Pegasus

Christian Peláez Fernández

uo258764@uniovi.es

Resumen

Este trabajo hace una pequeña introducción al spyware Pegasus, uno de los spyware para móviles(iOS) más sofisticados descubiertos hasta la fecha. Describiremos su descubrimiento, su metodología y etapas del ataque, sus características, la organización que lo desarrollo y un pequeño análisis del riesgo que provoca.

1. Introducción

En la actualidad, los móviles son el dispositivo privado más usado por los usuarios. Esto, los convierte en un objetivo de los atacantes, ya que, contienen mucha información privada del dueño: SMS, contactos, llamadas, etc. Una forma de ataque es el uso de spyware, malware cuyo objetivo es espiar la información del teléfono. Un referente de este tipo de programas es Pegasus, un spyware descubierto en 2016 que era capaz de monitorizar todas las comunicaciones de los teléfonos iOS, pasando completamente desapercibido e incluso siendo capaz de autodestruirse para no dejar ningún rastro.

2. Pegasus

2.1. ¿Qué es?

Pegasus es un spyware desarrollado por NSO Group, con el fin de infectar dispositivos iOS y poder espiar todas sus conversaciones.

2.2. Descubrimiento

Ilustración 1. Mensaje sospechoso enviado a Ahmed Mansoor[1]

En la mañana del 10 de agosto de 2016, Ahmed Mansoor (un activista Emiratí) recibió un SMS sospechoso. Al día siguiente, recibió un segundo SMS sospechoso con el mismo texto. El SMS prometía "nuevos secretos" sobre los detenidos torturados en las prisiones de los Emiratos Árabes. Debido a que Ahmed ya había sido objetivo de ataques cibernéticos anteriormente, se puso en contacto con Citizien Lab, enviándoles el SMS sospechoso. Posteriormente, el 12 de agosto Citizien Lab se pone en contacto con la empresa Lookout para realizar una investigación conjunta. El 15 de agosto, comunican a Apple

toda la información que han conseguido investigando el spyware. Finalmente, Apple publica una actualización (iOS 9.3.5) el 25 de agosto que solventa las 3 vulnerabilidades de día 0.

2.3. ¿Cómo funciona?

Pegasus se aprovecha de 3 vulnerabilidades críticas de día 0, llamadas *The Trident Vulnerabilities*.

2.3.1. The Trident Vulnerabilities

- CVE-2016-4657: Memory Corruption in Safari WebKit
  Esta vulnerabilidad en Safari Webkit, permite al atacante ejecutar de manera silenciosa código en el dispositivo del usuario, después de que este haya clicado en un link malicioso.

- CVE-2016-4655: Kernel Information Leak Circumvents *KASLR*
  Para que Pegasus pueda realizar el jailbreak del dispositivo, antes debe de poder determinar la ubicación del kernel en memoria. El Kernel Address Space Layout Randomization (KASLR) hace que esta tarea sea más complicada, ya que mapea el kernel en diferentes e impredecibles zonas de la memoria. A pesar de este impedimento, Pegasus es capaz de ubicar el kernel.

- CVE-2016-4656: Memory Corruption in Kernel leads to Jailbreak
  Gracias a esta vulnerabilidad se realiza el Jailbreak en el dispositivo iOS, tanto en la versión de 32 bits como la de 64.

2.3.2. Etapas del ataque

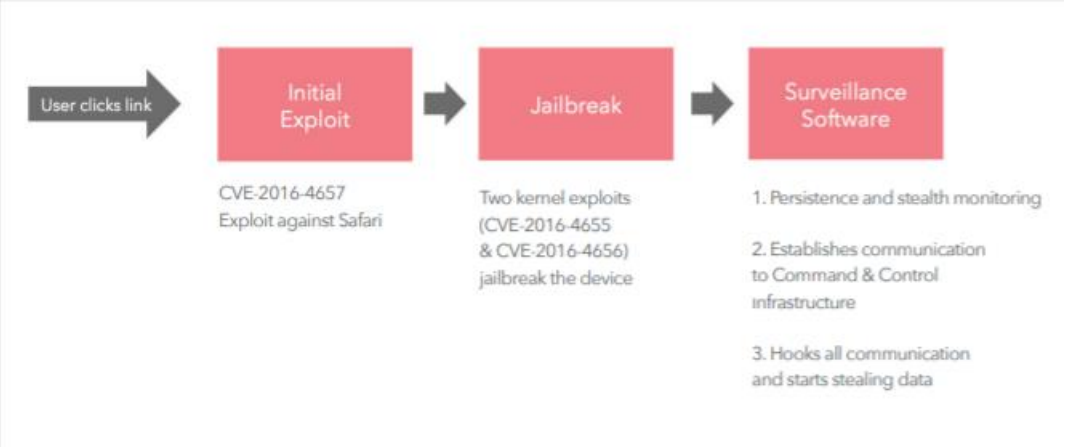

Ilustración 2. Etapas del ataque (mostrado en el informe de Lookout)[2]

El ataque consta de 3 etapas secuenciales.Para que una etapa finalice satisfactoriamente las anteriores ya lo deben de haber hecho. Las etapas son las siguientes:

1) Exposición y vulnerabilidad WebKit: Esta etapa comienza cuando el usuario clica en un link en forma de un archivo HTML, el cual explota la vulnerabilidad (CVE-2016-4657) en WebKit.

2) Jailbreak: En esta etapa se descarga el código malicioso de la etapa anterior. El código malicioso se descarga como paquetes encriptados, de esta manera los controles de red tradicionales son superados. Una vez se descarga el código necesario para explotar el kernel iOS (CVE-2016-4655 y CVE-2016-4656), se descarga y desencripta el paquete necesario para pasar a la etapa 3.

3) Software espía: En esta etapa ya se tienen todas las herramientas descargadas para realizar el espionaje, además de tener el dispositivo con jailbreak. Se instalan las herramientas para interceptar la información en las aplicaciones que se quieran espiar.

Como se puede observar, la secuencia del ataque sigue un esquema básico de phishing.

2.4. Características

Pegasus es un software espía complejo, eficiente y eficaz. Según Lookout, “es el software desarrollado por una entidad privada para atacar móviles más sofisticado, que han investigado” [3]. La complejidad y eficacia de este spyware es debida a varios factores:

- Hace uso de vulnerabilidades no descubiertas (vulnerabilidades de día cero).
- Funciona para diversas versiones de iOS.
- Los mecanismos estándar para comprobar si un dispositivo había sido explotado fallaban.
- Una vez instalado, desactiva la descarga automática de nuevas actualizaciones para el dispositivo.
- Es capaz de autodestruirse, si la situación así lo requiere.
- Monitoriza el estado de la conexión internet del dispositivo y el tipo de red a la que está conectado para determinar el ancho de banda y la capacidad que tendrá para poder enviar datos a través de la red.
- Desactiva la funcionalidad “Deep Sleep” de los móviles.
- La lista completa de aplicaciones de mensajería que puede espiar consta de 16 apps, entre ellas: Gmail, WhatsApp, iMessage, Facebook ,Skype, etc.

Estas son algunas de las funcionalidades que le permiten ser el mayor spyware de móviles descubierto hasta el momento.

2.5. Desarrolladores

Pegasus fue desarrollado por la firma cibernética israelí NSO Group. Según Karspersky: ”La forma de ganarse la vida de esta empresa es desarrollar spyware”[4], el cual vende a quien pague por él.

Pegasus tenía un precio muy elevado en el mercado, NSO Group vendió 300 licencias del software por 8.000.000$[5]

2.6. Riesgos en la seguridad

Lookout mostró en una conferencia un gráfico del nivel de riesgo que produce Pegasus en función del tipo de usuario:

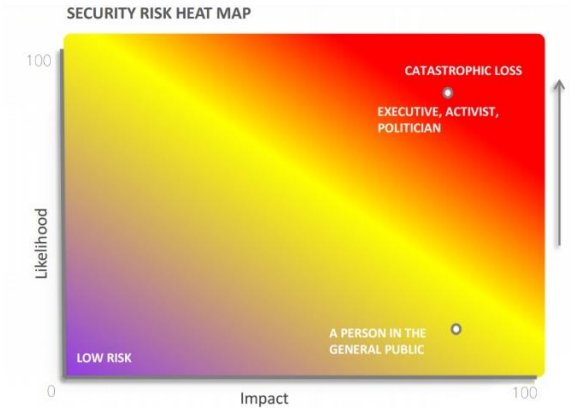

Ilustración 3. Mapa de riesgos mostrado en la conferencia

2.7. Android

NSO Group también ha desarrollado un spyware con las mismas funcionalidades de Pegasus, pero para los móviles Android, este es llamado Chrysaor.

3. Conclusión

Como hemos podido comprobar las vulnerabilidades críticas de día 0, tienen un impacto abrumador. Permiten que malware como Pegasus pueda monitorizar nuestras conversaciones libremente. El mercado de estas vulnerabilidades está actualmente más activo que nunca, por lo que se recomienda que todo dispositivo electrónico esté debidamente actualizado.

4. Referencias

- [1] https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
- [2] https://info.lookout.com/rs/051-esq-475/images/lookout-pegasus-technical-analysis.pdf
- [3] https://info.lookout.com/rs/051-esq-475/images/lookout-pegasus-technical-analysis.pdf
- [4] https://www.kaspersky.es/blog/pegasus-spyware/10374/
- [5] https://www.prensa.com/locales/ruta-pago-NSO-Group_0_4266323503.html

5. Bibliografía y Sitios Consultados

- https://www.youtube.com/watch?v=zyvwoWf6-ag
- https://info.lookout.com/rs/051-esq-475/images/lookout-pegasus-technical-analysis.pdf

- http://cert.europa.eu/static/SecurityAdvisories/CERT-EU-SA2016-136.pdf
- https://es.wikipedia.org/wiki/Pegasus_(spyware)
- https://www.kaspersky.es/blog/pegasus-spyware/10374/
- https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/