Peligroso Backdoor Se Encuentra En Los Smartphones Chinos

Existe un nuevo y peligroso Backdoor del que deben de preocuparse los propietarios de teléfonos inteligentes de China. Los investigadores de seguridad en Palo Alto Networks, han descubierto un Backdoor integrado en millones de teléfonos inteligentes **producidos por Coolpad**.

Este Backdoor ha sido llamado ***CoolReaper***, la puerta trasera pone a más de 10 millones de propietarios de teléfonos inteligentes en potencial riesgo. La firma de seguridad llevó a cabo investigaciones después que los usuarios se quejaron de algunos mensajes sobre actividades sospechosas en sus teléfonos. Después de descargar múltiples **copias del ROM** utilizado en el teléfono de CoolPad, se encontró que «la mayoría de las ROMs contenía **el Backdoor CoolReaper**«.

Un total de **77 ROMs fueron descargads**, y en 4 de ellos se encontraron incluidas el Backdoor. Unit 42 ha publicado un documento que detalla la capacidad del malware, pero los usuarios han informado de la instalación de software y anuncios emergentes no autorizados. Curiosamente, se ha informado de que CoolPad borra mensajes del administrador de mensajes. Por el momento no hay evidencia de que los ***dispositivos de Coolpad vendidos fuera de China y Taiwán*** están afectados, pero esto no es un consuelo para aquello que pueden estar en riesgo.

El CoolReaper es de preocupar, ya que contiene las siguientes características según el grupo de investigadores:

- Descargar, instalar o activar cualquier aplicación de

Android sin el consentimiento del usuario o notificación alguna.
- Borrar datos de usuario, desinstalar aplicaciones existentes, o aplicaciones del sistema y deshabilitarlas.
- Notificación a los usuarios de una falsificación Over-the-air (OTA) de actualización que no actualiza el dispositivo, pero instala aplicaciones no deseadas.
- Enviar o insertar mensajes SMS o MMS arbitrarias en el teléfono.
- Marcar a números de teléfono de forma arbitraria.
- Subir información acerca del dispositivo, su ubicación, uso de aplicaciones, historial de llamadas y SMS a un servidor de Coolpad.

El documento menciona:

> *En noviembre, un investigador de seguridad white hat, ha identificado una vulnerabilidad en el sistema de control de servicios de segundo plano llamada CoolReaper, lo que permitió ver cómo Coolpad controla la información por medio de un Backdoor.*

El trabajo de investigación da un desglose detallado de los resultados y advierte:

> *El impacto conocido de **CoolReaper hasta ahora se limita a China y Taiwán**, pero la posición de Coolpad en los planes de mercado y expansión mundial significa, que este Backdoor puede estar presente como una amenaza para los usuarios de Android en todo el mundo.*

CoolPad es el sexto **fabricante de teléfonos inteligentes más grande del mundo**, con una cuota global del 3,7 por ciento del mercado. Ademas se ubicó como el tercer fabricante más grande de China. La compañía se está expandiendo gradualmente en los EE.UU. y Europa, lo cual es preocupante. Hasta el momento es

difícil decir mucho sobre el **origen de la puerta trasera**. Los investigadores han determinado que ha existido al menos desde octubre del 2013, pero no es claro si existe o no una conexión directa con el gobierno chino.