El grupo de hackers detrás de la herramienta de desbloqueo *«Unc0ver»*, lanzó una nueva versión del software que es capaz de desbloquear todos los iPhone, incluyendo los que ejecutan la última versión de iOS, 13.5.

El desarrollador principal de Unc0ver, Pwn20wnd, dijo que es el primera jailbreak de día cero lanzado desde la versión 8 de iOS, y dijo que *«todos los demás jailbreak lanzados desde iOS 9 utilizaron exploits de 1 día que fueron parcheados en la siguiente versión beta o en el hardware».*

Aunque no mencionó qué vulnerabilidad en iOS fue explotada para el desarrollo de la última versión, el sitio web de Unc0ver también destacó las extensas pruebas que se realizaron para garantizar la compatibilidad en una amplia gama de dispositivos, desde el iPhone 6S hasta los nuevos modelos iPhone 11 Pro Max, que abarcan las versiones iOS 11.0 a iOS 13.5, pero excluyen las versiones 12.3 a 12.3.2 y 12.4.2 a 12.4.5.

«Utilizando las excepciones de sandbox del sistema nativo, la seguridad permanece intacta mientras se permite el acceso a los archivos de jailbreak», según Unc0ver, lo que quiere decir que la instalación del nuevo jailbreak probablemente no comprometerá las protecciones de sandbox de iOS.

El jailbreak es una escalada de privilegios que funciona explotando fallas en iOS para otorgar a los usuarios acceso root y control total sobre sus dispositivos. Esto permite a los usuarios de iOS eliminar todas las restricciones de software impuestas por Apple, permitiendo así el acceso a personalizaciones adicionales y aplicaciones prohibidas.

Sin embargo, esto debilita la seguridad del dispositivo, dejándolo vulnerable a todo tipo de ataques de malware. Los riesgos de seguridad adicionales, junto con el bloqueo constante de hardware y software de Apple, dificultaron el jailbreak de los dispositivos de forma deliberada.

Además, los jailbreaks tienden a ser muy específicos y se basan en vulnerabilidades previamente divulgadas, y dependen mucho del modelo de iPhone y la versión de iOS, para

que puedan replicarse exitosamente.

El desarrollo se produce cuando el corredor de exploits 0-Day, Zerodium, dijo que ya no compraría vulnerabilidades RCE de iOS durante los próximos meses, citando *«una gran cantidad de envíos relacionados con estos vectores».*

En agosto pasado, Pwn20wnd explotó una falla de SockPuppet (CVE-2019-8605) descubierta por Ned Williamson, para lanzar una versión pública de jailbreak, por lo que es la primera vez que se desbloquea un firmware actualizado en años, luego de que Apple reintrodujera de forma accidental un defecto previamente parcheado en iOS 12.4. La compañía luego lanzó una solución en iOS 12.4.1 para abordar la vulnerabilidad.

Después, en septiembre, un investigador de seguridad cibernética publicó los detalles de un exploit de bootrom permanente no parcheable, denominado checkm8, que podría utilizarse para hacer jailbreak a casi todos los tipos de dispositivos móviles de Apple lanzados entre 2011 y 2017, incluidos los iPhone, iPad, Apple Watch y Apple TV.

Aunque el nuevo jailbreak aprovecha una vulnerabilidad Zero Day aún desconocida, es seguro que Apple lance una actualización de seguridad en las siguientes semanas para solucionar la vulnerabilidad explotada por Unc0ver.