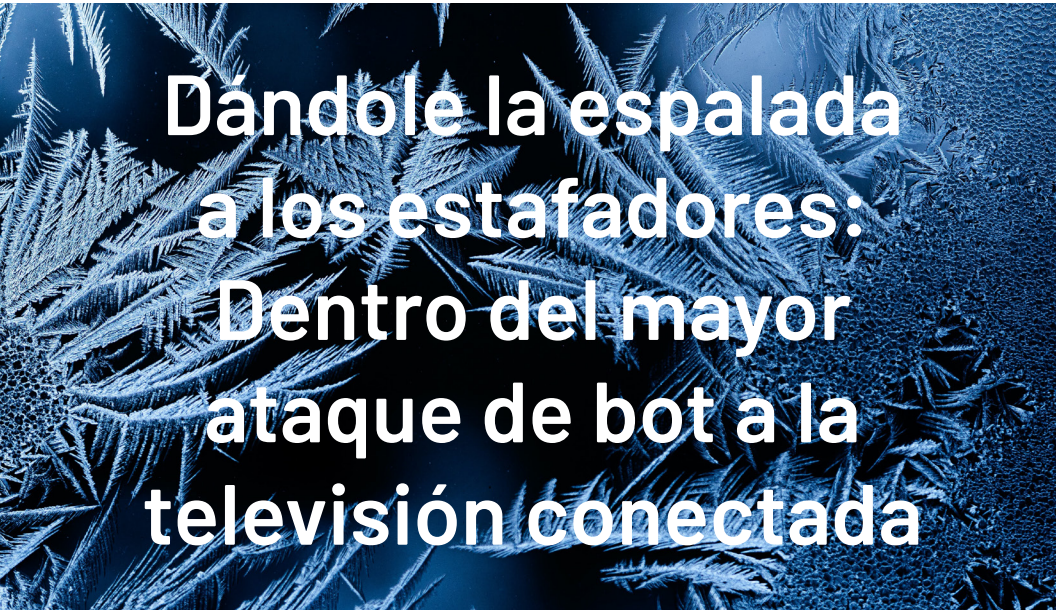
White Ops



Dándole la espalada a los estafadores: Dentro del mayor ataque de bot a la televisión conectada

White Ops

Dándole la espalada a los estafadores: Dentro del mayor ataque de bot a la televisión conectada

Investigadores : Dr. Mike Moran, Mikhail Venkov, Ryan Castellucci, Aaron DeVera, y Davide Mandrini

La televisión conectada (siglas en inglés: CTV) brinda oportunidades masivas para las marcas y los servicios de streaming de comprometerse con los consumidores por medio de la publicidad y de contenido atractivo. A causa de esta oportunidad, es sumamente importante que las marcas y el ecosistema de CTV trabajen juntos a través de una cadena de suministro de publicidad protegida de forma colectiva para asegurar que se reconozca, se aborde y se elimine el fraude tan pronto como sea posible, ya que los ciberdelincuentes siempre buscan el dinero. El fraude de publicidad puede ocurrir cuando se compra publicidad a través de canales no protegidos. El fraude de publicidad se puede eliminar fácilmente por medio de canales protegidos en los que hay relaciones directas, confianza y absoluta transparencia. Trabajar juntos a través de una cadena de suministro protegida de forma colectiva asegurará que el ecosistema logre los beneficios completos

de crear una muy buena experiencia para el cliente de CTV que sea libre de fraude publicitario.

Una nueva operación de fraude de publicidad en CTV, conocida como ICEBUCKET, comenzó en el canal ude publicidad programática donde la cadena de suministro es menos transparente, los vendedores no se reportan en los archivos sellers.json, y los compradores y vendedores por lo general no tienen relación directa. Las personas mal intencionadas detrás de ICEBUCKET tenían se mantuvieron bajo radar hasta que trataron de expandirse y redoblar sus esfuerzos. Sin embargo, trabajando con nuestros socios, bloqueamos el ataque, protegimos y compartimos información a lo largo de nuestra red de socios, y mejoramos la eficacia de nuestra plataforma para asegurarnos de estar un paso más adelante del fraude de publicidad y de los actores malintencionados que se encuentran detrás del mismo. Nuestro éxito es evidencia de un planeamiento a largo plazo, de procesos y prácticas establecidas entre nosotros y nuestros socios.

Recientemente, el equipo de Inteligencia e investigación de amenazas -Satori- de White Ops descubrió la operación de fraude de televisión conectada (CTV)-las más grande y amplia conocida. En el momento más intenso de su actividad, la operación ICEBUCKET suplantó a más de 2 millones de personas en más de 30 países. La operación falsificó más de 300 sitios web diferentes, robando inversión publicitaria al engañar

a los anunciantes por medios de hacerles creer que estaban difundiendo publicidad a personas reales, cuando en realidad estaban difundiendo publicidad a bots que se hacían pasar por gente real. La operación escondió sus bots sofisticados dentro de la limitada señal y transparencia de las impresiones de anuncios en video respaldadas por la inserción de anuncios del lado del servidor (SSAI, por sus siglas en inglés). La plataforma de mitigación de bots de White Ops es capaz de detectar este esquema de fraude y proteger a los anunciantes de caer víctimas de esta operación, y de otras similares.

Aquí están los detalles de cómo fue frenada la operación ICEBUCKET y cómo se evitó así un impacto alto sobre una cadena de suministro protegida de forma colectiva. En un esfuerzo por seguir protegiendo a los anunciantes, les dejamos nuestras recomendaciones para que las marcas y los ecosistemas de CTV permanezcan libres de fraude.

Un hielo, dos hielos, 28% de hielo (ICEBUCKET)

La operación ICEBUCKET es el mayor caso de suplantación por SSAI que haya sido descubierto. De acuerdo a nuestros datos internos, casi en su punto máximo de operación cerca del **28%** del tráfico programático de CTV del que White Ops tuvo visibilidad, **o cerca de 1,9**

mil millones de solicitudes de anuncios por día en el mes de enero provinieron de esta misma operación.

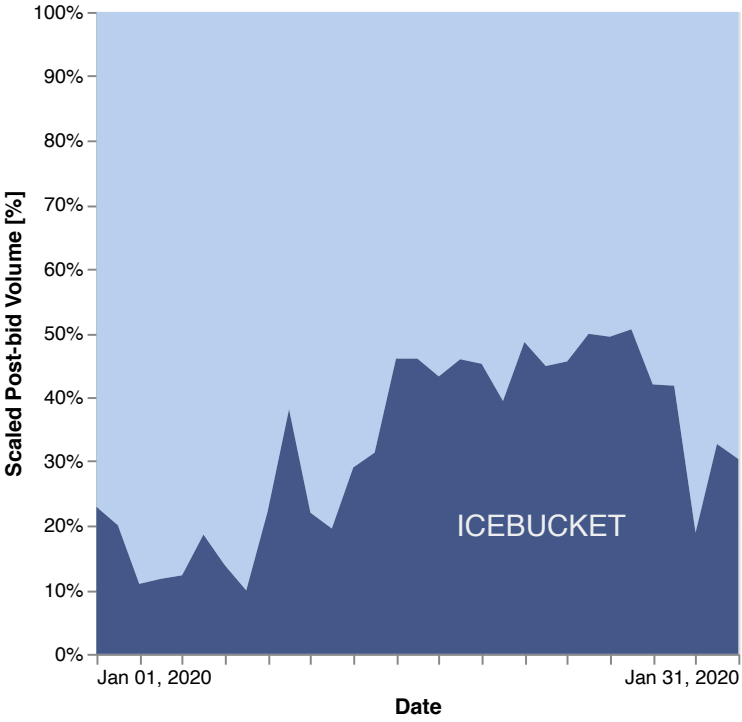


Imagen 1: porcentaje del tráfico programático de CTV involucrado en esta operación para enero del 2020.

En enero del 2020, el 66% del tráfico programático de SSAI usando medios de CTV y el 15% del tráfico programático de SSAI usando medios móviles que White Ops protege fueron parte de este esquema. Cuando

vemos los dispositivos que la operación utilizó, vemos varios dispositivos de CTV junto con el tráfico móvil. Abajo se muestra los principales dispositivos suplantados en este esquema. Algunos de los dispositivos que los estafadores suplantaron en esta operación son de líneas de producción discontinuadas. White Ops le brindó información acerca de esta amenaza a Roku, que les permitió verificar los resultados contra sus sistemas internos. Confirmaron la naturaleza de suplantación en esta operación, ya que no había actividad de ICEBUCKET en la plataforma de Roku.

Dispositivos	Proporción [%]
Roku (todas las marcas)	46.0%
TV inteligente de Samsung Tizen	26.8%
TV de Google	20.7%
Android (móvil)	6.1%

Tabla 1: Proporción del tráfico de ICEBUCKET en enero del 2020 para varios dispositivos declarados

Esta operación falsificó servidores de SSAI al generar tráfico para dispositivos periféricos ficticios (especialmente dispositivos móviles y de CTV) dentro del ecosistema de tecnología publicitaria. Para hacerlo, la operación utilizó:

- Más de 1.000 agentes de usuario diferentes, cerca de 500 de los cuales solo aparecen en esta operación

- Más de 300 appIDs diferentes de varios editores

- Al menos 2 millones de direcciones IP suplantadas de más de 30 países, de las que más del 99% estaban ubicadas en los Estados Unidos

- Cerca de 1.700 IPs de servidores de SSAI ubi cadas en 9 países generando tráfico

Para poder entender completamente la magnitud de la operación ICEBUCKET, es importante tener una idea de cómo funciona SSAI, del papel que juega en la publicidad programática en las plataformas de CTV, de por qué la suplantación de SSAI es tan difícil de detectar, y de qué es lo que hace a la suplantación de SSAI un objetivo tan atractivo para los estafadores.

¿Qué es la inserción de anuncios del lado del servidor (SSAI)?

La inserción de anuncios del lado del servidor, o SSAI, fue desarrollada por los editores para crear una mejor experiencia de anuncios para el usuario final. Los

anuncios están “cosidos” en la tela del contenido de video para que no haya demoras ni dificultades causadas por iniciar un reproductor de anuncios. SSAI se utiliza generalmente para publicidad en varias clases de dispositivos “periféricos”, tales como CTVs, teléfonos inteligentes, consolas de juegos, y otros. Entregar contenido de video publicitario a través de SSAI le ofrece a los anunciantes muchos beneficios, incluyendo la personalización del usuario y la reducción de la inactividad.

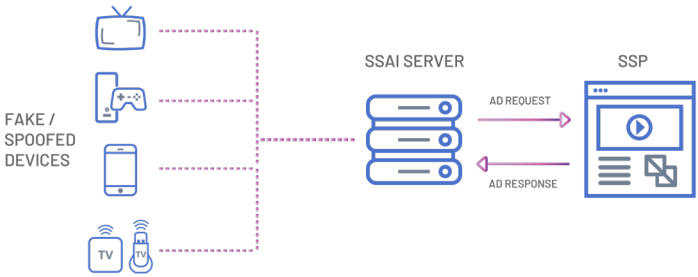


Imagen 2: Diagrama de cómo la suplantación de SSAI se relaciona con el ecosistema de tecnología publicitaria

Si bien SSAI es una solución elegante para la entrega de publicidad, todavía se encuentra en sus primeras etapas. Como sucede con todas las nuevas tecnologías, White Ops puede perever a los estafadores encontrando agujeros en el sistema y serpenteando para meterse. Los estafadores han encontrado una forma de suplantar los dispositivos periféricos para

replicar los servicios de SSAI.

La suplantación de SSAI, la técnica principal de fraude que los operadores de ICEBUCKET utilizaban, sucede cuando los estafadores envían un montón de solicitudes de anuncios de centros de datos de parte de dispositivos periféricos falsos o "suplantados". Un proveedor real de SSAI, transmite el origen de un centro de datos. En lugar de mostrar los anuncios a humanos, los estafadores llaman a las APIs de informes indicando que la publicidad ha sido "mostrada". A menudo, la información disponible para los anunciantes en un ambiente de SSAI se limita al agente de usuario del dispositivo y su dirección IP. Esta información puede enviarse en las cabeceras HTTP "X-Device-User-Agent" y "X-Device-IP", así como los lineamientos de la IAB sobre VAST, o por medio de otras cabeceras similares. Mientras que falsificar estos datos es relativamente simple, el matiz de hacerlo de manera convincente lo convierte en una forma sofisticada de ataque de bots.

Los anunciantes pagan para que sus publicidades sean vistas por un público humano que esté abierto a sus productos o servicios. En lugar de eso, estos estafadores toman el dinero de los anunciantes y se lo roban; las publicidades que "se entregan" o bien nunca llegan a ver la luz del día, o nunca son vistas por un humano. El público de los bots verdaderamente sofisticados es en verdad un público vacío.

White Ops

La operación ICEBUCKET

La operación ICEBUCKET presentó su tráfico como proveniente de un proveedor de SSAI legítimo (basado en la inclusión de cabeceras HTTP estándares) para una variedad de dispositivos y aplicaciones, utilizando código personalizado. ICEBUCKET montó solicitudes para que los anuncios fueran insertados en el contenido de video para los televidentes de dispositivos móviles y de CTV, pero ninguno de esos dispositivos o televidentes existía verdaderamente. Los agentes de usuario utilizados en la operación en su gran mayoría referían a clases de dispositivos obsoletos que ya no se utilizan en la población general, o dispositivos que nunca existieron en primer lugar. Las direcciones de IP mostraban signos de haber sido generadas por medio de algoritmos para imitar al público deseado.

Estas solicitudes de anuncios se originaron desde un pequeño conjunto de números de sistema autónomo (ASNs). Los sistemas autónomos constituyen la infraestructura de ruteo del back-end de la Internet, de la misma forma en que las carreteras conectan el tráfico entre las diferentes ciudades. Cada sistema está identificado con un número, el ASN, similar en su función al código postal. Si bien no podemos saber a ciencia cierta la motivación del actor de la amenaza para usar estos ASNs en la operación, podemos hacer algunos comentarios acerca de las posibles razones. Los ASNs tienen:

- Ejecución deficiente de los operadores de red con respecto a la actividad maliciosa conducida desde su centro de datos

- Servicios baratos de Servidor virtual privado (VPS, por sus siglas en inglés)

- Una gran cantidad de hosts dentro de ese espacio de IP que son vulnerables o que de otra forma están abiertos la explotación

Es probable que el actor detrás de ICEBUCKET haya operado desde estas ASNs debido a su confianza de que su comportamiento pasaría desapercibido. No todo el tráfico de estos ASNs es parte de la operación ICEBUCKET, ya que también hay tráfico no proveniente de ICEBUCKET en estos ASNs.

La operación ICEBUCKET es única en que un subgrupo del tráfico se genera para beneficiar a los medios de aplicaciones directamente por medio de tratos directos. Hemos observado casos en los que dichos medios mezclan tráfico orgánico con el de ICEBUCKET en lo que parecen ser los primeros indicios de esquemas de fuentes de tráfico para el tráfico de CTV. De nuestra observación de este tráfico "mezclado", tenemos dos hipótesis de por qué sucedería esto:

- **Esconder la operación:** Al crear un subgrupo de tráfico, los estafadores han generado ruido

para tapar la identificación de la operación. Las aplicaciones suplantadas son así beneficiarios inconscientes del tráfico generado.

• **Fraude como un servicio:** La operación genera tráfico de parte de los medios de las aplicaciones. El subgrupo de actividad fraudulenta se vuelve más difícil de detectar, y la operación tiene una fuente extra de recaudación para el esquema.

A este punto, no podemos determinar de manera concluyente entre las dos posibilidades. Existe la posibilidad de que ambas opciones estén presentes, dependiendo del subgrupo particular de tráfico en cuestión.

Bloquearles el acceso a los estafadores

La plataforma de mitigación de bots de White Ops nos permite proteger a nuestros socios bloqueando a los bots sofisticados una vez que hayamos identificado correctamente las firmas de la amenaza particular. Al controlar en busca de esas firmas en nuestro tráfico preliminar (pre-bid en ingles), podemos bloquear de manera automática el tráfico fraudulento y asegurarnos de que el dinero no vaya a los bolsillos de los estafadores. La plataforma también nos permite marcar las partes del ecosistema de tecnología publicitaria en las

que esta operación está prosperando, para que nuestros socios puedan tomar las acciones necesarias.

Toda clase de suplantación está diseñada para hacer que la entidad suplantada se asemeje a la víctima (un cliente, un anunciante, un desarrollador de aplicaciones; el objetivo depende de la operación). Utilizando varios huellas de fraude, podemos distinguir entre el tráfico humano real y el tráfico de estos dispositivos suplantados. White Ops tiene el cuidado de no impactar de manera negativa a las aplicaciones que son víctimas en los esquemas de fraude cuales suplantan o falsifican vsus appIDs. Trabajamos para cortar el flujo de dinero hacia los verdaderos estafadores, no hacia las aplicaciones verdaderas.

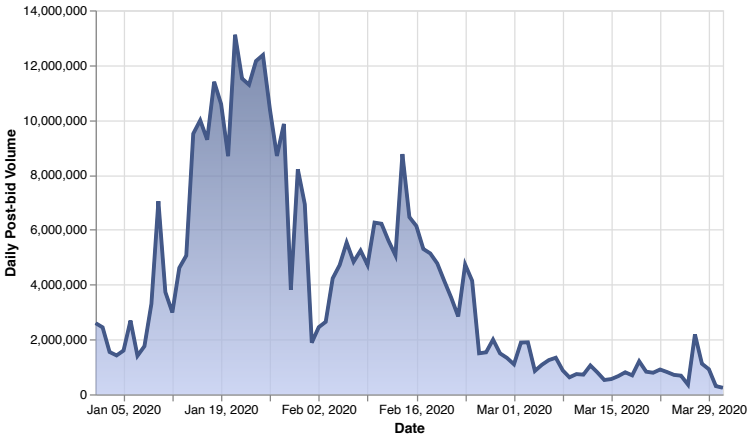


Imagen 3: impresiones posteriores asociadas con ICE-BUCKET para el 2020.

Tal como se señala arriba, ICEBUCKET es una operación corriente. Los volúmenes que muestra la imagen 3 no han bajado a cero. Los estafadores siguen allá afuera, pero nosotros podemos ejecutar nuestras técnicas de prevención y de mitigación de bots para detectarlos y proteger en contra de sus ataques; ahora estamos dando a conocer este descubrimiento para que otros puedan hacer lo mismo. Ya hemos desplegado nuestra defensa en contra de operaciones similares, y hemos expandido nuestra protegida colectiva más allá dentro del subgrupo de nuestro tráfico observado de "presunto SSAI". Nuestras técnicas de detección y prevención de bots están evolucionando continuamente para contrarrestar las amenazas emergentes, como así también para anticipar nuevas amenazas.

Frenando la tormenta de hielo (de ICEBUCKET)

Dado que la suplantación de CTV y SSAI son opciones lucrativas para nuestros adversarios debido a los altos CPMs en clientes de CTV, es de esperar ver que comiencen operaciones similares, o que operaciones existentes se vuelvan del tráfico web y móvil al de CTV.

Existen un par de cosas que nuestros colegas en la industria pueden hacer para tratar de mitigar la suplantación de SSAI:

White Ops

• Asegura que trabajes con una cadena de suministro publicitario protegida de forma colectiva donde haya relaciones directas, confianza y transparencia

• Tener declaraciones consistentes de appID/bundleID para brindar enlaces más fuertes de la aplicación al editor, tales como las pautas de identificación de aplicación del IAB

• Consulta con frecuencia con tus compañeros de tecnología publicitaria a través del ecosistema para asegurar que todos los que están alrededor entiendan bien esta nueva amenaza

• Desarrolla más estándares que aumenten la transparencia para el inventario de CTV, tales como:

  • Expandir el estándar app-ads.txt para que respalde completamente el tráfico de CTV

  • Adoptar completamente sellers.json para respaldar la visibilidad dentro de toda la cadena de suministro

  • Los fabricantes de dispositivos y los proveedores de SSAI deben respaldar

el desarrollo y la adopción de estándares que verifiquen la autenticidad de un dispositivo (por ejemplo: por medio de firmar criptográficamente sus solicitudes). Eso sería un gran paso adelante para combatir la suplantación de dispositivos.

Hemos visto acciones como estas tener un efecto dominó. Cuando el esquema se vuelva menos beneficioso, entonces habremos hecho nuestro trabajo: al cortar los flujos de recaudación para los actores malintencionados, los echamos fuera del ecosistema. Advertising Integrity (integridad publicitaria) de White Ops, con la ayuda de los socios con los que trabajamos, ofrece una cadena de suministro publicitario protegida de forma colectiva para asegurar que los anunciantes no caigan víctimas de los ataques de bots más sofisticados en CTV y por toda la Internet.

La educación acerca de la suplantación de SSAI es solo el comienzo; los equipos necesitan comenzar a controlar este comportamiento. El ecosistema de publicidad programática necesita los estándares de la industria para sacar a estos estafadores de una vez por todas.

Apéndice

Subgrupo de ASNs identificado como las fuentes de tráfico de esta operación:

29182
49392
51167
51659
59729
203004
204490
204601
204957

No todo el tráfico de estos ASNs es parte de la operación ICEBUCKET, ya que también hay tráfico no proveniente de ICEBUCKET en estos ASNs.

Los agentes de usuario presentes: icebucket-uas.txt

> No todos los agentes de usuario incluidos son específicos de la operación ICEBUCKET. Ya que la operación trata de hacerse ver como tráfico legítimo, hay algunos dispositivos representados aquí que pueden ser vistos fuera de esta operación.

White Ops®

White Ops is the global leader in bot mitigation. We protect more than 200 enterprises - including the largest internet platforms - from sophisticated bots by verifying the humanity of more than one trillion online interactions every week. The most sophisticated bots look and act like humans when they click on ads, visit websites, fill out forms, take over accounts, and commit payment fraud. We stop them. To learn more, visit whiteops.com.