Análisis del *malware MiniDuke*

Ignacio Ballesteros González
w140062
05448027V

29 de mayo de 2017

Índice

Resumen

Segunda práctica de la asignatura de *Seguridad de las Tecnologías de la Información*. Se realizará el estudio de una muestra del código malicioso *MiniDuke*. Se ha elegido la opción *(c)* de estudio en base a las normas establecidas.

$$1 + ((5448027 * 726391632) \ mod \ 330) = 175$$

1. Introducción

MiniDuke es un malware que utiliza un *exploit 0-day* de Adobe Reader para lograr acceso a la máquina objetivo. El término de *MiniDuke* también se aplica a la campaña que usaba esta herramienta, enmarcada en una operación de espionaje a gobiernos. [1]

Código malicioso *MiniDuke*

Tipo No autorreplicante

Familia *Spyware, Backdoor, APT*

2. Ficha resumen

Denominación

Origen/autor

Destinatario

Fecha de lazamiento

Fecha de descubrimiento

Tipo de código malicioso

Funcionamiento general

- **Modo de Infección**
- **Modo de replicación**
- **Modo de propagación**
- **Modo de ocultación**
- **Ejecución de la carga**

Tiempo de vulnerabilidad relacionada

Modo de desinfección

Ejemplo de ataque donde se ha empleado

Medidas de seguridad tomadas tras su descubrimiento

Resto de miembros de su familia

Otra información relevante

3. Conclusiones

Referencias

[1] F-Secure. The Dukes, 7 years of Russian cyberspionage. https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf, 9 2015.