Un investigador de seguridad que hace un año omitió la característica de privacidad macOS de Apple, encontró nuevamente una nueva forma de eludir las advertencias de seguridad al realizar «*clics sintéticos*» en nombre de los usuarios in requerir de su interacción.

Apple introdujo en junio pasado, una función de seguridad básica en MacOS que obligó a todas las aplicaciones a tomar el permiso de los usuarios antes de acceder a datos o componentes confidenciales en el sistema, incluida la cámara o micrófono del dispositivo, ubicación de datos, mensajes e historial de navegación.

Los clics sintéticos son clics invisibles y programáticos generados por un programa de software en lugar de un humano. MacOS tiene la funcionalidad integrada para clics sintéticos, pero como una función de accesibilidad para que aquellas personas con discapacidad puedan interactuar con la interfaz del sistema.

Por lo tanto, la función solo está disponible para las aplicaciones aprobadas por Apple, lo que evita que las aplicaciones maliciosas abusen de dichos clics.

Sin embargo, el investigador de seguridad, Patrick Wardle, encontró una falla crítica en MacOS que podría haber permitido que las aplicaciones malintencionadas instaladas en un sistema específico virtualmente hicieran «clic» en los botones de aviso de seguridad sin la interacción del usuario o el consentimiento real.

Aunque Apple solucionó el problema luego de algunas semanas de la divulgación pública, Wardle demostró una vez más de forma pública una nueva forma de evitar que las aplicaciones realicen «*clics sintéticos*» para acceder a los datos privados de los usuarios sin su permiso explícito.

Wardle dijo a THN que en Mojave, existe un error de validación en la forma en que MacOS verifica la integridad de las aplicaciones en la lista blanca. El sistema operativo comprueba la existencia del certificado digital de una aplicación, pero no puede validar si la aplicación fue manipulada.

> *«Los intentos del sistema para verificar/validar en estas aplicaciones permitidas en la lista blanca no se han subvertido, pero su comprobación es defectuosa, lo que significa que un atacante puede subvertir cualquiera de estas, además de agregar o inyectar código para realizar clics sintéticos arbitrarios, por ejemplo, para interactuar con las alertas de seguridad y privacidad en Mojave para acceder a la ubicación del usuario, el micrófono, cámara web, fotos, registros de llamadas, SMS»*, dijo Wardle.
>
> *«Esas aplicaciones de la lista blanca no tienen que estar presentes en el sistema. El atacante podría traer una de las aplicaciones de la lista blanca al sistema y ejecutarla en segundo plano, para generar clics»*, agregó.

Mientras demostraba la vulnerabilidad de día cero en la conferencia de Objective By the Sea, en Monte Carlo, Wardle abusó de VLC Player, una de las aplicaciones aprobadas de Apple, para incluir su malware como un complemento no firmado y realizar clics sintéticos en un mensaje de consentimiento programático sin necesidad de ninguna interacción del usuario.

Wardle se refiere a la nueva vulnerabilidad de clics sintéticos como un *«ataque de segunda etapa»*, lo que significa que un atacante debería tener acceso remoto a la computadora MacOS de la víctima o haber instalado una aplicación maliciosa.

El investigador reportó sus hallazgos a Apple la semana pasada y la compañía confirmó haber recibido su informe, pero no aclaró cuándo planea solucionar el problema.