Nro. Alerta:	AL-2025-002	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	13-ene-2025	El malware Badbox	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Incidente
Tipo de Incidente: Malware
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- *Badbox - figura referencial*

El malware BadBox apunta ahora a smart TVs basados en AOSP (Android Source Open Projects) este tipo de malware compromete severamente los televisores Android TV y Google TV, específicamente los que no cuentan con el certificado Google Play Protect.

Entre las consecuencias graves que provoca van desde el robo de información personal y financiera, pasando por ataques de DDoS a través del dispositivo contagiado siendo parte de una botnet del malware, hasta la generación de cuentas de servicios y Adware o publicidad fraudulenta.

III. INTRODUCCIÓN

El malware Badbox ha sido detectado en smart TVs que pertenecen a dispositivos Android basados en la AOSP, esto es un proyecto de Google Open Source del que Google brinda acceso a sus socios para la edición del código fuente, estos sistemas al no ser de edición final de Google no han pasado por pruebas de seguridad y

compatibilidad que el propio Google ofrece para sus servicios, por lo que no cuentan con el Certificado de Google Play Protect.

BadBox se caracteriza por estar integrado directamente en el firmware de los dispositivos durante su fabricación. Esto significa que los dispositivos ya salen de la fábrica infectados.

IV. VECTOR DE ATAQUE

El malware tiene la capacidad para eludir sistemas de protección y robar datos personales y financiera, lo que resulta en un fraude y la perdida de privacidad, también esta reciente variante explota dispositivos para actividades maliciosas como proxys residenciales, instalación remota de código, abuso de cuentas y fraude publicitario. Además, permite cargar código nuevo sin el conocimiento del usuario, creando vulnerabilidades a futuros ataques al abrir backdoors (puertas traseras) que los atacantes pueden usar para instalar otros malware en el dispositivo, lo que amplía los riesgos de seguridad.

V. IMPACTO

El malware presenta varias formas de ataque, entre las que destacan convertir los smart tv en proxy residenciales, consumiendo recurso de internet como el ancho de banda y uso de la ip para actividades maliciosas, también como la formación de botnets.

Permite la instalación remota de código malicioso, lo que permite al dispositivo empezar a descargar y ejecutar programas sin control y permiso del usuario. El malware dentro del dispositivo infectado genera Adware, como fraudes publicitarios y abusos de cuentas, lo que podría comprometer tus datos personales.

VI. INDICADORES DE COMPROMISOS

Se conoce que el malware Babdox viene integrado de fábrica en el firmware de los smart TV y se ha logrado identificar algunos de estos equipos infectados, son 8 tipos diferentes de dispositivos que presentan el método de backdoors, siendo estos 7 TV boxs los modelos T95, T95Z, T95MAX, X88, Q9, X12PLUS y MXQ Pro 5G y 1 tablet Android modelo J5-W.

Otros modelos encontrados con la afectación son Android TV Box R4, TV BOX y KJ-SMART4KVIP, que ejecutan AOSP versión 7, 10 o 12, junto también con equipos de marca Yandex de los modelos YNDX-00091 al YNDX-000102 son Smart TV 4K de la marca conocida.

Sumado también en dispositivos con versiones obsoletas de Android que son especialmente vulnerables debido a la falta de actualizaciones de seguridad y la ausencia de protecciones avanzadas.

VII. RECOMENDACIONES:

- Revisar y optar por dispositivos certificados: Elige dispositivos certificados por Google Play Protect, ya que garantizan pruebas de seguridad y compatibilidad.
- Evitar dispositivos baratos de marcas no reconocidas: Los dispositivos de bajo costo de fabricantes desconocidos pueden venir con malware preinstalado.
- Evitar instalar aplicaciones de fuentes no verificadas o no oficiales.
- Mantener actualizado el sistema operativo y las aplicaciones para reducir la exposición a vulnerabilidades conocidas.
- Desactivar la instalación de aplicaciones desde orígenes desconocidos en la configuración de seguridad del dispositivo.
- Usar contraseñas fuertes para proteger los dispositivos y las cuentas asociadas.
- Ser cauteloso con los anuncios y las solicitudes de inicio de sesión en la pantalla del televisor.
- Mantén el firmware actualizado para corregir vulnerabilidades conocidas y mejorar la seguridad.
- En el caso de equipos portátiles con Android evitar redes Wi-Fi públicas o no seguras y preferir redes protegidas con contraseñas robustas.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

https://www.infobae.com/tecno/2024/12/18/cuidado-30-mil-dispositivos-android-en-peligro-por-un-malware/

https://www.darkreading.com/vulnerabilities-threats/badbox-operation-targets-android-devices-in-fraud-schemes

https://unaaldia.hispasec.com/2024/12/alemania-neutraliza-badbox-el-malware-oculto-en-30-000-dispositivos-iot-android.html

https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/BADBOX/badbox_node.html

https://pisapapeles.net/una-nueva-variante-del-malware-badbox-vuelve-a-infectar-los-smart-tv-con-android/?utm_source=twitter&utm_medium=social&utm_campaign=ap

https://www.svconline.com/proav-today/new-batch-android-tv-malware