Cuando el Smart TV se convierte en monitor: Riesgos de ACR en entornos sensibles

StringManolo
Cybersecurity Researcher
github.com/StringManolo

Publicado: Noviembre 2025 | **Tiempo de lectura:** 3 min | **Tags:** #SmartTV #ACR #Privacidad #Ciberseguridad

⚠ **Atención:** Si usas un Smart TV como monitor de tu PC u otro dispositivo, este artículo te interesa. Tu televisor podría estar espiando todo lo que muestras.

Introducción: El caballo de Troya en tu salón

Trasteando con dispositivos IoT y analizando sus comunicaciones. Hay una brecha enorme entre lo que la gente cree que hace su Smart TV y lo que realmente hace. Cuando conectas tu portátil, smartphone, consola o PC a un televisor "inteligente", la mayoría asume que se comporta como un monitor tradicional. **Error.**

Bajo la superficie, muchos de estos dispositivos ejecutan motores de ACR (Automatic Content Recognition) diseñados para analizar **lo que se muestra en pantalla** y vincularlo con publicidad, analíticas o perfiles de usuario.

Si usas un Smart TV como monitor principal, estás confiándole **todo** lo que muestras: credenciales, documentos internos, llamadas de Teams, dashboards financieros, código fuente... mientras el mismo motor de captura diseñado para "programas de TV" puede seguir activo. Este artículo busca mapear ese riesgo con suficiente detalle técnico como para que tomes decisiones informadas.

¿Cómo funciona realmente ACR?

Métodos técnicos de implementación

Automatic Content Recognition (ACR) es una tecnología embebida en Smart TVs que identifica el contenido mostrado capturando muestras (frames de vídeo o audio) y comparándolas contra una base de datos de referencia.

```
Dos métodos principales:

 Watermarking (marcas de agua):
- Contenido lleva marcador embebido imperceptible
- El TV detecta y reporta el watermark
- Menos común en contenido HDMI/externo

 Fingerprinting (huella digital):
- TV captura frames/audio y genera hash descriptivo
- Usa algoritmos como SIFT, ORB o redes neuronales
- Envía hash a servidor para identificación
- Método más peligroso en modo monitor
```

Flujo técnico detallado

Desde el punto de vista del dispositivo:

1. **Captura:** El firmware del TV muestrea frames de vídeo (incluso de HDMI o Wi-Fi) y/o fragmentos de audio
2. **Procesamiento local:** Aplica algoritmos de extracción de características para generar "huella"
3. **Transmisión:** La huella + metadatos (device ID, timestamp) se envía vía HTTPS
4. **Identificación:** Servidor compara con su BD y devuelve match (si existe)
5. **Explotación:** Datos se usan para analytics, recomendaciones, publicidad o delitos electrónicos

> **Evidencia empírica:** Investigaciones recientes (Anselmi et al. 2024) confirman que el tracking por ACR **persiste en entradas HDMI**. En pruebas con TVs Samsung y LG, se detectó tráfico de fingerprinting incluso mostrando contenido de ordenador.

Modelo de amenazas: Tu TV como elemento de espionaje

Escenarios comunes

- **Navegación:** Relleno de formularios (credenciales y data personal), consulta de correos electrónicos
- **R&D/Desarrollo:** Prototipos, diagramas de arquitectura, código fuente
- **Videoconferencias:** Reuniones internas, pizarras colaborativas
- **Dashboards:** Métricas financieras, datos de clientes, KPI internos
- **Remote Desktop:** Sesiones RDP/VNC con sistemas críticos

Cadena de ataque completa

```
Attack Chain ACR + Lateral Movement:

1. Reconocimiento: Compromiso inicial del TV (ej: CVE-2021-1479 en WebOS), de las comunicaciones o del servidor de destino
2. Captura: Análisis de tráfico ACR para entender patrones de trabajo
3. Explotación: Uso de datos para spear-phishing personalizado o login con credenciales extraidas
4. Movimiento lateral: Pivotaje hacia PC u otros dispositivos de red mediante shared network
5. Exfiltración: Datos sensibles capturados via ACR + otros sistemas
```

Mitigaciones prácticas

Nivel Dispositivo

- Deshabilitar ACR en menús de privacidad
- Reset de fábrica tras updates de firmware y reconfiguración
- Cinta aislante en micrófono/cámara
- Desconectar red cuando sea posible

Nivel Red

- VLAN aislada para TVs

- Firewall bloqueando tráfico saliente
- DNS filtering (Pi-hole/pfBlockerNG)
- Monitorización con Wireshark

Nivel Organizacional

- Política explícita prohibiendo Smart TVs
- Inventory de displays como endpoints
- Awareness training específico
- Preferir displays "dumb"

Comandos prácticos de bloqueo

Dominios a bloquear en Pi-hole/pfSense:

```
# Samsung
samsungcloudsolution.com
acr0.samsungcloudsolution.com

# LG
lgad.cjpowercast.com
us.lgtvsdp.com

# Samba TV (común en Sony, TCL)
sambavideo.com
config.samsungads.com
```

Conclusión

El mensaje es claro: si conectas tu equipo a un Smart TV, no lo trates como un monitor. Trátalo como un dispositivo de red que potencialmente está capturando todo lo que muestras y enviándolo a terceros.

Deshabilitando ACR, segmentando la red, estableciendo firewall, manteniendo el firmware actualizado y tratando el TV como parte de tu superficie de ataque, reduces significativamente el riesgo.

Referencias Técnicas

- Anselmi et al. "Watching TV with the Second-Party: A First Look at Automatic Content Recognition Tracking in Smart TVs" - IMC 2024
- Documentación técnica y artículos de Samba TV

© 2025 StringManolo - Cybersecurity Researcher