| | | | |
|---|---|---|---|
| Nro. Alerta: | EC-2022-73 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTA DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
| TLP: | TLP:BLANCO | | |
| Fecha: | 20-mayo-2022 | **Ejecución de malware en dispositivos iPhone, Incluso si está apagado** | Versión 1.1 |

## I. DATOS GENERALES:

**Clase de alerta:** Malware
**Tipo de incidente:** Código malicioso
**Nivel de riesgo:** Media

## II. ALERTA

Investigadores descubrieron y alertaron sobre la posibilidad de ejecutar malware sobre dispositivos iPhone, incluso cuando estén apagados. Esto se debe a que, cuando el iPhone está apagado, ciertos chips inalámbricos permanecen encendidos, lo que permite que el teléfono siga enviando señales que pueden ayudar a localizarlo.

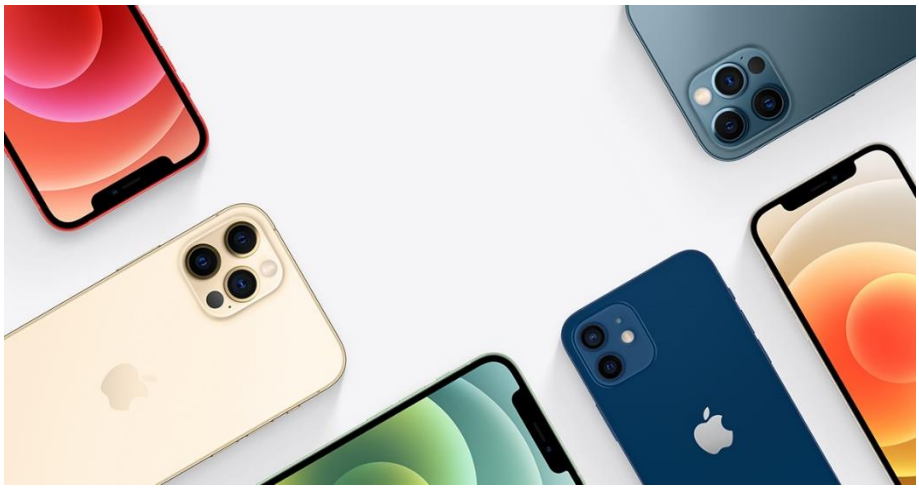

**Figura 1.** Fotos de Iphones
**Fuente:** https://www.apple.com/la/iphone/buy/ec/

## III. INTRODUCCIÓN

Académicos del Laboratorio de Redes Móviles Seguras (SEEMOO) de la Universidad Técnica de Darmstadt en Alemania, escribieron un artículo titulado "Evil Never Sleeps: When Wireless Malware Stays On After Turning Off iPhones". El cual abarca un análisis de seguridad de la función Find My.



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | EC-2022-73 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTA DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
| TLP: | TLP:BLANCO | | |
| Fecha: | 20-mayo-2022 | **Ejecución de malware en dispositivos iPhone, Incluso si está apagado** | Versión 1.1 |

El primer análisis de seguridad de su tipo de la función Find My de iOS identificó una nueva superficie de ataque que hace posible manipular el firmware y cargar malware en un chip Bluetooth que se ejecuta mientras el iPhone está "apagado".

El mecanismo aprovecha el hecho de que los chips inalámbricos relacionados con Bluetooth, la comunicación de campo cercano (NFC) y la banda ultra-ancha (UWB) siguen funcionando mientras iOS se apaga al entrar en un modo de bajo consumo (LPM) de "reserva de energía".

Esto se hace para habilitar funciones como Find My y facilitar las transacciones de Express Card, los tres chips inalámbricos tienen acceso directo al elemento seguro, dijeron académicos del Laboratorio de Redes Móviles Seguras ( SEEMOO ) de la Universidad Técnica de Darmstadt, en su artículo titulado "Evil Never Sleeps".

Las características de LPM, recientemente introducidas el año pasado con iOS 15, hacen posible rastrear dispositivos perdidos utilizando la red Find My, incluso cuando se han quedado sin batería o se han apagado. Los dispositivos actuales con soporte de banda ultra-ancha incluyen iPhone 11, iPhone 12 y iPhone 13.

Los investigadores dijeron en su artículo titulado "Evil Never Sleeps", que pudieron demostrar que es posible instalar malware en el chip Bluetooth. Sin embargo, es importante tener en cuenta que, en este momento, esta investigación es principalmente teórica y no hay evidencia de que este tipo de ataque se haya utilizado en la naturaleza. Además, como señalan los investigadores en el documento, los piratas informáticos primero tendrían que hackear y liberar el iPhone para poder acceder al chip Bluetooth y explotarlo, lo que podría hacerlo un poco redundante en la mayoría de los casos.

Los investigadores concluyen que la implementación de Apple de este modo de bajo consumo en última instancia mejora la seguridad de los usuarios porque les permite encontrar un teléfono perdido o robado incluso si está apagado. Pero debido a que los chips inalámbricos todavía están encendidos, también representan un nuevo modelo de amenaza.

## IV. VECTOR DE ATAQUE

Red, hardware vulnerable



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | EC-2022-73 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTA DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
| TLP: | TLP:BLANCO | | |
| Fecha: | 20-mayo-2022 | **Ejecución de malware en dispositivos iPhone, Incluso si está apagado** | Versión 1.1 |

## V. IMPACTO

Según el estudio publicado por los investigadores, el enfoque central se encuentra en el chip de Bluetooth, que funciona independientemente del procesador central del iPhone. Este chip no está firmado, por lo que no tiene protección contra modificaciones y los atacantes podrían ejecutar malware de Bluetooth incluso después del apagado del teléfono. Después, este chip está ligado al elemento de seguridad en el chip NFC del iPhone, que es el encargado de asegurar y guardar información sensible, como Apple Pay. En caso de que un criminal ataque el chip Bluetooth, también podría obtener acceso al chip NFC. Por último, este modo de bajo gasto de batería está implementado a nivel hardware, lo que quiere decir que Apple no puede corregirlo con un parche.

## VI. IMPACTO

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Permanecer atentos a los canales oficiales de comunicación del fabricante, a la espera de una posible mitigación o barrera de seguridad a implementar para evitar la ocurrencia de un posible incidente de explotación de esta vulnerabilidad.

## VII. DESCARGO DE RESPONSABILIDAD

- La información en esta alerta es con fines informativos. El Centro de Respuestas de ARCOTEL, EcuCERT, no respalda ningún producto o servicio comercial, incluidos aquellos sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante, no constituye ni implica respaldo, recomendación o favorecimiento por parte de EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | EC-2022-73 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTA DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
| TLP: | TLP:BLANCO | | |
| Fecha: | 20-mayo-2022 | **Ejecución de malware en dispositivos iPhone, Incluso si está apagado** | Versión 1.1 |

## VIII. REFERENCIAS:

THE HACKERS NEWS (16 de mayo de 2022). Researchers Find Potential Way to Run Malware on iPhone Even When it's OFF. Obtenido de: https://thehackernews.com/2022/05/researchers-find-way-to-run-malware-on.html

VICE (16 de mayo de 2022). *Malware Can Be Loaded Even Onto Phones That Are Turned Off, Researchers Show*. Obtenido de: https://www.vice.com/en/article/g5q4vj/malware-can-be-loaded-even-onto-phones-that-are-turned-off-researchers-show

FLIPBOARD (16 de mayo de 2022). *Malware Can Be Loaded Even Onto Phones That Are Turned Off, Researchers Show*. Obtenido de: https://flipboard.com/@h3adhuntr/cybersecurity-fucpihpbz/malware-can-be-loaded-even-onto-phones-that-are-turned-off-researchers-show/a-GPCeXEIqTJGnW1ItrpfE8g%3Aa%3A549267514-1c46f5192e%2Fdigg.com

QORE (17 de mayo de 2022). *Investigadores inventan malware que afecta iPhones apagados*. Obtenido de: https://www.qore.com/noticias/83737/Investigadores-inventan-malware-que-afecta-iPhones-apagados

LA VERDAD (18 de mayo de 2022). *Malware en el iPhone puede ejecutarse incluso cuando está apagado*. Obtenido de: https://laverdadnoticias.com/tecnologia/Malware-en-el-iPhone-puede-ejecutarse-incluso-cuando-esta-apagado-20220516-0073.html