I. DATOS GENERALES:

Clase de alerta: Técnica de ataque

Tipo de incidente: Fuerza Bruta

Nivel de riesgo: Medio

II. ALERTA

Investigadores han detectado la ejecución de una técnica de ataque de tipo de fuerza bruta que inhabilitaría los controles de acceso basados en huellas digitales, lo cual pone en riesgo la privacidad de los activos de información.

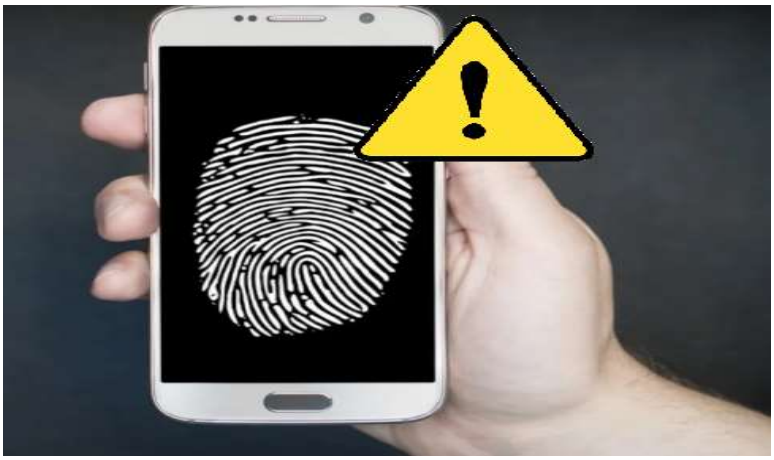

Figura 1.- lustración relacionada a la técnica de ataque BRUTEPRINT
Fuente: Elaboración Propia

III. INTRODUCCIÓN

La técnica de ataque denominada “BRUTEPRINT” se enfoca en anular el límite de intentos de los intentos de control biométrico existentes den dispositivos Android. El límite de intentos se anula debido a la inhabilitación de las funciones Cancel-After-Match-Fail CAMF y Match-After-Lock MAL.

La vulnerabilidad a las funciones de contabilización checksum Considerando que el ataque asume la posesión del dispositivo en manos del ciber atacante, el objetivo del ataque es realizar intentos ilimitados de autenticación a partir de una base de datos de patrones de autenticación biométrica.

El proceso de ataque ha sido probado en 10 diferentes modelos y marcas de teléfonos inteligentes, evidenciándose diferentes niveles de compromiso del sistema respecto del acceso a los dispositivos con sistemas operativos tanto Android como iOS.

IV. VECTOR DE ATAQUE:

- Ejecución directa de técnica en dispositivo.

V. IMPACTO:

- Filtración de activos de información.
- Uso ilícito de dispositivo para otros ataques.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Actualizar el sistema operativo del dispositivo.
- Descargar aplicaciones de sitios autorizados.
- Establecer múltiples factor de autenticación para el acceso al dispositivo.

VII. REFERENCIAS:

- Toulas, B. Bleeping Computer: Android phones are vulnerable to fingerprint brute-force attacks. (21 de 05 de 2023). Obtenido de https://www.bleepingcomputer.com/news/security/android-phones-are-vulnerable-to-fingerprint-brute-force-attacks/.
- Centro Nacional de Seguridad Digital. Alerta Integral de Seguridad Digital (23 de 05 de 2023). Obtenido de https://cdn.www.gob.pe/uploads/document/file/4591821/Alerta%20integrada%20de%20seguridad%20digital%20120-2023-CNSD.pdf