	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 120	**Fecha: 23-05-2023**
		Página 9 de 46

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Los piratas informáticos utilizan la técnica de intercambio de SIM para obtener acceso a las máquinas de Microsoft Azure		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G01
Clasificación temática familia	Fraude		

Descripción

ANTECEDENTES:

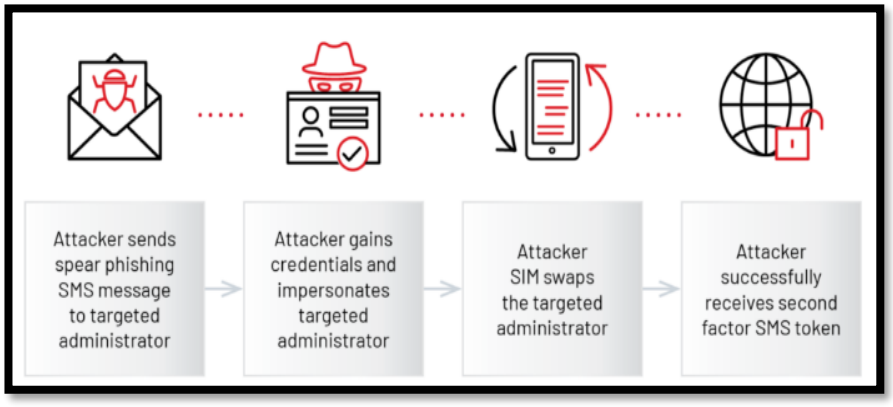
El 20 de mayo del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se ha detectado a un grupo de amenazas motivado financieramente conocido como 'UNC3944' que emplea técnicas de phishing y de intercambio de SIM para tomar el control de las cuentas de administrador de Microsoft Azure.

DETALLES:

Permitiéndoles explotar la consola serial de Azure en máquinas virtuales para la instalación persistente de software de administración remota y vigilancia encubierta a través de extensiones de Azure.

UNC3944, un grupo de amenaza identificado, ha estado operando activamente desde mayo de 2022, según informó Mandiant. Su objetivo principal es extraer datos confidenciales de organizaciones objetivo aprovechando el servicio de computación en la nube de Microsoft.

Aquí, para firmar sus controladores de kernel, los actores de amenazas utilizaron cuentas de desarrollador de hardware de Microsoft robadas a través de las cuales operaron sus procedimientos. Para el acceso inicial, los actores de amenazas se basan principalmente en las credenciales comprometidas de los administradores u otras cuentas privilegiadas.



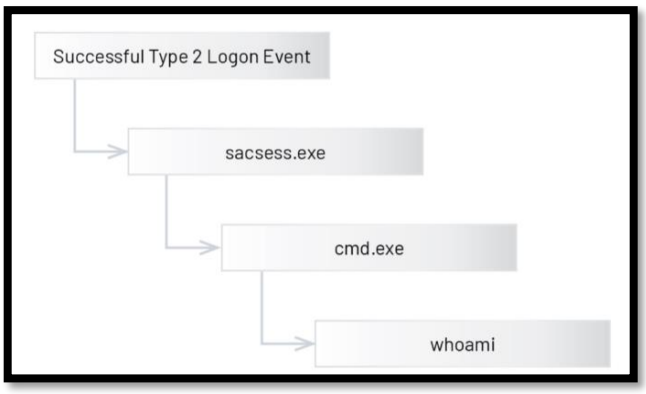
El atacante utiliza el phishing de SMS y el intercambio de SIM para hacerse pasar por usuarios privilegiados y engañar a los agentes de la mesa de ayuda para que proporcionen códigos de reinicio de múltiples factores. Aún así, Mandiant carece de datos suficientes para identificar los detalles de la técnica de intercambio de SIM.

UNC3944 emplea Azure Extensions durante la fase de ataque subsiguiente, empleando vigilancia encubierta y técnicas de recopilación de información para camuflar sus actividades maliciosas como operaciones diarias ordinarias, mezclándose efectivamente con las actividades cotidianas.

Las extensiones de Azure son características y servicios adicionales diseñados para mejorar la funcionalidad y la automatización de las máquinas virtuales de Azure, y ofrecen una variedad de capacidades adicionales y opciones de automatización de tareas cuando están integradas. Al ejecutarse dentro de la máquina virtual y utilizarse principalmente con fines legítimos, estas extensiones poseen un sigilo inherente, lo que las hace parecer menos sospechosas.

El actor de amenazas explotó las capacidades inherentes de las extensiones de diagnóstico de Azure, específicamente la función "CollectGuestLogs", para recopilar archivos de registro del punto final comprometido. Para el acceso directo de la consola administrativa a las máquinas virtuales, UNC3944 aprovecha Azure Serial Console.

Esto permite a los actores de amenazas operar el puerto serie para ejecutar comandos a través del símbolo del sistema.



RECOMENDACIONES:

- Limitar el acceso de administración remota y se abstengan de usar SMS como una opción de autenticación multifactor siempre que sea factible para mejorar las medidas de seguridad.
- Mitigar los riesgos potenciales al reducir la exposición al acceso no autorizado y mejorar los protocolos de autenticación.

Fuentes de información	▪ hxxps://gbhackers.com/sim-swapping-technique-to-gain-access-to-microsoft-azure-machines/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 120	**Fecha: 23-05-2023**
		Página 11 de 46

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Los teléfonos Android son vulnerables a los ataques de fuerza bruta de huellas dactilares		
Tipo de ataque	Ataque de fuerza Bruta	Abreviatura	AtaqFueBru
Medios de propagación	Red, Correo, Navegación de Internet		
Código de familia	A	Código de subfamilia	A01
Clasificación temática familia	Acceso no autorizado		

Descripción

ANTECEDENTES:

El 21 de mayo del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se tiene conocimiento los Investigadores de Tencent Labs y la Universidad de Zhejiang han presentado un nuevo ataque llamado 'BrutePrint', que fuerza la fuerza bruta con las huellas dactilares en los teléfonos inteligentes modernos para eludir la autenticación del usuario y tomar el control del dispositivo.

DETALLES:

Los ataques de fuerza bruta se basan en muchos intentos de prueba y error para descifrar un código, clave o contraseña y obtener acceso no autorizado a cuentas, sistemas o redes.

Los investigadores chinos lograron superar las salvaguardas existentes en los teléfonos inteligentes, como los límites de intento y la detección de vida que protegen contra los ataques de fuerza bruta, al explotar lo que afirman son dos vulnerabilidades de día cero.

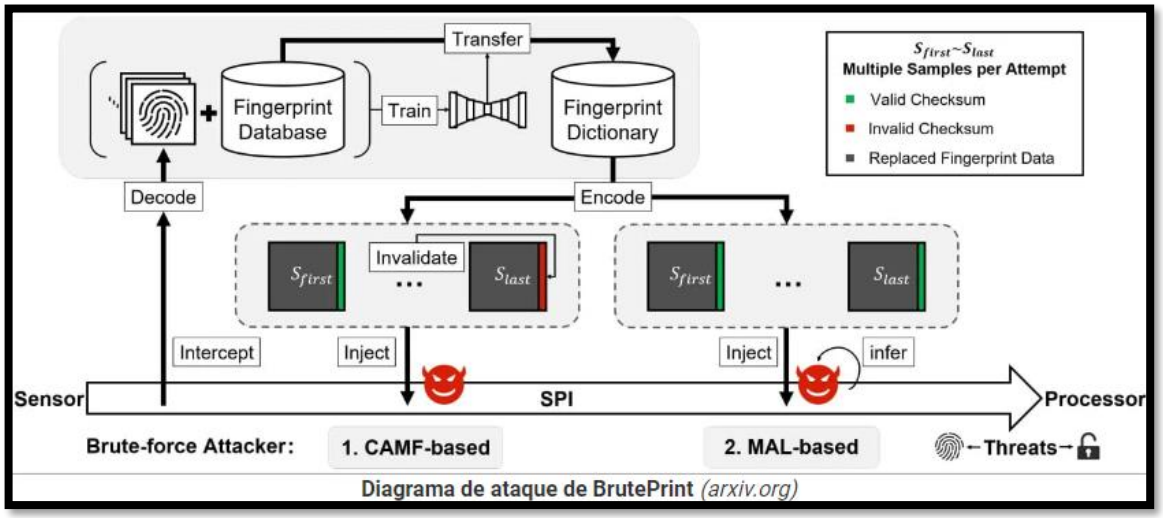


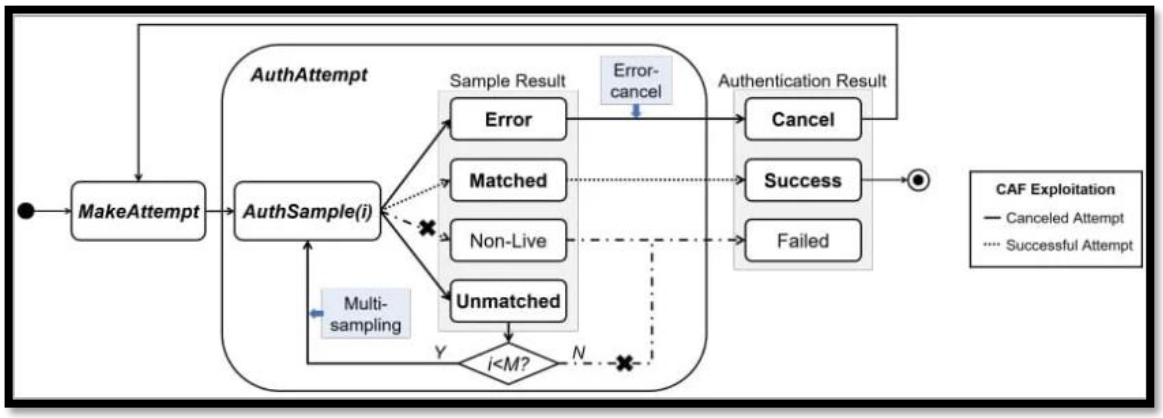
Diagrama de ataque de BrutePrint *(arxiv.org)*

Los autores del artículo técnico publicado en Arxiv.org también encontraron que los datos biométricos en la interfaz periférica en serie (SPI) de los sensores de huellas dactilares no estaban protegidos adecuadamente, lo que permitía un ataque de intermediario (MITM) para secuestrar imágenes de huellas dactilares. Los ataques BrutePrint y SPI MITM se probaron contra diez modelos populares de teléfonos inteligentes, logrando intentos ilimitados en todos los dispositivos Android y HarmonyOS (Huawei) y diez intentos adicionales en dispositivos iOS.

La idea de BrutePrint es realizar un número ilimitado de envíos de imágenes de huellas dactilares al dispositivo de destino hasta que coincida la huella dactilar definida por el usuario.

El atacante necesita acceso físico al dispositivo de destino para lanzar un ataque BrutePrint, acceso a una base de datos de huellas dactilares que se puede adquirir a partir de conjuntos de datos académicos o fugas de datos biométricos.

Al contrario de cómo funciona el descifrado de contraseñas, las coincidencias de huellas dactilares usan un umbral de referencia en lugar de un valor específico, por lo que los atacantes pueden manipular la Tasa de falsa aceptación (FAR) para aumentar el umbral de aceptación y crear coincidencias más fácilmente.



BrutePrint se encuentra entre el sensor de huellas digitales y el entorno de ejecución confiable (TEE) y explota la falla CAMF para manipular los mecanismos de muestreo múltiple y cancelación de errores de la autenticación de huellas digitales en los teléfonos inteligentes.

CAMF inyecta un error de suma de verificación en los datos de la huella digital para detener el proceso de autenticación en un punto prematuro. Esto permite a los atacantes probar las huellas dactilares en el dispositivo de destino mientras que sus sistemas de protección no registrarán los intentos fallidos, por lo que les dará intentos infinitos.

El modo de bloqueo es un sistema de protección que se activa después de un cierto número de intentos de desbloqueo consecutivos fallidos. Durante el "tiempo de espera" del bloqueo, el dispositivo no debería aceptar intentos de desbloqueo, pero MAL ayuda a eludir esta restricción.

El componente final del ataque BrutePrint utiliza un sistema de "transferencia de estilo neuronal" para transformar todas las imágenes de huellas dactilares en la base de datos para que parezcan escaneadas por el sensor del dispositivo de destino. Esto hace que las imágenes parezcan válidas y, por lo tanto, tengan mejores posibilidades de éxito.

RECOMENDACIONES:

- Mantén el sistema actualizado y parches de seguridad automáticos.
- Descarga aplicaciones solamente de fuentes confiables, esto garantiza que las aplicaciones sean legítimas.
- Establezca contraseñas únicas para todas sus cuentas y guárdelas de forma segura.

Fuentes de información	▪ hxxps://www.bleepingcomputer.com/news/security/android-phones-are-vulnerable-to-fingerprint-brute-force-attacks/#comments