Análisis del *malware MiniDuke*

Ignacio Ballesteros González
w140062
05448027V

2 de junio 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 Exfiltración, *Spyware, Backdoor, APT*

2. Ficha resumen

Denominación MiniDuke

Origen/autor The Dukes (Rusia)[1] [1, p. 26]

Destinatario Instituciones gubernamentales y afiliadas. [2, p. 18]

País	**Red**
Ucrania	Gobierno, Empresas privadas
Bélgifa	Embajada / Gobierno
Portugal	Gobierno
Rumanía	Gobierno
Irlanda	Gobierno
Estados Unidos	*Think tank(s)*, Sistema de Salud
Hungría	Social foundation

Fecha de lazamiento *Loader*[2]: julio de 2010. *Backdoor*: mayo de 2011.

Fecha de descubrimiento 27 de febrero de 2013 [3]

Tipo de código malicioso *downloader, backdoor*, exfiltración.

Funcionamiento general

Modo de infección El vector de infección que se ha encontrado ha sido mediante *ingeniería social* con la infección de *PDFs* en *emails*. La vulnerabilidad utilizada fue un *0-day*[3] de Adobe Reader[4] y Acrobat. [4]

2012 CVE-2011-2462
2013 CVE-2013-0640

Modo de replicación No aplica.

Modo de propagación Campañas de *phising*.

Modo de ocultación Uso de vulnerabilidas no conocidas (*0-day*). Comunicación con el exterior mediante *IPs* fiables (*Twitter, Google*) para pasar desapercibido en la exfiltración. Compresión del código del *payload*. [2, p. 5]

[1] Atribución no del todo clara. Basada en las suposiciones del grupo investigador *F-Secure*.

[2] Parte de MiniDuke fue usado antes por otro malware, *PinchDuke*, pero aquí se le llamará *loader*

[3] Vulnerabilidad no conocida hasta el momento del descubrimiento del *malware* que la explota.

[4] Adobe Reader y Acrobat 9.x anterior a 9.5.4, 10.x anterior a 10.1.6, y 11.x anterior a 11.0.02

Ejecución de la carga Usa el mismo *payload* que *Itaduke*. Código *JavaScript* comprimido que detecta el *PDF* de infección y crea un fichero temporal de instalación. Posteriormente pasa a ejecutar un *dropper* específico para las características del ordenador de la víctima. [2]

Tiempo de vulnerabilidad relacionada

Según los últimos datos, el *loader* de *MiniDuke* se ha utilizado desde 2010 hasta 2015. [1] En la figura 1 (en azul) se puede ver el periodo de actividad comparado con el resto de *malware* de su familia.

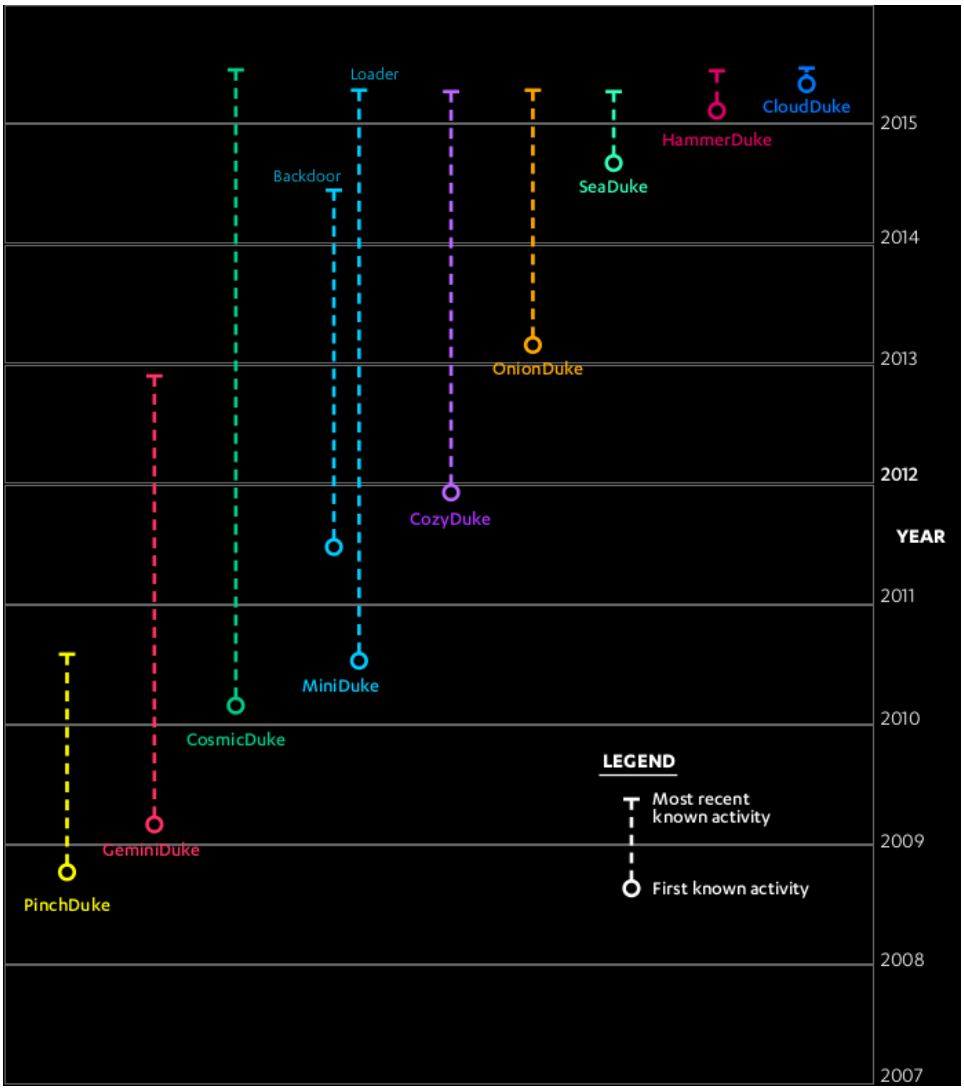

Figura 1: Linea temporal de varias herramientas de la familia *Duke*.

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, 2015.

[2] Costin Raiu, Igor Soumenkov, Kurt Baumgartner, and Vitaly Kamluk. The miniduke mystery: Pdf 0-day government spy assembler 0x29a micro backdoor. https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/themysteryofthepdf0-dayassemblermicrobackdoor.pdf, 2013.

[3] CrySyS Malware Intelligence Team and Kaspersky Labs GREAT Team. Miniduke: Indicators. Technical report, Laboratory of Cryptography and System Security (CrySyS Lab), 2013. http://www.crysys.hu/miniduke/miniduke_indicators_public.pdf.

[4] Marius Tivadar, Bíró Balázs, and Cristian Istrate. A closer look at miniduke. Technical report, Bitdefender, 2013. https://labs.bitdefender.com/wp-content/uploads/downloads/2013/04/MiniDuke_Paper_Final.pdf.