VIII JORNADAS STIC CCN-CERT

La defensa del patrimonio tecnológico frente a los ciberataques

10 y 11 de diciembre de 2014

CCN-CERT centro criptológico nacional

Rootkits
Quién te ha visto y quién te ve

Francisco Oca

Innotec System

francisco_oca@innotecsystem.com

Josechu Migoya

Innotec System

josechu_migoya@innotecsystem.com

Índice

1

Introducción

1 Introducción: ¿qué son?

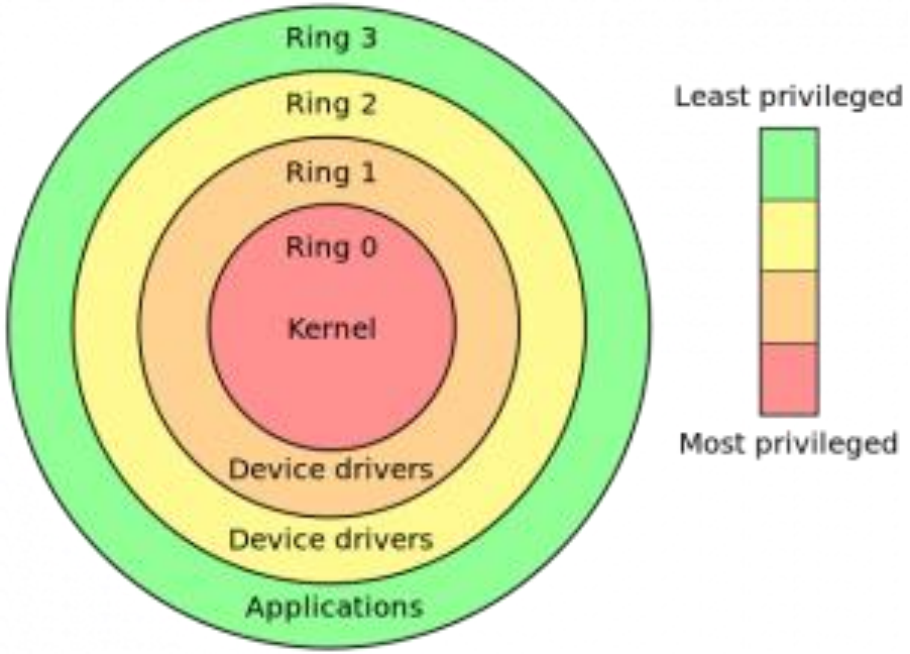
- Un *rootkit* es un tipo de *malware* que se ejecuta con máximos privilegios en el sistema infectado y que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.

- Características
  - *Malware* que funciona a nivel de *kernel*
  - Avanzado
  - Requiere privilegios de administrador
  - Se instala como un driver/módulo

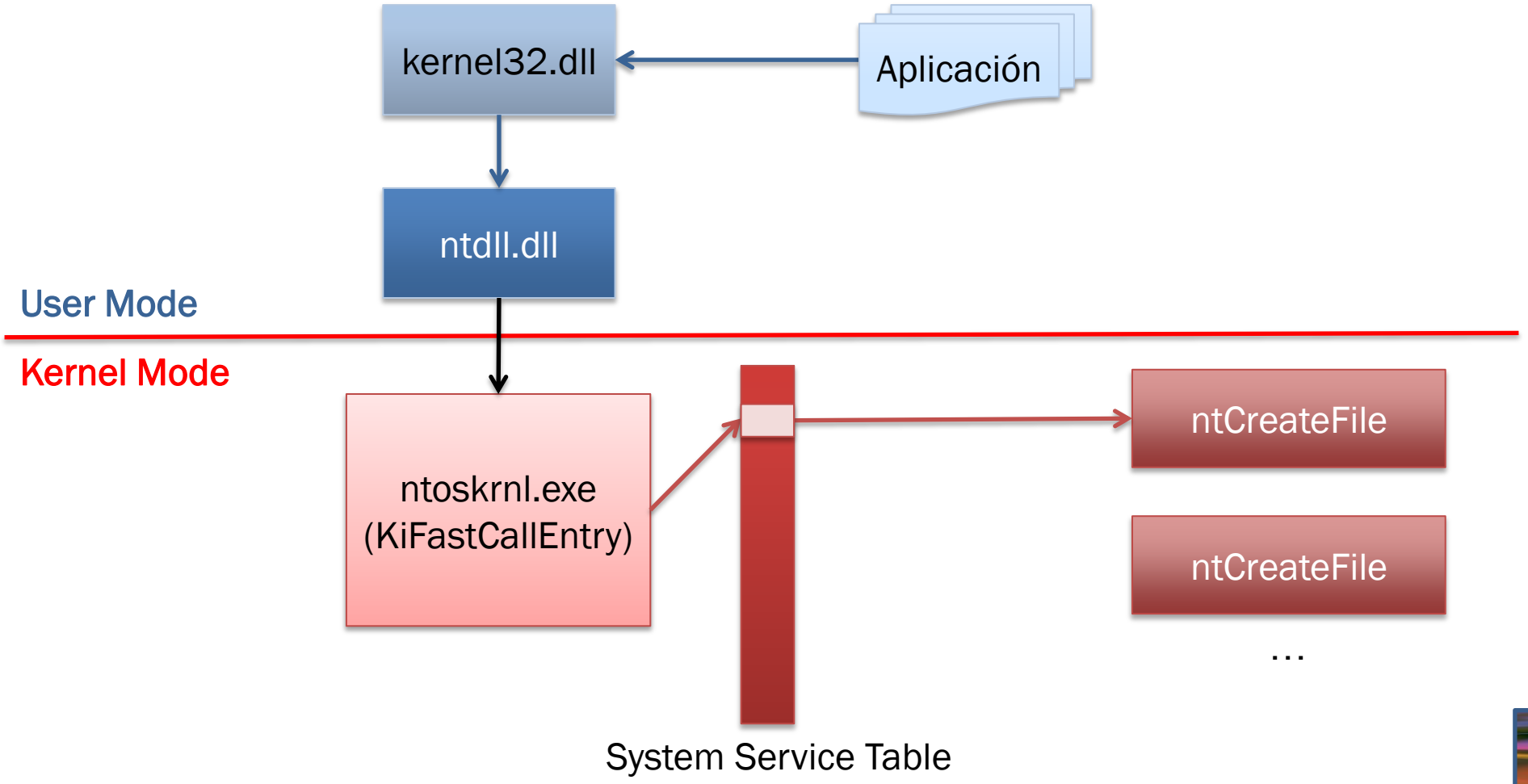
- Trabajar a nivel de *kernel* le permite:
  - Ocultarse
  - Dificultar su detección
  - Tener acceso completo a todos los recursos

- Es una de las amenazas más peligrosas

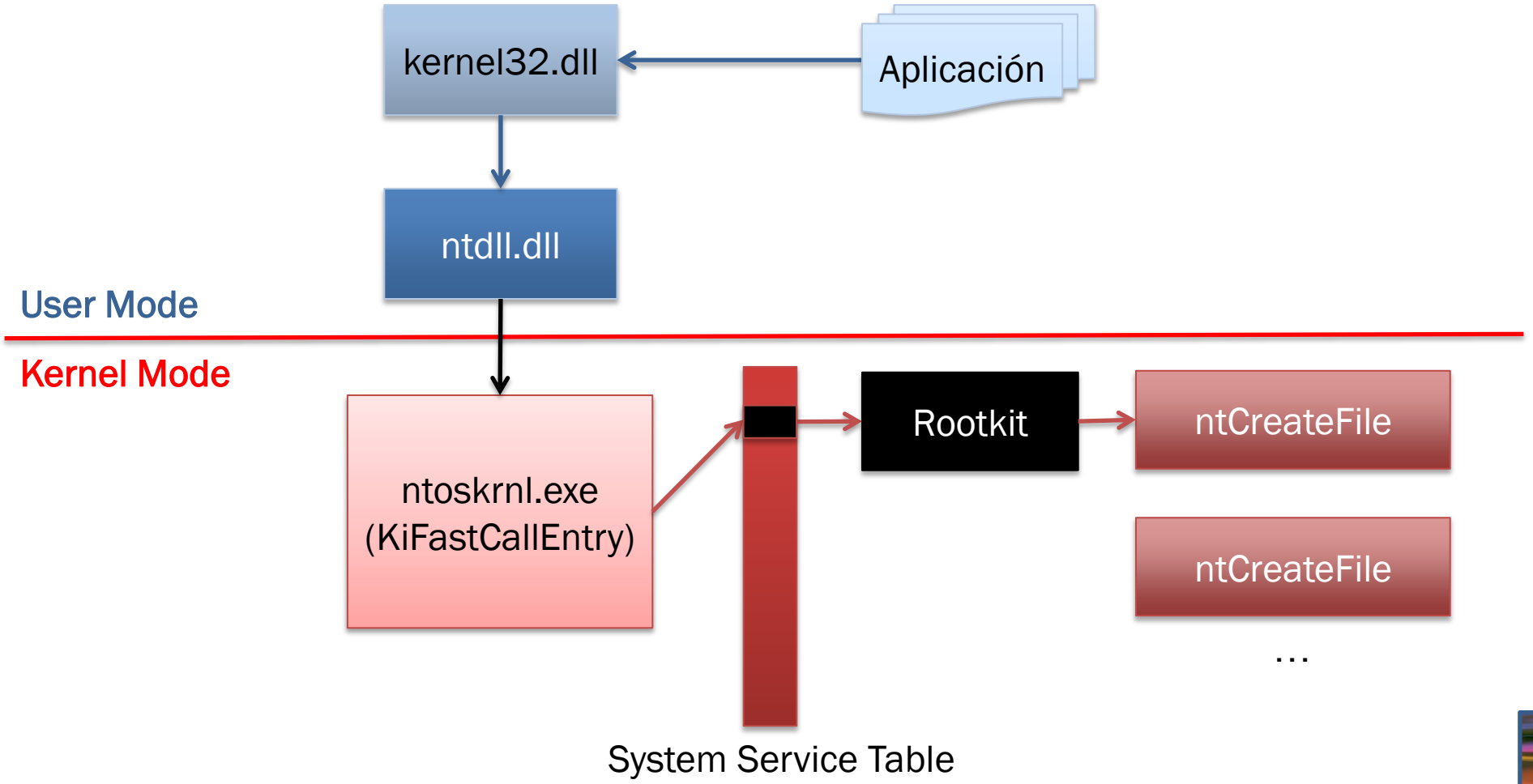
1 Introducción: ¿nivel de *kernel*?



1 Introducción: ¿cómo funcionan?



1 Introducción: ¿cómo funcionan?

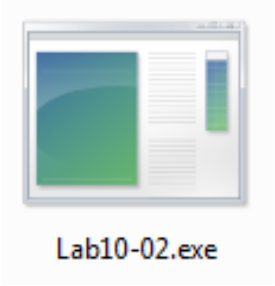


2

Análisis por comportamiento

2 Análisis por comportamiento

- El análisis por comportamiento consiste en examinar las acciones e inter-relaciones que realiza el código analizado con el sistema mientras se ejecuta. En esta fase no se analiza el código.



DEMO

- Demostración de una infección.
- Verificar que se escribe un fichero .sys que no aparece

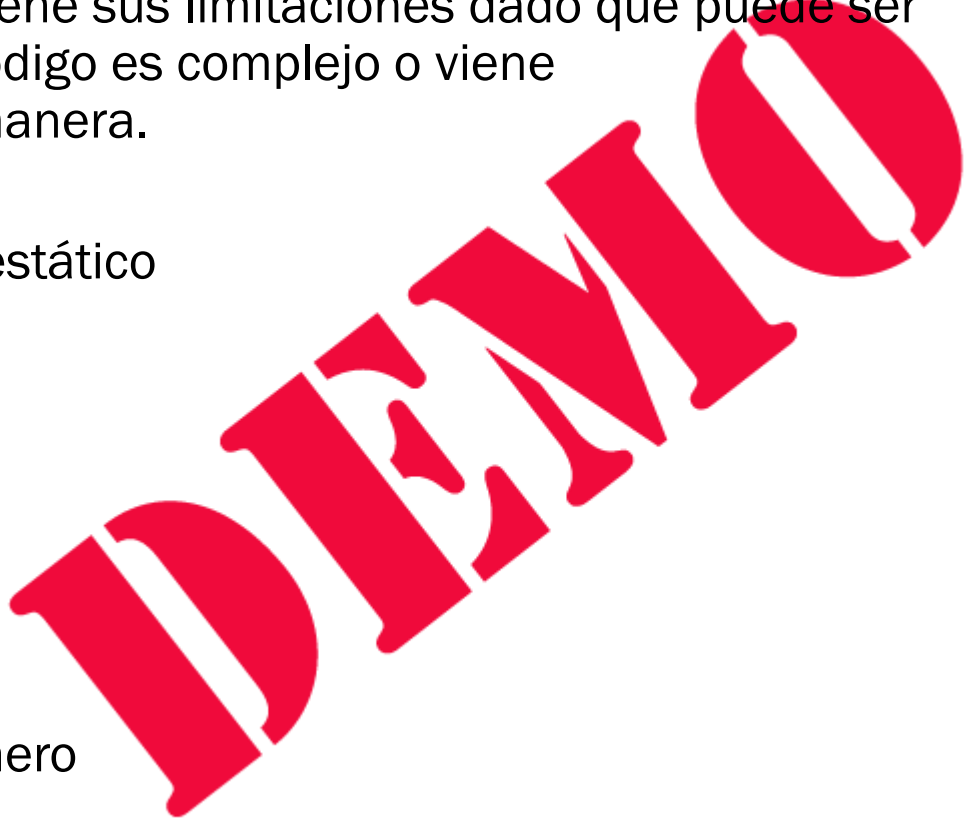
3

Análisis estático

3 Análisis estático

- El **análisis estático** consiste en examinar el código ejecutable sin ponerlo en ejecución lo que permite hacerse una idea de qué hace el mismo. Este tipo de análisis tiene sus limitaciones dado que puede ser complicado de realizar si el código es complejo o viene ofuscado/cifrado de alguna manera.

- Demostración de un análisis estático
- Análisis del instalador
- Recurso FILE
- Carga un driver
- Extraer el recurso
- Análisis del recurso
- Hookeo de la SSDT
- Demostración de crear un fichero



4

Análisis dinámico

4 Análisis dinámico

- El **análisis dinámico** se basa en el análisis del código en funcionamiento pudiendo verificar su comportamiento en su sistema real, con datos y escenarios completos. Este tipo de análisis sobre un ***rookit*** tiene una complejidad añadida: si se usa un ***debugger*** dentro del ***kernel***, al detener el código para su análisis, el sistema se detiene… incluido el ***debugger***.

- Laboratorio:
  - Windbg escuchando al puerto serie para analizar
  - Crear entrada en boot.ini debug por un puerto serie
  - Se conectan ambos por cable serie

DEMO

5

Conclusiones

5 Conclusiones

- No tener privilegios de administración
- Herramientas
  - GMER
  - IceSword
  - Sysinternals Rootkit Revealer
  - rkhunter
  - chkrootkit

- **E-Mails**
  - ccn-cert@cni.es
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - sondas@ccn-cert.cni.es
  - redsara@ccn-cert.cni.es
  - carmen@ccn-cert.cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es

Síguenos en Linked in