White Ops

CTV DEVICE IMPER-SONATION:

THE RACE BETWEEN FRAUDSTERS & DEFENDERS

NOVEMBER 2019

WHITEOPS.COM

WHITE PAPER

INTRODUCTION:

INTRODUCTION

It's the case all over: as soon as money begins to pour into a new marketplace, fraudsters looking to make a quick buck will show up and do whatever they can to steal away a piece of the pie before they get noticed and driven away. And it's the responsibility of the people who were there before to find ways to block the bad guys.

The rise of the connected TV (CTV) marketplace has followed this pattern, too. According to eMarketer, more than half of programmatic video spending in 2018 was on CTV/OTT platforms and services, and the total spend on CTV ads was expected to nearly double within the next three years.

For our part, the White Ops platform has seen a spike in the number of CTV-based bid opportunities. Between Q1 of 2018 and Q1 of 2019, the CTV footprint has jumped 1,300%, with a further rise expected. (For context, White Ops currently observes more than 100 billion CTV-based bid opportunities per month.)

The race between the fraudsters and the CTV defenders has begun. This paper will examine one common type of CTV fraud—device impersonation—and how it works, as well as how to ensure that the defenders win this race. We'll look at a real-life example of device impersonation that the White Ops Threat Intelligence team spotted in the wild, and we'll offer insight into how White Ops can protect against it.

THE RACE

WHAT IS DEVICE IMPERSONATION? IVT TAXONOMY:

FALSE REPRESENTATION

DEFINITION: AN ACTUAL AD IS RENDERED TO A DIFFERENT DEVICE THAN THE ONE REQUESTING.

THE RACE

Device impersonation, also known as device spoofing, is a fraud tactic in which ad requests are faked to look like they're coming from CTV devices, but the ads that are then served aren't shown on real CTV devices to real people. Since CTV is a relatively new environment for advertisers, fraudsters and defenders are racing against each other to develop tactics and technologies to carry out their goals.

CTV is a fragmented ecosystem with a variety of device manufacturers, ad platforms, SSAI services, and content stores that all come together. The fragmented ecosystem, along with uncertain industry best practices, is making it possible for fraudsters to employ basic, unsophisticated techniques through device impersonation.

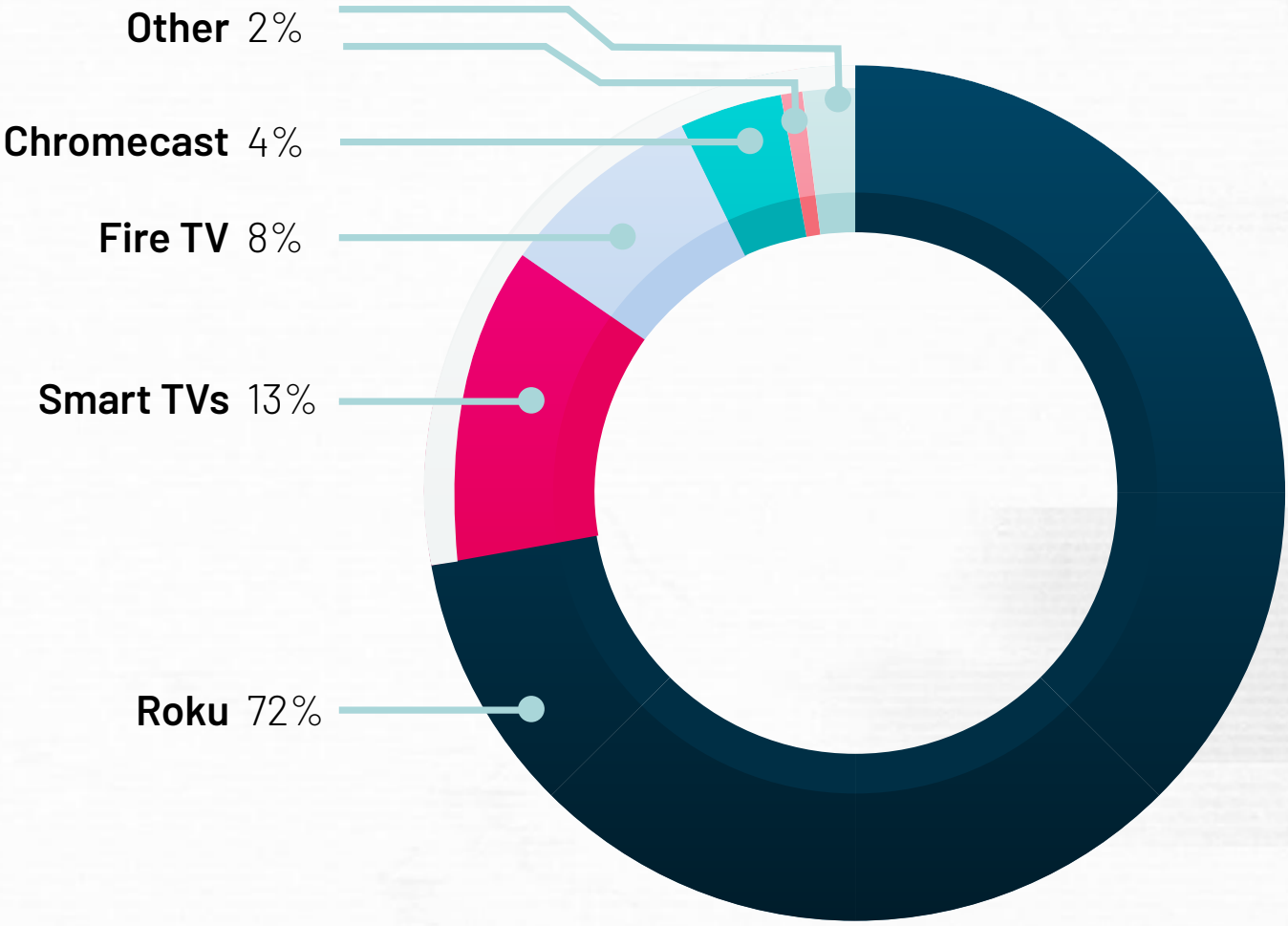
Many ads on CTV devices are delivered using server-side ad insertion (SSAI), making fraud a challenge to detect: all of the requests appear to be coming from a single IP address. To an ad server receiving tracking information, the reports look similar to classic fraud techniques, but SSAI is a complex system used to attach ads to content legitimately, so it's not as simple as blacklisting the IP address from which the requests originate. (We will explore SSAI spoofing in greater detail in a later report.)

Even though CTV platforms are closed systems, fraudsters are able to fake the entire system by spoofing the devices and the apps. This is beyond the control of the individual device stores or the app publishers.

THE RACE-TRACK

As of today, this is the breakdown of CTV devices that we see within the White Ops platform:

DEVICE DISTRUBUTION



This breakdown, as noted above, covers more than 100 billion CTV-based bid opportunities each month.

THE RA-CERS

The Fraudsters' Race

Why is device impersonation a problem in CTV?

Because CTV is such a new environment, there's a broad variety of standards and platforms on which advertisers are trying to get their content. Without a single clearinghouse like the Google Play Store or Apple's App Store to work from, advertisers are expected to learn systems across a wide variety of providers in order to get the market adoption they are hoping for. With no single protocol, it can be a challenge for media buyers to know what every platform's rules and regulations are, not to mention which platforms are trustworthy and which ones should be avoided.

The Fraudsters' Race

However, industry players are coming together to build standards across the ecosystem. Until those initiatives are fully implemented, though, fraudsters will have leeway to operate and scale. In 2018, the IAB released its guidelines for Identifier for Advertising (IFA): a series of recommendations on how to maintain a high-quality advertising experience within over-the-top (OTT) television environments. IAB is currently working to develop a User Agent & Bundle ID naming standard in OTT that is as consistent as possible.

Advertisers are buying CTV inventory identified from user agent strings, device type fields, deal IDs and a few others. Fraudsters can command bots to send fake user agent IDs as well as bundle/app IDs pretending to be legitimate devices. With the advent of SSAI, fraudsters have sought out and found ways to beat the system. Fraudsters can deploy machines that mimic the proxy servers that handle SSAI processing for some providers, allowing them to sneak into the supply chain.

How are fraudsters scaling CTV operations?

Fraudsters, once they discover a money-making scheme, will look for ways to ramp up that scheme: anything worth doing is worth doing a lot. Even unsophisticated, simple techniques can be scaled to cause huge monetary damage in a very short period of time before they're discovered and shut down. There are several ways that fraudsters can scale CTV device impersonation efforts:

Data Center Bots:

Picture a data center full of servers, each running several virtual machines, and each virtual machine pretending to be a CTV device, calling home and asking for ads to be delivered. 3ve is a good example of a data center-based botnet: one of the three takedown operations uncovered that a portion of 3ve was powered by bots running in data centers. It also cleverly leveraged compromised residential IP address space as a proxy, making it appear that the requests are coming from homes and businesses in high premium markets.

Hijacked Residential Devices:

Today, more than 75% of bot activity comes from residential machines. This new real estate allows bots to closely mimic human behavior, rendering traditional methods that focus on identifying non-human behavior less effective. Once devices are hijacked, they can be utilized to mimic any other device by manipulating the headers in the request sending fake user agent IDs, bundle/app IDs. s in high premium markets.

Emulators / Custom software automation:

Fraudsters are able to deploy custom software tools or emulators to scale up the volume on fake traffic and setup device farms.

Recently, White Ops Threat Intelligence saw a version of this situation unfold: a threat actor was impersonating several popular CTV devices, such as Roku and Apple TV. This rare, in-the-wild look demonstrates the low barrier to entry for fraudsters looking for opportunities in the CTV ecosystem.

The threat actor first developed an improvised ad server that would generate API requests to be sent to the advertisers. Also, the threat actor tunneled their traffic through residential IP addresses. We can see in the URL the API endpoint "VAST" appears to be targeting the API template commonly used to serve video ads. The threat actor likely developed this page to easily generate requests and review them before sending.

In another server maintained by the same threat actor, we see specific inclusion of the names of popular CTV devices, such as Roku. The ad network did not know this was a fraudster. Thus, the threat actor was rewarded for ad impressions on a Roku device that does not exist.

These snapshots provide a firsthand look at the opportunity that fraudsters see in CTV.

While the market for streaming content continues to explode, so will the risk of fraudsters attempting to exploit advertisers. We recommend consistent and intelligent inspection of traffic. If an API request is not complying with the specifications set forth by a given API, don't validate it. This concerted effort can make all the difference when determining whether requests are bot or not.

The Defenders' Race

How White Ops is Staying Ahead

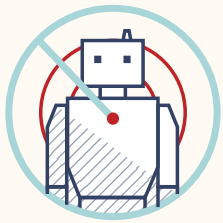
White Ops uses a multilayered approach for all environments—including CTV—that allows us to detect and prevent invalid traffic with unprecedented accuracy, without compromising anyone's viewing experience.

- An in-house threat intelligence team proactively hunts for new threats on the Internet. They attribute those threats to specific botnet operators and campaigns, then feeding findings back into detection algorithms.

- Our global visibility and scale by observing more than 100B+ CTV bid opportunities every month allows us to have large data sets to build machine learning models.

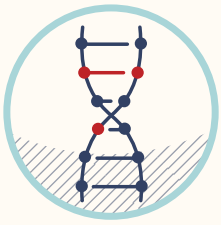
- Security researchers probe all CTV devices for hundreds of data points on the network, device, and application configuration to detect technical evidence of compromise.

The Defenders' Race



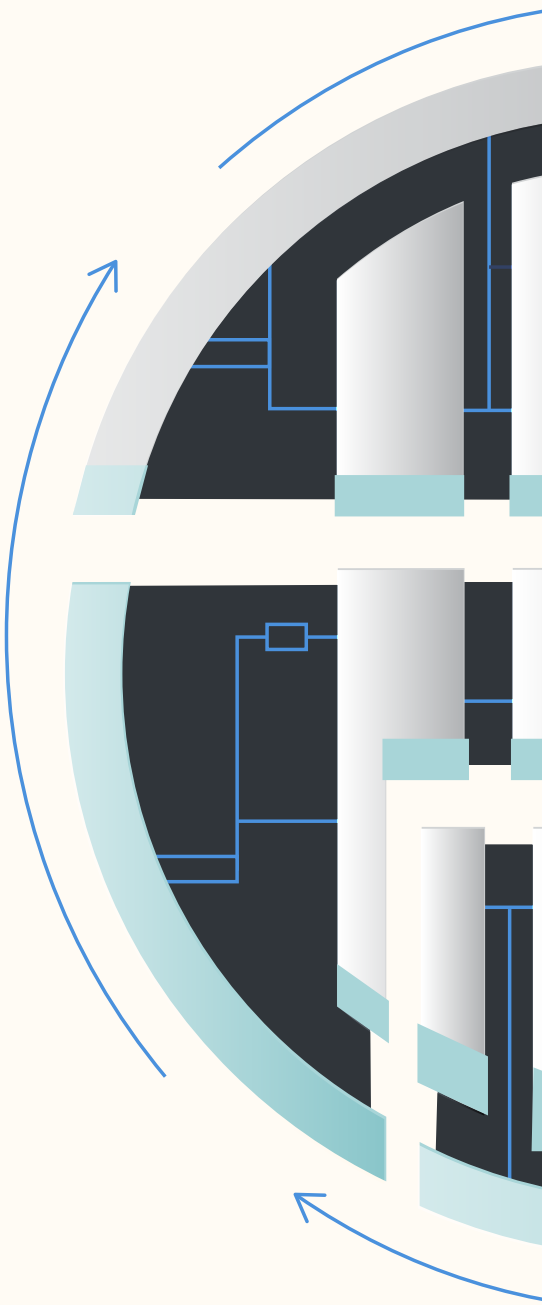
CTV DETECTION ALGORITHMS

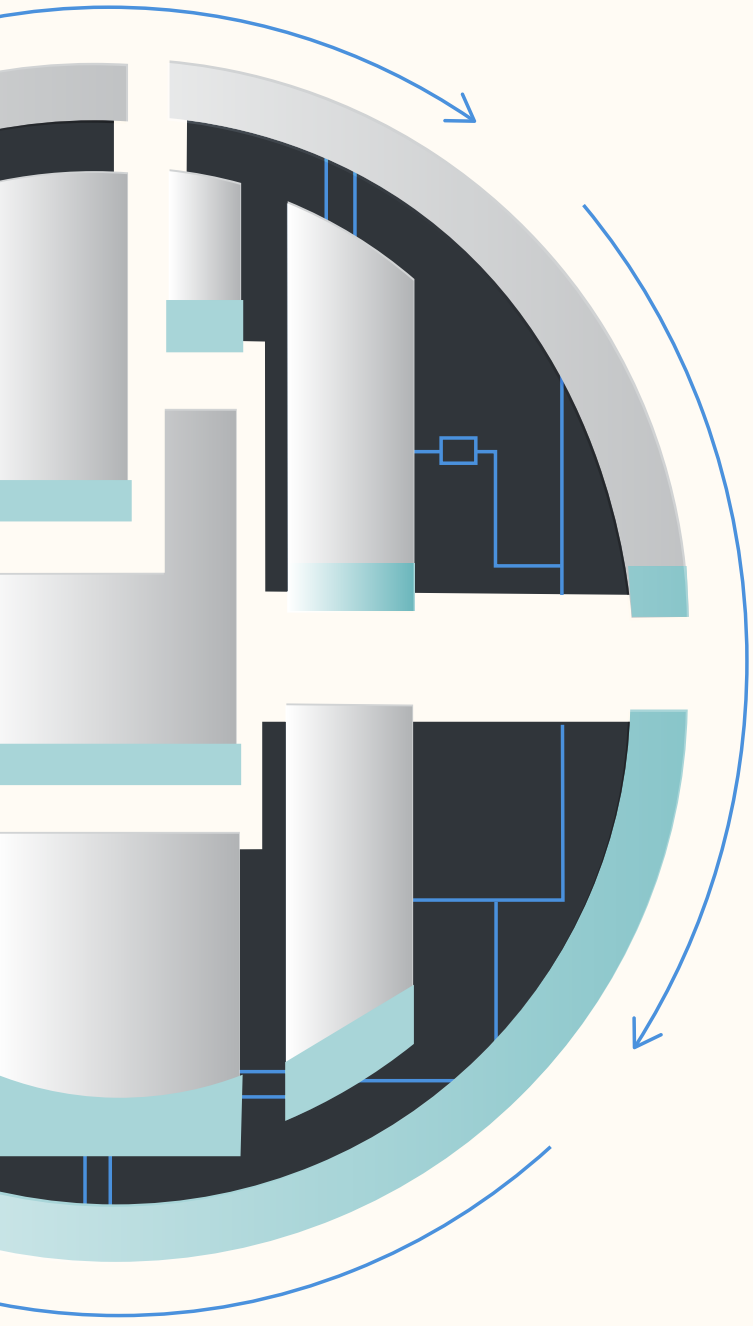
Identify fraudulent behavior by probing device information, OS signals, and network signals

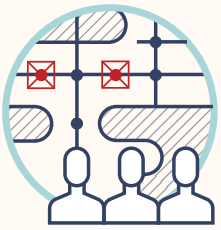


CONTINUOUS ADAPTATION

Create new detection algorithms to stay ahead of our adversaries and new CTV threats

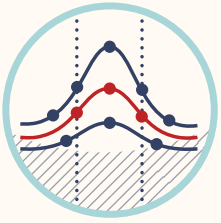






DEDICATED CTV SECURITY RESEARCHERS

Inform detection by performing threat hunting, malware reverse engineering, and CTV threat modeling



MACHINE LEARNING

Analyze signals across CTV populations for broader detection

TECHNIQUES WE UTILIZE

Understanding of each device OS/network stack by using detailed research on firmware and hardware for particularities of each model.

Developing statistical and machine learning models that differentiate normal users watching TV in their living room from actors impersonating organic activity.

Setting up internal device labs with a variety of different connected TVs, apps, and channels to understand device capabilities and identify emerging threats.

IP reputation: Building an internal reputation system that classifies traffic such as proxy, VPN, invalid data center, SSAI etc.

“”

We partnered with White Ops because they share our commitment to fostering a clean and safe environment in the programmatic landscape. We can say that White Ops is a part of our efforts to keep CTV a fraud-free environment and we look forward to being partners and helping to keep the ecosystem clean for many years to come.

– Katie Evans, Chief Operating Officer, Telaria

CONCLUSION

The race is not yet won by either side. Every day, the fraudsters work to make the defenders' work obsolete, and every day, the defenders work to block the fraudsters' efforts to trip us up. It'll take an industry-wide effort for the defenders to win. Our faith in the integrity of our entertainment providers is on the line, so it's a fight that all of us are invested in. White Ops is working hard to stay ahead of tactics like device impersonation.

Here are a couple steps each of us can do as an industry:

Collaborate with industry groups:

Organizations like the IAB and the ANA advocate on behalf of advertisers to ensure that advertising ecosystem is constantly moving forward technologically. Active participation in industry organizations is a crucial way to stay on the forefront of new developments in the ongoing fight against ad fraud. It is imperative for everyone to work together to develop a User Agent & Bundle ID naming standard for OTT to help fight fraudulent behavior.

Adopt Industry Standards such as app-ads.txt:

Every player in the CTV ecosystem should be well-educated on (and ideally, participating in) the app-ads.txt initiative. App-ads.txt is an extension of the original ads.txt: it's a mechanism for publishers to declare who can sell their ad space. Buyers can ensure through app-ads.txt that they're working exclusively with authorized sellers. Participation in the app-ads.txt initiative should be, for advertisers, the bare minimum criteria for publishers.

NOVEMBER 2019

WHITEOPS.COM

WHITE PAPER