Reto 2

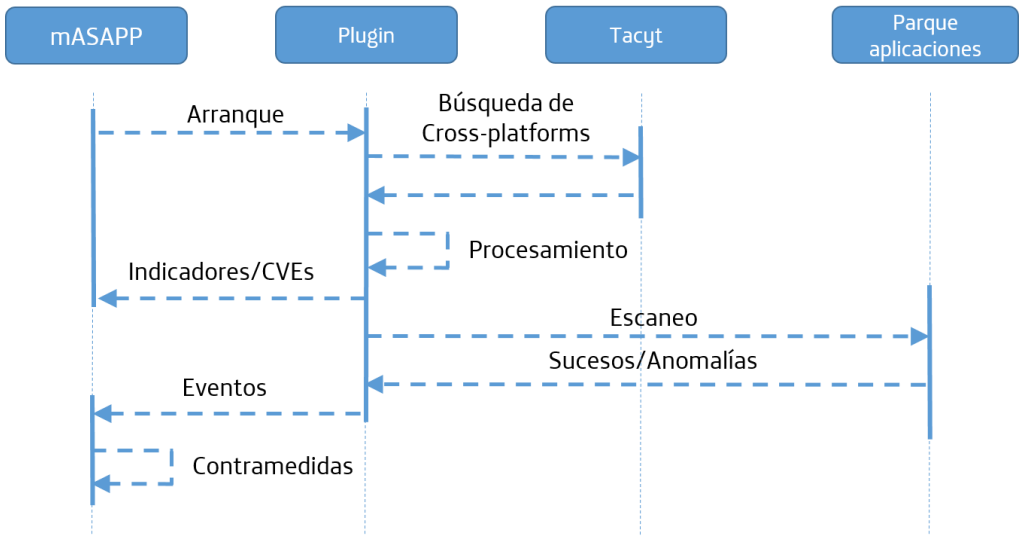
Programa de Tutorización Universitaria para la Transferencia Orientada mediante Retos de Innovación Avanzada (TUTORÍA) para la Red de Cátedras Telefónica: 1ª edición 2018

Reto 2. Análisis de aplicaciones móviles para la prevención avanzada de seguridad.	
INFORMACIÓN DEL TUTOR	
Departamento	Área de Innovación y Laboratorio de ElevenPaths. https://www.elevenpaths.com/ Telefónica Digital España
Responsable	Marcos Arjona Fernández. marcos.arjona@11paths.com Director de proyectos de investigación e innovación
INFORMACIÓN GENERAL	
Carácter	Investigación científico-técnica con desarrollo experimental
Tipo	Módulo auxiliar, el resultado podría llegar a ser integrado en un producto.
Recursos de apoyo	☒ Repositorios de software, APIs y conectores necesarios, librerías, etc. ☐ Orientación técnica relativa a la productivización e industrialización para mercado, consejos y metodologías de desarrollo, orientación técnica, sugerencias de configuraciones, etc. ☒ Licencias de productos y plataformas ElevenPaths, ☒ Servicios de asistencia y soporte especialista a la investigación y el desarrollo.
DETALLES DE LA PROPUESTA	
Contexto y Motivación	Actualmente las plataformas móviles están pobladas de numerosos tipos de amenazas y riesgos de seguridad para los usuarios que en muchos casos son permitidas por los propietarios y gestores de los markets de aplicaciones y repositorios comerciales. Uno de los grandes problemas surge cuando se da cobijo de forma abierta a software potencialmente malicioso (Potential Unwanted Program/Application – PUP/PUA), Adware o bien software anómalo que propicia riesgos y amenazas de seguridad en los dispositivos. La permisividad hacia estas aplicaciones es tan amplia, que a día de hoy supone el principal factor generador de amenazas de seguridad, debido a su propagación y alcance ante la confianza de los usuarios en las plataformas de apps, resultando una de las actividades más incómodas e intrusivas de cara a cualquier consumidor de dichos markets. Donde adicionalmente las aplicaciones de esta índole pueden abrir la puerta a novedosos componentes maliciosos y malware embebido mucho más perjudicial, normalmente facilitando 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 colector de indicios que permita identificar este tipo de aplicaciones y sus actividades proporciona un indudable valor de cara a la seguridad y a evitar perjuicios a los usuarios, proporcionándoles garantías respecto al software de descargan y se instalan.
Descripción	ElevenPaths posee una serie de herramientas de ciberinteligencia de diversa índole para dar soporte a los analistas y consultores de seguridad. Dos de estas herramientas son Tacyt y mASAPP, desarrolladas para realizar un análisis profundo de las aplicaciones existentes en markets para SmartPhones y dispositivos móviles. Ambas herramientas comparten un mismo núcleo operativo, aunque sus objetivos son distintos. Tacyt es capaz de analizar los perfiles de las aplicaciones para obtener información y detalles de los que se pueden realizar determinados estudios y correlaciones de diversa índole sobre un conjunto muy amplio de aplicaciones simultáneamente. Por otro lado, mASAPP se ha concebido para facilitar la tarea corporativa de protección y prevención de amenazas de seguridad en el ecosistema de aplicaciones que posee o desarrolla una empresa, aunque su fundamento arranca del análisis de la misma información que Tacyt. Pero realizando un ciclo continuo de evaluaciones y comprobaciones específicamente creado y diseñado para un subconjunto de aplicaciones concretas. Esto incluye búsquedas específicas o personalizadas para el contenido o la índole del parque de aplicaciones a evaluar. Gracias a los distintos mecanismos de búsqueda disponibles en Tacyt 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, atribución y análisis detallado de aspectos funcionales, permitiendo deducir y correlar hechos basados en hipótesis de investigación de alta complejidad. Y gracias a mASAPP se podrían generar mecanismos preventivos e incluso paliativos para las amenazas detectadas, que podrían ser desde meras notificaciones, bloqueos anticipados, o acciones remediativas en aquellos casos donde sea posible y cobre sentido. Este reto trata por tanto de propiciar un estudio sobre un conjunto de aplicaciones móviles que permita aportar fundamentos y justificación de algún descubrimiento relativo a ciberseguridad. Con este estudio y una vez demostrado que dichos elementos podrían ser acotados para generar mecanismos de detección de riesgos y vulnerabilidades de seguridad, se podría proceder con el desarrollo por parte de los equipos investigadores de paliativos para algunas de dichas anomalías encontradas. Y en este caso se utilizaría mASAPP. Los equipos científicos pueden optar a resolver este reto desde un prisma meramente científico o bien científico con desarrollo tecnológico. Estas dos aproximaciones quedarían de la siguiente forma: Carácter científico El equipo podrá establecer un enfoque puramente científico basado únicamente en la fuente de información que Tacyt es capaz de proveer a los investigadores. Este enfoque destinado a producción científica en forma de publicaciones, informes, deducciones y estudios deben permitir elevar el grado de conocimiento al respecto de PUPs, Adware, Malware y vulnerabilidades encontradas en los markets de aplicaciones móviles.

	El equipo investigador 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 riesgos encontrados. Carácter científico-técnico El equipo a partir del esfuerzo científico previo y siempre que haya justificado, gracias a Tacyt, la detección de indicios suficientes para generar mecanismos avanzados de detección de riesgos, vulnerabilidades y amenazas. Este tipo de capacidades solamente podrían ser logradas si se puede llegar a concluir de forma precisa el grado de maliciosidad que posee dicho software, lo que a su vez permitiría obtener valoraciones de ciberseguridad útiles, evolutivas y escalables. Así como permitir anticipar la identificación de los mismos indicativos en otros markets, usable incluso por otros usuarios/clientes. Para cumplir con este paso de un plano meramente científico a uno práctico adquiere sentido la herramienta mASAPP que dispone de una plataforma propia de generación de plugins, las cuales mediante una API y una arquitectura definida permiten incorporar plugins específicamente creados para abordar riesgos, vulnerabilidades y 0-days detectados. De esta manera la capacidad de propagación de paliativos de seguridad se ve reforzada gracias a esta funcionalidad, la cual puede llegar a clientes, empresas y usuarios de forma prácticamente inmediata. Esto permite reducir los esfuerzos de la comunidad a la hora de resistir ataques o evitar la propagación de algún tipo de software malicioso a través de los markets de aplicaciones móviles.
Factores de investigación e innovación	Carácter Científico - Capacidad de realizar una investigación centrada en aspectos anómalos de aplicaciones móviles en los markets de aplicaciones atendiendo a la información que provee Tacyt junto a las que el equipo investigador considere oportuna, útil y compatible con la plataforma. - Capacidad deductiva para localizar indicadores de elementos maliciosos a través de diversa naturaleza y surgidos de la investigación previa Carácter Científico-Técnico - Creación de plugins utilizando para ello mASAPP adecuando la tipología de los mecanismos de detección y paliativos a los objetivos de dicha plataforma. - Desarrollo e implementación de los mecanismos avanzados para la detección junto a la arquitectura necesaria para ser integrado en mASAPP. - (Extra) Estudio de las capacidades proporcionadas por el plugin en un despliegue controlado, efectuado en determinados clientes para evaluar las capacidades que los plugins podrían proporcionar en un entorno real.
Hitos	Carácter Científico (Ejemplos) 1. Estudio constatable y justificado al respecto de alguna familia de software potencialmente malicioso, Adware, Malware, Spyware, etc. 2. Producción científica y publicaciones relacionadas con la detección amenazas y riesgos de seguridad a través de Tacyt. 3. Informes de evaluación y prospección de Spyware en los markets, históricos y evolución del mismo a lo largo del tiempo 4. Detección y anticipación de nuevos PUPs y Adware en fase de propagación en algún market de aplicaciones.

	Carácter Científico-Técnico (Ejemplos) 0. (Los hitos del carácter científico) 1. Producción científica con mecanismos avanzados de detección de amenazas o vulnerabilidades de seguridad en aplicaciones móviles 2. Producción científica con mecanismos avanzados para detectar e identificar aplicaciones maliciosas, detección de amenazas o vulnerabilidades de seguridad en aplicaciones móviles, Adware o malware de diversa naturaleza. 3. Creación de plugins específicos para detectar y remediar vulnerabilidades de seguridad detectadas en aplicaciones móviles. 4. Creación de plugins con carácter genérico y adaptativo que permitan proporcionar paliativos a nuevas vulnerabilidades/0-days encontrados
Caso de Uso Científico	Una de las medidas de seguridad generalizadas en los markets de aplicaciones Android, es la ofuscación de código. Y generalmente tras esa operación, las capacidades funcionales, las operaciones y el flujo de datos no se alteran, sino que simplemente el código resulta menos comprensible de cara al exterior. Sin ignorar las ventajas relativas a la seguridad, existe la incertidumbre de qué ocurre con los ofuscadores de terceros, incluyendo los que pertenecen a los propios markets de aplicaciones, cuando realizan la ofuscación de las aplicaciones de los usuarios. Lo que a priori debe producir una copia funcional exacta de las APKs, en el fondo podrían introducirse una serie de elementos difícilmente detectables por los analizadores. Por tanto, existe cierto margen para evaluar si en la práctica ocurre esta circunstancia y por qué. Y, además, resulta sumamente interesante descubrir qué modificaciones se introducen y con qué propósito, incluso si éstas alteraciones responden a elementos puramente de seguridad que permiten validar y garantizar la integridad del documento ofuscado. Este estudio se realizaría únicamente con la información que provee Tacyt y permitiría agregar un tipo de funcionalidad en esta plataforma para poder administrar información relativa al tipo de ofuscación, el software utilizado y el riesgo existente en caso de que sea detectado mediante algún proceso de análisis de software malicioso.
Caso de Uso Técnico	Los desarrolladores de aplicaciones Android utilizan diferentes frameworks de desarrollo e IDEs según sus necesidades. Pero muchos de ellos aprovechan las ventajas de los entornos crossplatform a la hora de implementar la funcionalidad esperada y que ésta sea replicada en diferentes sistemas operativos. De esta forma se abstraen de desarrollos en modo nativo, de los que solamente deben sacrificar algunas funcionalidades y detalles específicos que no ofrecen este tipo de software multipropósito. Pudiendo obtener de forma cómoda y económica versiones de las aplicaciones en desarrollo para Android, IOs y Windows. Ante esta circunstancia subyace un interés muy específico ya que tales sistemas incorporan a los compilados diferentes librerías de terceros, dependencias no necesarias y una serie de elementos añadidos que a priori no forman parte de la implementación del desarrollador ni poseen responsabilidad funcional, y que en determinadas circunstancias abre la puerta a factores desconocidos y no controlados del software final. Además, este proceso puede sufrir reempaquetados y reconfiguraciones durante el compilado susceptible de incorporar sutilmente nuevos elementos adicionales de naturaleza incierta. Por tanto, mediante Tacyt y mASAPP se podría realizar el estudio del árbol de dependencias y elementos auxiliares que forman parte de las APKs. Obteniendo un compendio de aquellos elementos anómalos o sospechosos y activar contramedidas en caso de que alguno de los indicadores al respecto detecten estos indicios en el parque de aplicaciones de la empresa que utiliza mASAPP.

	
Alcance e Impacto	Los dos casos de uso presentados en este reto como ejemplos, permitirían no solo incrementar el estado de consciencia relativo a este tipo de riesgos y vulnerabilidades, sino que ayudarían a mejorar las capacidades de detección conforme a reglas y consultas de alto nivel. La omnipresencia de dispositivos móviles como smartphones y tablets junto a la inmensa cantidad de aplicaciones que se desarrollan a diario, cuyo ritmo de creación y actualización es tan elevado que resultan imposibles de controlar y verificar para comprobar las garantías de seguridad que proporcionan, y por tanto esta necesidad convierte en prioritarios todos los esfuerzos en este sentido destinados a mejorar la ciberseguridad. El conjunto de avances y progresos que se derivan de este reto permitirán sentar un trabajo futuro de colaboración entre ElevenPaths y el equipo de investigación, no solo para seguir mejorando las capacidades de Tacyt y mASAPP al respecto, sino para descubrir y optimizar procesos avanzados para la detección y clasificación de aplicaciones maliciosas.
Enlaces de Interés	- Evaluating Malware Mitigation by Android Market Operators. https://www.usenix.org/system/files/conference/cset16/cset16-paper-kikuchi.pdf - Large-scale Third-party Library Detection in Android Markets. https://faculty.ist.psu.edu/wu/papers/LibD-TSE-18.pdf - DroidCat: Effective Android Malware Detection and Categorization via App-Level Profiling. https://pdfs.semanticscholar.org/1890/cc8f7894677eef6c3ad32380e88ee684ead2.pdf - MalDozer: Automatic framework for android malware detection using deep learning. www.dfrws.org/sites/default/files/session-files/paper.pdf - AndRadar: Fast Discovery of Android Applications in Alternative Markets. https://www.cs.ucy.ac.cy/~eliasathan/papers/dimva14.pdf - Tacyt. https://www.elevenpaths.com/es/tecnologia/tacyt/index.html - mASAPP. https://www.elevenpaths.com/es/tecnologia/masapp/index.html
TRL Científico	TRL 2: Concepto y/o aplicación tecnológica formulada.
TRL Técnico	TRL 5: Validación de componente y/o disposición de los mismos en un entorno relevante.