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: ElevenPaths. Telefónica Cyber Security Unit.

B.2 Portal web: (de la organización o aquel en el que haya información sobre el reto propuesto)
www.elevenpaths.com

B.3 Persona de contacto: Nombre, cargo, email, teléfono contacto.
Marcos Arjona, Consultor de Investigación e Innovación, marcos.arjona@11paths.com, 666985706.

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:
marcos.arjona@11paths.com

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:
ElevenPaths realizará un esfuerzo de difusión en sus medios de comunicación, así como en eventos y jornadas de índole científica donde se podrán presentar conjuntamente con el equipo de investigación, los avances actuales y el progreso de la solución al reto. Además, ElevenPaths apoyará en todo momento la hoja de ruta, facilitando el uso de las instalaciones, sistemas y datos necesarios para cumplir con los objetivos de la solución.

El vínculo entre la entidad investigadora junto a ElevenPaths podrá generar un proceso colaborativo propicio para ambas instituciones, mejorando el clima de cooperación y facilitando investigaciones y desarrollos relacionados con el reto en curso.
Los equipos investigadores que trasladen el conocimiento y producción de los retos a iniciativas empresariales propias o spin-offs podrán optar de manera privilegiada al programa de emprendimiento y aceleración de Wayra, una iniciativa de Telefónica a través de Open Future que se facilitará a las empresas siempre que cumplan con las características de admisión necesarias.
Pese a no tener un fondo de financiación definido, ElevenPaths realizará un seguimiento proactivo de la solución al reto, agilizando e incentivando su desarrollo, fomentando nuevas colaboraciones en el ámbito de la solución. Finalmente, según el progreso del reto podrían establecerse contratos privados de investigación sobre el reto para la creación del PoC o su continuidad.

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.):
- Acceso a las plataformas pertinentes.
- Asistencia y tutorial de uso de las plataformas.

C.8 Requisitos de confidencialidad (tanto para los investigadores, como para los miembros del Comité que evalúen la propuesta):
Acuerdo de Confidencialidad sobre la documentación y software utilizado por los investigadores durante la ejecución del reto.

C.9 Condiciones de aceptación (limitaciones para la aceptación de solicitudes):
- Posesión de experiencia en el ámbito del reto bien sea a través de publicaciones en conferencias o revistas.
- Se valorará positivamente desarrollos previos y PoC realizados por el mismo equipo científico en áreas científicas similares o cuyo conocimiento pueda proporcionar valor añadido a la solución.

C.10 Condiciones de rechazo (cuestiones que quieran evitarse en las solicitudes):
- Equipo de investigación no consolidado o sin trayectoria científica demostrable.
- La propuesta del equipo de investigación no aborda una solución al reto que incluya Tacyt como plataforma de uso.

D. RETO PROPUESTO

D.1 Título del reto:
Análisis y correlación en Android de PUPs & Adware

D.2 Antecedentes:
Actualmente el software potencialmente malicioso (Potential Unwanted Program/Application – PUP/PUA) y el Adware están presentes en gran parte de las aplicaciones disponibles en los repositorios comerciales. Su inclusión se ha generalizado a todo tipo de software como juegos, antivirus, optimizadores y todo tipo de herramientas. Tal es su expansión que este tipo de software y sus acciones se han convertido en las

actividades más incómodas e intrusivas de cara a los usuarios. Donde adicionalmente las aplicaciones de esta índole pueden contener componentes maliciosos y malware embebido o facilitar la instalación de éstos de forma inadvertida.

En este sentido, los desarrolladores de PUPs y Adware utilizan técnicas cada vez más agresivas y avanzadas gracias a la permisividad que se les confiere, ya que su software no se clasifica como malware y están amparadas en un marco legal válido y protegido. Por tanto, ya que es inviable penalizar dicho software por vía legal, la importancia de detectar este tipo de software para evitar su uso es cada vez más elevada y cualquier técnica, metodología o indicio que permita identificar este tipo de aplicaciones y sus actividades proporciona un indudable valor de cara a la seguridad y a la experiencia de usuario, proporcionándoles garantías respecto al software de descargan y se instalan.

D.3 Motivación:

ElevenPaths posee una serie de herramientas de ciberinteligencia de diversa índole para dar soporte a los analistas y consultores de seguridad. Una de estas herramientas es Tacyt, que fue desarrollada para realizar un análisis profundo de las aplicaciones existentes en markets para Smart Phones y dispositivos móviles. Repositorios software especialmente interesantes al ser el principal origen de software para la mayoría de usuarios.

Ante esta perspectiva, el análisis de los perfiles de las aplicaciones permite obtener información y detalles de los que se pueden realizar determinados estudios y correlaciones de diversa índole. La principal virtud es que dichos procesos de análisis se pueden realizar sobre un conjunto muy amplio de aplicaciones simultáneamente, teniendo en cuenta además el ritmo tan elevado de crecimiento de estos almacenes de software.

Por tanto, gracias a los distintos mecanismos de búsqueda disponibles en Tacyt sobre dicha información y sobre conjuntos amplios de aplicaciones, se pueden efectuar numerosas consultas que combinen diversos criterios y filtros. Permitiendo a los usuarios realizar investigaciones y estudios de clasificación, clustering, atribución y análisis detallado de aspectos funcionales, permitiendo deducir y correlar hechos basados en hipótesis de investigación de alta complejidad.

D.4 Descripción del reto:

Este reto tiene un marcado carácter científico para el equipo implicado ya que inicialmente centra el foco en la generación de una serie de publicaciones, informes y deducciones que permitan elevar el grado de conocimiento respecto a PUPs y Adware existente en markets de aplicaciones móviles. El equipo de investigación dispondrá de libertad a la hora de decidir cuál será su enfoque y procedimiento para realizar el procesado de datos obtenidos en Tacyt. Pero idealmente sus deducciones deberían ser capaces de alimentar la plataforma de cara a mejorar sus capacidades de detección e incrementar la experiencia y conocimiento sobre este tipo de Spyware.

Estos estudios permitirán no solo incrementar el estado de consciencia relativo a este tipo de software, sino que permitirá mejorar las capacidades de detección conforme a reglas de alto nivel y consultas de gran precisión. Un conjunto de avances y progresos que permitan sentar un trabajo futuro de colaboración entre ElevenPaths y el equipo de investigación, no solo para seguir mejorando las capacidades de Tacyt al respecto sino para introducir mejoras técnicas destinadas a la detección y clasificación proporcionadas por el grupo de investigación. Extensiones que serían gestadas en futuros acuerdos y contrataciones con la Universidad.

Entre los muchos objetivos que el equipo de investigación puede proponer, ElevenPaths puede priorizar cuales son los más interesantes desde el punto de vista estratégico, pero sin duda los más interesantes podrían ser:

- Detección de firmas conocidas de PUPs y Adware
- Correlación entre PUPs firmados y no firmados
- Pay per install en markets
- Spyware en Portátiles y ordenadores vs Smart Phones
- Análisis de las técnicas y mecanismos de propagación

- Análisis preventivo de Spyware
- Influencia de las tendencias en la aparición de Spyware.
- Mecanismos inteligentes de identificación de PUPs y Adware
- Otros

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

Según la solución, alcance y tipo de enfoque se proporcionará al equipo de investigación acceso a la información, conjuntos de datos y APIs necesarias para la resolución del reto. Esta cesión documental puede estar sujeta a un acuerdo de confidencialidad debido a su naturaleza privada y corporativa.

En concreto y como se desprende de la descripción, el equipo investigador tendrá que hacer uso de la plataforma Tacyt de ElevenPaths para realizar el estudio y prospección de los markets de aplicaciones. Por tanto se habilitaran credenciales de acceso y uso adecuadas para la realización del reto.

D.6 Avances realizados actualmente por el retador:

ElevenPaths ha realizado numerosos estudios bajo demanda privada y generado determinados estudios que los clientes solicitaban de acuerdo a sus necesidades. Pese a eso, la prospección y detección de PUPs y Adware no tiene aún un enfoque claro y determinista que permita satisfacer la necesidad actual de prevención y contención de dicho tipo de software y sus actividades relacionadas. Sobre todo en lo que respecta a la constante evolución y actualización de dicho software.

Si bien el estado del arte de las iniciativas existentes para detectar y analizar este software tiene numerosas publicaciones y equipos científicos abordándolo, ElevenPaths requiere el uso de sus herramientas específicas para mejorar su servicio privado. De todos los posibles avances que hemos tratado de integrar, pocos eran aptos para nuestra plataforma Tacyt y es por ello que las mejoras deben integrarse gracias a los avances de un equipo científico adecuado, que permita definir las necesidades idóneas, concluyentes y conforme a las deducciones y datos correlados obtenidos.

D.7 Alcance:

Las expectativas de este reto, de acuerdo al entorno de usabilidad limita por defecto el alcance del mismo, con unas expectativas de un TRL 3 que permita la generación de estudios e investigaciones basada en los distintos objetivos acordados. Teniendo en cuenta que las conclusiones tienen que ser constatables y que demuestren un enfoque innovador respecto a las capacidades de detección de PUPs y Adware en markets de aplicaciones móviles.

El alcance de este reto viene marcado por su carácter meramente científico y se consensuará directamente con el equipo de investigación, pero entre los logros esperados para cuantificar el alcance se podrían mencionar:

- Publicaciones relacionadas con la detección de PUPs y Adware utilizando Tacyt
- Informe de evaluación y prospección de Spyware en los markets, históricos y evolución del mismo a lo largo del tiempo
- Estudio de alguna familia de PUPs o Adware y su modelo de financiación y retroalimentación.
- Generación de un conjunto de reglas de detección que permitan algún tipo de clustering o clasificación innovadora.
- Detección y anticipación de nuevos PUPs y Adware en fase de propagación en algún market de aplicaciones.

D.8 Casos de uso:

El siguiente caso de uso aborda la funcionalidad de Tacyt, lo que permite percibir el sentido de dicho software como elemento principal de detección de PUPs y Adware en markets de aplicaciones.

CU1:

Precondición: Existen numerosas aplicaciones PUPs y Adware que ocultan su funcionamiento y modus operandi tras la imagen y marca de otra compañía de la que toman su identidad. Mientras esta suplantación no sea detectada, dichas aplicaciones podrían propagarse a los usuarios que confían en la compañía suplantada. Esto provoca dos circunstancias bien diferenciadas, por un lado, la ventaja estratégica que las aplicaciones obtienen al falsear su imagen, haciendo creer a los usuarios que son la empresa legítima. Y por otro lado, el impacto negativo provocado sobre la empresa suplantada que perjudicará la opinión del usuario debido a las escasas consideraciones de seguridad del gestor del market y de la compañía que se ha dejado suplantar.
Descripción: Es necesario introducir reglas y mecanismos que permitan de forma anticipada detectar aplicaciones que traten de suplantar a otras, bien sea porque las empresas privadas desarrollan comprobaciones y disparadores que se ejecutan bajo ciertos criterios y parámetros, o que existan ciertas comprobaciones recurrentes en los markets que mediante un análisis exhaustivo y profundo puedan percibir este tipo de acciones de manera anticipada.
Secuencia:

1) Alice es un usuario conocido por poblar markets de aplicaciones con software plagado de Adware y con atisbos de malware.
2) MercadoA es un market de Android que utiliza Tacyt para comprobar el tipo de software que se sube a la plataforma
3) Alice sube su aplicación en MercadoA, especificando una imagen y características similares a un conocido antivirus llamado RAV, iconografía, branding e incluso el nombre presta a confusión al usuario: RAV Ransomware detector.
4) MercadoA recibe la subida del fichero y comprueba utilizando Tacyt cuáles serían los datos esperados de los ficheros subidos por la compañía RAV
5) Los datos que ofrece Tacyt demuestran que ni la firma, ni los desarrolladores encajan con los incluídos por RAV Ransomware. Datos que proceden de varios markets simultáneamente. Además el nombre del desarrollador da indicios de ser Alice, un conocido usuario con ilícitas intenciones.
6) MercadoA bloquea el uso de RAV Ransomware y marca al usuario y sus datos como aportes no deseados en la plataforma

Postcondición: Gracias a las reglas de exploración de Tacyt se ha podido prevenir la inclusión de una aplicación con Spyware en el market. Permitiendo la detección temprana de dichas aplicaciones, capturando a la vez un contenido que será fundamental para futuras comprobaciones de aplicaciones, donde cualquier coincidencia con las detectadas en RAV Ransomware permitirá agilizar la detección y categorización de software similar.

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

Por las características del reto las soluciones actuales similares no son competidores directos que afecten al enfoque de la propuesta.

D.10 Estudios/Investigaciones relacionados:

M. Lindorfer et al. “AndRadar: fast discovery of android applications in alternative markets” in Proceedings of the 11th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2014.(PDF)
J. Hallett and D. Aspinall. 2016. AppPAL for Android. In Proceedings of the 8th International Symposium on Engineering Secure Software and Systems - Volume 9639 (ESSoS 2016). Springer-Verlag. New York, NY, USA, 216-232. (PDF)
V. Svajcer and S. McDonald, ”Classifying PUAs in the Mobile Environment”. (Oct 2013) (PDF)

D.11 Documentación/Bibliografía de interés:

M. Lindorfer, M. Neugschwandtner and C. Platzer, "MARVIN: Efficient and Comprehensive Mobile App Classification through Static and Dynamic Analysis," 2015 IEEE 39th Annual Computer Software and Applications Conference, Taichung, 2015, pp. 422-433.

Arp, Daniel et al. "DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket." *NDSS* (2014).(PDF)

W. Wu and S. Hung. 2014. DroidDolphin: a dynamic Android malware detection framework using big data and machine learning. In Proceedings of the 2014 Conference on Research in Adaptive and Convergent Systems (RACS '14). ACM, New York, NY, USA, 247-252.

Y. Kikuchi et al. "Evaluating Malware Mitigation by Android Market Operators". 9th Workshop on Cyber Security Experimentation and Test (CSET'16), 2016. Austin, TX (PDF)

D.12 Otras consideraciones a tener en cuenta:

Los equipos de investigación que aborden estas soluciones no deben limitar su enfoque científico ni acotar su ambición tecnológica a los términos expresados en este reto si esto supone un perjuicio de cara a la ambición o a las expectativas alcanzables por los investigadores. Se valorará positivamente la incorporación de factores de valor diferenciales que permitan trazar una hoja de ruta mucho más ambiciosa e innovadora.

E. SEGUIMIENTO

E.1 Hitos esperados (puntos de seguimiento de la investigación):

La lista de milestones serán factores que se acordarán adecuadamente con los equipos de investigación implicados, de esta manera se podrán adaptar las expectativas a criterios reales tales como la experiencia de los investigadores y el tipo de solución propuesta. Sin embargo, varios hitos serían deseables para el control de la investigación:

1) Aprendizaje del motor de reglas de Tacyt
2) Realización de una publicación del avance y enfoque científico.
3) TRL 3 de la investigación con un valor de peso en innovación.

E.2 **TRL** objetivo para el primer año (Nivel de madurez que se espera que tengan las propuestas de solución recibidas): TRL1

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):

12 meses

http://2017.jnic.es/