://cpi-offers.com/fantastic.html?size=0&red=0&ids=&lastid=&apid=813&info=affl
    ▼ https://go2.lkjlkjkljsdflkjsdfklsfjklsd.com/click?pid=813&offer_id=11976246&sub1=-
      ▼ https://rprt.ndrvds39.com/url4?ip=69.167.32.186&d=&ua=Mozilla%2F5.0+%28iP
          https://tps.doubleverify.com/visit.jpg?ctx='          2&cmp=IQM&sid=
```

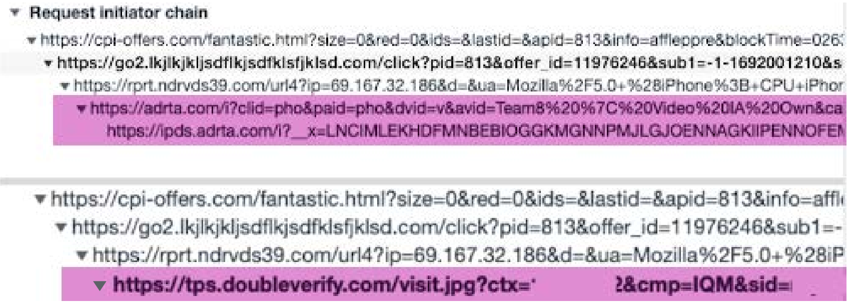
2. The calls are routed through multiple hops to obfuscate the path taken. Examples include:
   a. A gibberish domain such as **lkjlkjkljsdflkjsdfklsfjklsd.com**
   b. One of the multiple domains operated by the fraudsters such as **ndrvds[##].com**



```
▼ Request initiator chain
  ▼ https://cpi-offers.com/fantastic.html?size=0&red=0&ids=&lastid=&apid=813&info=affleppre&blockTime=026:
    ▼ https://go2.lkjlkjkljsdflkjsdfklsfjklsd.com/click?pid=813&offer_id=11976246&sub1=-1-1692001210&s
      ▼ https://rprt.ndrvds39.com/url4?ip=69.167.32.186&d=&ua=Mozilla%2F5.0+%28iPhone%3B+CPU+iPhor
        ▼ https://adrta.com/i?clid=pho&paid=pho&dvid=v&avid=Team8%20%7C%20Video%20IA%20Own&ca
            https://ipds.adrta.com/i?__x=LNCIMLEKHDFMNBEBIOGGKMGNNPMJLGJOENNAGKIIPENNOFEN

  ▼ https://cpi-offers.com/fantastic.html?size=0&red=0&ids=&lastid=&apid=813&info=affl
    ▼ https://go2.lkjlkjkljsdflkjsdfklsfjklsd.com/click?pid=813&offer_id=11976246&sub1=-
      ▼ https://rprt.ndrvds39.com/url4?ip=69.167.32.186&d=&ua=Mozilla%2F5.0+%28iP
          https://tps.doubleverify.com/visit.jpg?ctx='          2&cmp=IQM&sid=
```

3. A domain operated by the fraudsters (such as ndrvds[##].com) fires verification pixels that were previously stripped from falsified ad requests.



```
▼ Request initiator chain
  ▼ https://cpi-offers.com/fantastic.html?size=0&red=0&ids=&lastid=&apid=813&info=affleppre&blockTime=026:
    ▼ https://go2.lkjlkjkljsdflkjsdfklsfjklsd.com/click?pid=813&offer_id=11976246&sub1=-1-1692001210&s
      ▼ https://rprt.ndrvds39.com/url4?ip=69.167.32.186&d=&ua=Mozilla%2F5.0+%28iPhone%3B+CPU+iPhor
        ▼ https://adrta.com/i?clid=pho&paid=pho&dvid=v&avid=Team8%20%7C%20Video%20IA%20Own&ca
            https://ipds.adrta.com/i?__x=LNCIMLEKHDFMNBEBIOGGKMGNNPMJLGJOENNAGKIIPENNOFEN

  ▼ https://cpi-offers.com/fantastic.html?size=0&red=0&ids=&lastid=&apid=813&info=affl
    ▼ https://go2.lkjlkjkljsdflkjsdfklsfjklsd.com/click?pid=813&offer_id=11976246&sub1=-
      ▼ https://rprt.ndrvds39.com/url4?ip=69.167.32.186&d=&ua=Mozilla%2F5.0+%28iP
        ▼ https://tps.doubleverify.com/visit.jpg?ctx='          2&cmp=IQM&sid=
```

## DV Has You Covered

Advertisers working with DV are protected from SSAI and verification stripping schemes like ViperBot. DV offers comprehensive fraud coverage across both CTV and mobile devices. Here are the top five ways DV keeps the ecosystem 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, DV provides maximum brand protection throughout the media transaction — pre and post-bid, across all media channels and device types. DV updates its internal fraud database globally within 8 minutes and its 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 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, DV uses the following approach.

- DV engages 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 works 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

DV Video Filtering provides comprehensive protection for schemes such as ViperBot that target video; it works by preventing ads from serving on fraudulent inventory in CTV, mobile and desktop environments even when blocking is not available. DV 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 Targeting Certification** for programmatic platforms — designed to protect advertisers from fraudulent and invalid traffic in the CTV space. With DV's CTV Targeting 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 Adtheorent, Amobee, Adform, Adelphic, Beeswax, Hawk, MediaMath, Quantcast, SpotX, Tremor Video, The Trade Desk, Unruly, VideoAmp, Xandr and Yahoo!.

## 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, DV's Fraud Lab monitors 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 making the digital advertising ecosystem stronger, safer and more secure.

**To learn more about our fraud solutions and how we help advertisers protect their brands and publishers protect their inventory, reach out to sales@doubleverify.com.**