Se ha encontrado una nueva cepa simple pero muy peligrosa de malware para Android en la naturaleza, que roba las cookies de autenticación de los usuarios de la navegación web y otras aplicaciones, incluidas Chrome y Facebook, instaladas en los dispositivos comprometidos.

Nombrado como *«Cookiethief»* por investigadores de Kaspersky, el troyano adquiere derechos de root de superusuario en el dispositivo de destino, y posteriormente, transfiere cookies robadas a un servidor remoto de comando y control (C2) operado por atacantes.

> *«Esta técnica de abuso no es posible debido a una vulnerabilidad en la aplicación de Facebook o en el navegador en sí. El malware podría robar archivos de cookies de cualquier sitio web de otras aplicaciones de la misma forma y lograr resultados similares»,* dijeron los investigadores.

Las cookies son pequeñas piezas de información que los sitios web utilizan por lo general par diferencia a un usuario de otro, ofrecer continuidad en la web, rastrear sesiones de navegación en distintos sitios web, servir contenido personalizado y cadenas relacionadas con anuncios dirigidos.

Debido a que las cookies en un dispositivo permiten a los usuarios permanecer conectados a un servicio sin tener que iniciar sesión repetidamente, Cookiethief tiene como objetivo explotar el mismo comportamiento para permitir a los atacantes obtener acceso no autorizado a las cuentas de las víctimas sin conocer sus contraseñas de cuentas en línea reales.

> *«De esta forma, un pirata informático armado con una cookie puede hacerse pasar por la víctima desprevenida y usar la cuenta de este último beneficio personal»*, agregaron los investigadores.

Kaspersky teoriza que podría haber más formas en que el troyano podría aterrizar en el dispositivo, incluida la plantación de dicho malware en el firmware del dispositivo antes de la compra o la explotación de vulnerabilidades en el sistema operativo para descargar aplicaciones maliciosas.

Una vez que el dispositivo está infectado, el malware se conecta a una puerta trasera, denominada «Bood», instalada en el mismo teléfono inteligente para ejecutar comandos de superusuario que facilitan el robo de cookies.

Los atacantes evita la protección multinivel de Facebook

Facebook tiene medidas de seguridad para bloquear cualquier intento de inicio de sesión sospechoso, como direcciones IP, dispositivos y navegadores que nunca antes se utilizaron para iniciar sesión en la plataforma.

Sin embargo, los piratas informáticos solucionaron el problema aprovechando la segunda aplicación de malware, llamada *«Youzicheng»,* que crea un servidor proxy en el dispositivo infectado para suplantar la ubicación geográfica del propietario de la cuenta para que las solicitudes de acceso sean legítimas.

> *«Al combinar estos dos ataques, los ciberdelincuentes pueden obtener un control completo sobre la cuenta de la víctima y no levantar sospechas de Facebook»,* dijeron los investigadores.

Aún no está claro qué buscan realmente los atacantes, pero los investigadores encontraron una página que se encuentra en los servicios de publicidad del servidor C2 para distribuir spam en redes sociales y mensajeros, llevándolos a la conclusión de que los delincuentes

podrían aprovechar Cookiethief para secuestrar las redes sociales de los usuarios.