Investigadores de seguridad cibernética descubrieron lagunas en el proceso de investigación de habilidades de Amazon para el ecosistema de asistente de voz de Alexa, que podrían permitir a un atacante publicar una habilidad engañosa con cualquier nombre de desarrollador arbitrario e incluso realizar cambios en el código de backend luego de la aprobación para engañar a los usuarios para que entreguen información confidencial.

Los hallazgos fueron presentados el miércoles en la conferencia Network and Distributed System Security Symposium (NDSS) por un grupo de académicos de la Ruhr-Universität Bochum y la Universidad Estatal de Carolina del Norte, quienes analizaron 90.194 habilidades disponibles en siete países, incluyendo Estados Unidos, Reino Unido, Australia, Canadá, Alemania, Japón y Francia.

Amazon Alexa permite a los desarrolladores externos crear funciones adicionales para dispositivos como los altavoces inteligentes Echo, mediante la configuración de «*habilidades*» que se ejecutan sobre el asistente de voz, lo que facilita a los usuarios iniciar una conversación con la habilidad y completar una tarea específica.

El principal de los hallazgos es la preocupación de que un usuario pueda activar una habilidad incorrecta, lo que puede tener graves consecuencias si la habilidades que se activa está diseñada con una intención insidiosa.

El problema surge del hecho de que varias habilidades pueden tener la misma frase de invocación.

De hecho, la práctica es tan frecuente que la investigación detectó 9,948 habilidades que comparte el mismo nombre de invocación con al menos otra habilidad solo en la tienda de Estados Unidos. En las siete tiendas de habilidades, solo 36,055 habilidades tenían un nombre de invocación único.

Debido a que los criterios reales que utiliza Amazon para habilitar de forma automática una habilidad específica entre varias habilidades con los mismo nombres de invocación siguen

siendo desconocidos, los investigadores advirtieron que es posible activar la habilidad incorrecta y que un adversario puede salirse con la suya con las habilidades de publicación al utilizar nombres de empresas conocidas.

> *«Esto ocurre principalmente porque Amazon actualmente no emplea ningún enfoque automatizado para detectar infracciones por el uso de marcas comerciales de terceros, y depende de la investigación manual para detectar esos intentos malévolos que son propensos a errores humanos. Como resultado, los usuarios pueden quedar expuestos a ataques de phishing lanzados por un atacante»*, dijeron los investigadores.

Además, un atacante puede realizar cambios de código luego de la aprobación de una habilidad para persuadir a un usuario de que revele información confidencial como números de teléfono y direcciones activando una intención inactiva.

En cierto modo, esto es análogo a una técnica denominada control de versiones, que se utiliza para eludir las defensas de verificación. El control de versiones se refiere a enviar una versión benigna de una aplicación a la tienda de apps de Android o iOS, con el fin de generar confianza entre los usuarios, solo para reemplazar el código base con el tiempo con funciones maliciosas adicionales a través de actualizaciones posteriores.

Para poder probar esto, los investigadores desarrollaron una habilidad de planificador de viajes que permite a un usuario crear un itinerario de viaje que posteriormente se modificó luego de la investigación inicial para *«preguntar al usuario su número de teléfono para que la habilidad pueda enviar un mensaje de texto (SMS) directamente al itinerario de viaje»*, engañando así al individuo para que revele su información personal.

Además, el estudio encontró que el modelo de permiso que usa Amazon para proteger los datos confidenciales de Alexa puede ser eludido. Esto significa que un atacante puede solicitar de forma directa datos del usuario que fueron diseñados originalmente para estar acordonados por API de permisos.

La idea es que, aunque las habilidades que solicitan datos confidenciales deben invocar las API de permiso, no impide que un desarrollador deshonesto solicite dicha información directamente al usuario.

Los investigadores aseguraron haber identificado 358 habilidades capaces de solicitar información que idealmente debería estar asegurada por la API.

Finalmente, en un análisis de las políticas de privacidad en distintas categorías, se encontró que solo el 24.2% de todas las habilidades proporcionan un enlace de política de privacidad, y que alrededor del 23.3% de dichas habilidades no revelan por completo los tipos de datos asociados con los permisos solicitados.

Al afirmar que Amazon no exige una política de privacidad para las habilidades dirigidas a niños menores de 13 años, el estudio planteó preocupaciones sobre la falta de políticas de privacidad ampliamente disponibles en las categorías «niños» y «salud y estado físico».

> *«Como defensores de la privacidad, creemos que las habilidades relacionadas con 'niños' y 'salud' deben cumplir con estándares más altos con respecto a la privacidad de los datos. Si bien estas aplicaciones facilitan la interacción de los usuarios con dispositivos inteligentes y refuerzan una serie de servicios adicionales, también plantean problemas de seguridad y privacidad debido al entorno personal en el que operan»,* dijeron los investigadores.