JNIC - Programa de Transferencia

Ficha de reto científico

Edición 2017

1 FICHA DE RETO

El mero hecho de proponer un reto a través del presente formulario implica la aceptación de las bases del Programa de Transferencia JNIC.

El formulario o Ficha Reto para documentar la propuesta de reto contiene los siguientes campos.

FICHA DE RETO JNIC

A. INFORMACIÓN SOBRE LA EDICIÓN DEL PROGRAMA EN LA QUE SE PRESENTA EL RETO

A.1 Edición Programa Transferencia JNIC: **2017**

B. INFORMACIÓN SOBRE EL RETADOR

B.1 Nombre de la Organización: INCIBE

B.2 Portal web: (de la organización o aquel en el que haya información sobre el reto propuesto)
Haga clic aquí para escribir texto.

B.3 Persona de contacto: Nombre, cargo, email, teléfono contacto.
Alejandro López, responsable de área

B.4 Información de soporte (buzón de email / teléfono u otros) para dar respuesta a las dudas que los investigadores puedan plantear sobre el reto:
apoyo.investigacion@incibe.es indicando "[Reto Malware]" en el título del correo

C. CARACTERÍSTICAS RELATIVAS AL RETO

C.1 Tipo de reto (abierto / restringido): Abierto

C.2 Se facilitará información confidencial que requiera un acuerdo previo formal (SI/NO):SI

C.3 Tipo de incentivo:

Nota: Es objetivo del Programa la publicación de los resultados obtenidos fruto de la investigación realizada para la solución del reto.

- ☐Sin incentivos
- ☐Premio en metálico mejor/es propuesta/s
- ☐Financiación de la investigación para generación de prototipo o una PoC
- ☒Reconocimiento para la mejor/es propuesta/s
- ☒Utilización de instalaciones/equipos del retador durante la investigación
- ☒Otros

Comentarios sobre los incentivos seleccionados:
Otros incentivos ofrecidos:
La propuesta de solución ganadora, recibirá una invitación para presentar y exponer su propuesta en la siguiente edición del evento ENISE (organizado por INCIBE), dentro del espacio dedicado a emprendimiento. Igualmente, si la solución obtiene una puntuación superior a 25 puntos (de los 60 posibles) y con no menos de 3 puntos en cada criterio de valoración, obtendrá una plaza como finalista en la próxima edición del certamen de emprendimiento incubadora Ciberemprende

(promovido por INCIBE). En dicho certamen se ofrecen servicios de formación y mentoring para ayudar, de forma práctica, en la constitución y lanzamiento de spin-offs en ciberseguridad.

C.4 (si procede) Cuantía económica para el premio a la mejor propuesta
Haga clic aquí para escribir texto.

C.5 (si procede) Cuantía económica para la financiación (1 año de trabajo investigador).
Haga clic aquí para escribir texto.

C.6 Se solicita revisión previa de cualquier publicación científica generada en la resolución del reto (SI/NO):
SI

C.7 Servicios que se ponen a disposición (utilización de hardware/software, posibilidad de estancias en las instalaciones del retador para conocer el reto, etc.):
Set de datos

C.8 Requisitos de confidencialidad (tanto para los investigadores, como para los miembros del Comité que evalúen la propuesta):
Firma de NDA

C.9 Condiciones de aceptación (limitaciones para la aceptación de solicitudes):
Haga clic aquí para escribir texto.

C.10 Condiciones de rechazo (cuestiones que quieran evitarse en las solicitudes):
Haga clic aquí para escribir texto.

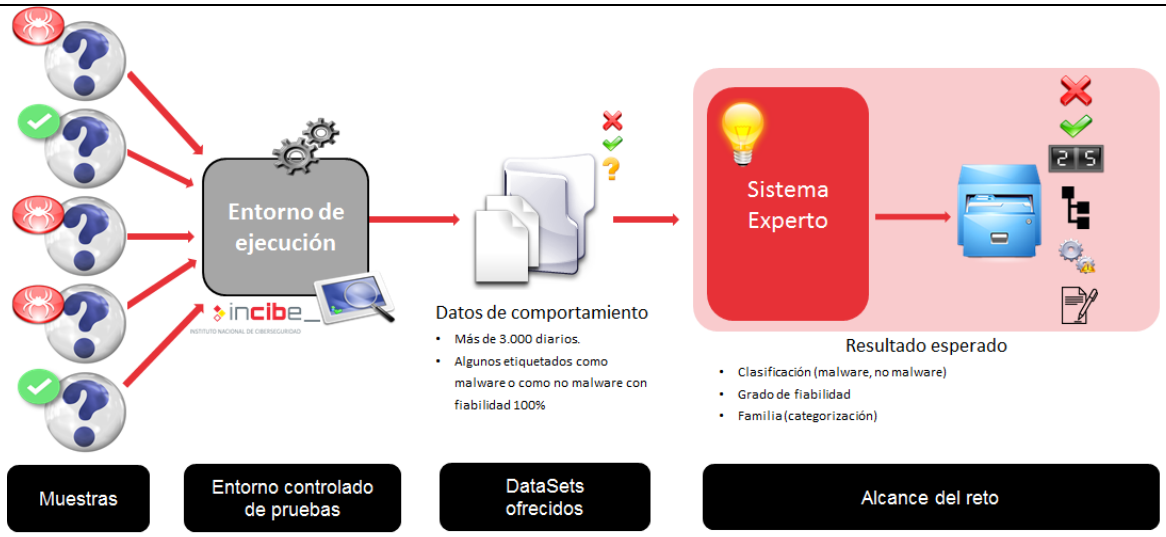
D. RETO PROPUESTO

D.1 Título del reto:
Detección de muestras maliciosas a partir del análisis dinámico

D.2 Antecedentes:
Diariamente se distribuyen multitud de muestras (ficheros, documentos, media, etc.) que representan una amenaza para el receptor puesto que se tratan de malware que intentan explotar alguna vulnerabilidad en los sistemas informáticos o engañar al usuario para que los ejecute e infectar el equipo con fines maliciosos o delictivos.

D.3 Motivación:
Detectar patrones de comportamiento que permitan determinar con alta probabilidad de acierto que una muestra que se distribuye a través de Internet (correo electrónico y otros servicios expuestos) es maliciosa

D.4 Descripción del reto:
Ser capaces de identificar automáticamente patrones de comportamiento malicioso e indicadores de compromiso a partir de las trazas ofrecidas por INCIBE, las cuales han sido obtenidas mediante la ejecución de muestras en un entorno de análisis dinámico controlado (sandbox). Dicho entorno está basado en el sistema de análisis de malware *Cuckoo* y los patrones de comportamiento e indicadores de compromiso se deben modelar en base a firmas de *Cuckoo* (*signatures*).
Junto a la identificación de las *signatures*, se solicita determinar el grado de su fiabilidad y categorizar el resultado en base a una jerarquía de familias/subfamilias a definir, así como especificar los motivos que han llevado a considerar cada detección o cada descarte.



D.5 Recursos de apoyo que se pondrán a disposición de los investigadores (data-sets, etc.):
Data-sets de resultados de análisis dinámicos

D.6 Avances realizados actualmente por el retador:
Actualmente INCIBE cuenta con un sistema de análisis de malware basado en *Cuckoo* que realiza los análisis a partir de un conjunto de *signatures* generadas manualmente. Sin embargo, se desea ampliar el mismo mediante la incorporación de nuevas *signatures* automáticas que aumenten su eficacia.
Para no parcializar los resultados ni la forma de trabajo, las *signatures* actuales no serán aportadas, esperando que sea el propio equipo de investigación quien cree sus propias asociaciones y conclusiones, de tal forma que sus resultados puedan llegar a ser complementarios, al utilizar otra metodología cuyas *signatures* puedan acoplarse a las existentes y así tener un sistema de detección más fiable, capaz de obtener unos mejores resultados.

D.7 Alcance:
Trazas de ejecuciones de muestras ejecutadas en el sistema de análisis de malware *Cuckoo* para los sistemas operativos Windows y Linux

D.8 Casos de uso:
CERT: detección y reacción ante incidentes

D.9 Soluciones actuales que dan cobertura parcial al reto:
Haga clic aquí para escribir texto.

D.10 Estudios/Investigaciones relacionados:
Haga clic aquí para escribir texto.

D.11 Documentación/Bibliografía de interés:
Haga clic aquí para escribir texto.

D.12 Otras consideraciones a tener en cuenta:
Haga clic aquí para escribir texto.

E. SEGUIMIENTO

E.1 Hitos esperados (puntos de seguimiento de la investigación):
Entregables cada 4 meses con los resultados de los avances

E.2 **TRL** objetivo para el primer año (Nivel de madurez que se espera que tengan las propuestas de solución recibidas): TRL3

F. EVOLUCIÓN DEL RETO

F.1 **TRL** objetivo para el final de la investigación (Nivel de madurez final que desea el retador para dar por finalizado el reto de forma exitosa):

TRL4

F.2 **Plazo** del reto (fecha límite para alcanzar el TRL final de investigación):

2 años

http://2017.jnic.es/