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)
N/A

B.3 Persona de contacto: Nombre, cargo, email, teléfono contacto.
Luis Fernández Prieto, Responsable de Desarrollo de Tecnologías de Ciberseguridad

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 BOTNETS]`" en el título del correo

C. CARACTERÍSTICAS RELATIVAS AL RETO

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

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
Por definir.

C.5 (si procede) Cuantía económica para la financiación (1 año de trabajo investigador).
Por definir.

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.):
Posibilidad de reuniones con el retador para definir objeto, alcance, requisitos, resolver dudas, etc.
Posibilidad de aportación de conjunto de datos de prueba por parte del retador.

C.8 Requisitos de confidencialidad (tanto para los investigadores, como para los miembros del Comité que evalúen la propuesta):
Tanto el objeto de la investigación, como la información intercambiada, como los posibles datos de prueba aportados deberán regirse por un contrato de confidencialidad.

C.9 Condiciones de aceptación (limitaciones para la aceptación de solicitudes):
El resultado de la investigación debe terminar en una prueba de concepto que verifique la viabilidad de integración práctica en un producto o servicio final.

C.10 Condiciones de rechazo (cuestiones que quieran evitarse en las solicitudes):
No disponer de una prueba de concepto que permita comprobar la viabilidad de la solución al problema.

D. RETO PROPUESTO

D.1 Título del reto:
Detección de bots y servidores de comando y control (C&C)

D.2 Antecedentes:
INCIBE está realizando un piloto actualmente de obtención de información de bots mediante la compra de dominios obtenidos de fuentes (públicas y privadas) de DGAs (Domain Generation Algorithms).

D.3 Motivación:
INCIBE, como centro especializado en la ciberseguridad, está interesado en la obtención de información propia relativa a amenazas (en este caso concreto botnets) para obtener conocimiento acerca de su funcionamiento y poder así establecer medidas de mitigación apropiadas.

D.4 Descripción del reto:
El reto consiste es la investigación y posterior desarrollo de una prueba de concepto para la detección de bots y servidores de comando y control (C&C).

En el apartado D.8 se proponen unos Casos de Uso de ejemplo, pero se da libertad a los equipos de investigación para proponer otras posibles aproximaciones para lograr el objetivo aquí planteado, teniendo en cuenta lo planteado en esta ficha.

D.5 Recursos de apoyo que se pondrán a disposición de los investigadores (data-sets, etc.):
Dominios de DGA disponibles en INCIBE.

D.6 Avances realizados actualmente por el retador:

Investigación sobre el problema. Recopilación de conjuntos de datos para entrenar sistemas.

D.7 Alcance:

Detección de bots y servidores de comando y control (C&C)

D.8 Casos de uso:

Caso de uso 01:

En base a la investigación inicial se selecciona una estrategia de detección de bots, se implementa en una PoC y se demuestra su viabilidad mediante la obtención de información de bots pertenecientes a una o varias botnets. La información que se desea obtener acerca del bot es al menos la siguiente: IP, timestamp del momento en que se realiza la detección. También sería deseable, si es posible, obtener información adicional sobre el comportamiento de cada Botnet en concreto, como por ejemplo el protocolo de comunicación utilizado entre bots y servidores C&C, puertos, etc.

Caso de uso 02:

En base a la investigación inicial se selecciona una estrategia de detección de paneles C&C, se implementa en una PoC y se demuestra su viabilidad mediante la obtención de información de bots pertenecientes a una o varias botnets. La información que se desea obtener acerca del C&C es al menos la siguiente: IP, timestamp del momento en que se realiza la detección. También sería deseable, si es posible, obtener información adicional como por ejemplo el protocolo de comunicación utilizado entre bots y servidores C&C, puertos, URL completa donde se encuentra el panel, tecnología subyacente del panel, información acerca del servidor en el que está alojado, etc.

D.9 Soluciones actuales que dan cobertura parcial al reto:

El análisis de soluciones y estrategias de detección formará parte del trabajo de investigación.

D.10 Estudios/Investigaciones relacionados:

El análisis de estudios/investigaciones formará parte del trabajo de investigación.

D.11 Documentación/Bibliografía de interés:

El análisis de documentación/bibliografía formará parte del trabajo de investigación.

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):

Hito 1: Periodo de investigación

Como resultado del periodo de investigación se entregará un informe que contendrá, como mínimo:

- Introducción y motivación del problema.
- Revisión del estado del arte de la investigación en este campo.
- Descripción de las soluciones o estrategias seleccionadas que se utilizarán en la PoC.
- Análisis de las ventajas y limitaciones de las soluciones o estrategias seleccionadas.

Hito 2: Acuerdo de los requisitos

Como resultado del periodo de investigación se entregará un informe que contendrá, como mínimo:

- Alcance de la PoC que se entregará.
- Especificación de los requisitos.
- Justificación de las tecnologías y lenguaje de programación utilizados.
- Interfaz de comunicación y ejecución de la PoC.
- Forma de entrega de la PoC (docker, máquina virtual).

Hito 3: PoC (Prueba de Concepto)

Como resultado del periodo de investigación se entregará un informe que contendrá, como mínimo:

- Entrega de la PoC previamente definida.
- Descripción de la PoC entregada y su documentación.
- Resultados de evaluación de dicha PoC, donde se especificará el conjunto de datos utilizados en las pruebas y los resultados obtenidos.
- Informe con recomendaciones acerca de la evolución de la PoC como posible herramienta o servicio y recomendaciones de futuras investigaciones relacionadas.

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):

TRL3

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

1 año (desde el inicio del trabajo de investigación)

http://2017.jnic.es/