PROYECTO DE INVESTIGACIÓN INTERNO PII-17-14

"Detección de Ransomware a gran escala por medio de seguridad cognitiva"

En la ciudad de Quito D.M., a los tres días del mes de febrero del año dos mil veinte, comparecen a la celebración de la presente Acta de Finalización del Proyecto de Investigación Interno ***PII-17-14 "Detección de Ransomware a gran escala por medio de seguridad cognitiva"***, por una parte la ***Ph.D. Alexandra Patricia Alvarado Cevallos*** en calidad de ***Vicerrectora de Investigación, Innovación y Vinculación*** de la Escuela Politécnica Nacional, y por otra la ***Ph.D. Myriam Beatriz Hernández Álvarez*** en calidad de ***Directora del Proyecto de Investigación Interno PII-17-14***, al tenor de lo siguiente:

1. ANTECEDENTES:

a) El 4 de julio de 2017, el Consejo de Investigación y Proyección Social mediante Resolución 079/17, aprueba el Cronograma para el lanzamiento de la Convocatoria para la presentación de Proyectos de Investigación Internos, Semilla, Junior y Multi e Interdisciplinarios 2017, y mediante Resolución 092/17 del 1 de agosto del 2017 se aprueba una reforma al Cronograma de la Convocatoria de Proyectos de Investigación del 2017; con lo cual se aplaza la fecha de cierre de la convocatoria.

b) El 8 de enero de 2018, al amparo de lo dispuesto por Consejo de Investigación y Proyección Social, mediante Resolución R167/17, se aprobaron los proyectos internos 2017, entre ellos el denominado: *"Detección de Ransomware a gran escala por medio de seguridad cognitiva"*, presentado por la Ph.D. Myriam Hernández.

c) Mediante Memorando EPN-VIPS-2018-0555-M del 13 de marzo de 2018, se informa a los Directores de los proyectos Internos 2017 que la fecha de inicio de los proyectos es el 9 de abril del 2018.

2. DATOS GENERALES DEL PROYECTO:

Código de Proyecto	*PII-17-14*
Nombre del Proyecto	*Detección de Ransomware a gran escala por medio de seguridad cognitiva*
Directora del Proyecto	*Myriam Beatriz Hernández Álvarez*
Colaboradores del Proyecto	*Sang Guun Yoo* *Lorena Isabel Barona López* *Ángel Leonardo Valdivieso Caragual*
Departamento	*Informática y Ciencias de la Computación (DICC)*
Líneas de Investigación	*Seguridad y Privacidad* *Machine learning*
Objetivo	*Diseñar un modelo de detección y prevención de Ransomware, mediante la identificación de patrones y comportamientos sospechosos a través de herramientas que interpretan, aprenden y procesan la inteligencia de seguridad*
Duración del Proyecto	• *Inicio: 9 de abril del 2018* • *Fin planificado: 8 de abril del 2019* • *Prórroga Ordinaria: 6 meses, hasta el 8 de octubre de 2019* • *Duración total: 18 meses*
Entrega del Informe Final	*23 de enero del 2019*
Presupuesto asignado	*$ 4.998,53 USD (cuatro mil novecientos noventaiocho dólares americanos, con 53/100)*
Presupuesto ejecutado	*$ 4.722,00 USD (cuatro mil setecientos veintidós dólares americanos, con 00/100)*

Vicerrectorado de Investigación, Innovación y Vinculación
Campus Politécnico "J. Rubén Orellana R / Av. Ladrón de Guevara E11-253 y Andalucía/ Teléfono: 2976300 Ext. 1050
Quito-Ecuador

3. INFORME FINAL:

Mediante Memorando Nro. EPN-PII-17-14-2020-0001-M del 23 de enero de 2020 la Ph.D. Myriam Hernández, Directora del Proyecto PII-17-14, presenta el Informe Final del Proyecto Interno, y mediante Memorando Nro. EPN-PII-17-14-2020-0002-M del 27 de enero de 2020 hace la entrega del acta de asignación de bienes del proyecto. La información es revisada por la Dirección de Investigación, y se anexa y forma parte integrante del Acta de Finalización, cuyas conclusiones y productos generados son:

CONCLUSIONES:

- El mayor entregable del proyecto es un dataset con el cual se pudieron obtener modelos para detección y prevención de Ransomware. Para la generación de modelos se definieron atributos de los datos a través de la gran cantidad de procesos ejecutados tanto en memoria como en el sistema, el número de claves de registro alteradas, el número de peticiones que se realizan a los servidores o host externos y la gran cantidad de URLs almacenadas en memoria. Se listaron estas características y se asociaron a los respectivos artefactos. Con los modelos generados se puede identificar si hay un ataque y si se relaciona con una muestra de CryptoLocker, CryptoWall, PetrWrap, Petya o WannaCry.

- Siendo el dataset de carácter público, la comunidad científica lo podrá utilizar para generar nuevos modelos de detección de Ransomware usando diferentes tipos de algoritmos de aprendizaje automático.

PRODUCTOS:

- Artículo: "*A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters*"; Herrera Juan, Barona Lorena, Valdivieso Ángel, Hernández Myriam; "Remote Sensing" (Scopus Q1); ISSN: 20724292; DOI: 10.3390/rs11101168; abril 2019.

- Artículo: "*Ransomware dataset based on dynamic analysis*"; Herrera J.A., Veloz F.D.B., López L.I.B., Caraguay Á.L.V., Hernández M.; "RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao" (Scopus Q3); ISSN: 1646-9895; enero 2019.

- Artículo publicado: "*Key indicators in ransomware detection*"; Veloz F.D.B., López L.I.B., Caraguay Á.L.V., Hernández M.; "RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao" (Scopus Q3); ISSN: 1646-9895; enero 2019.

- Proyecto de titulación finalizado en Ingeniería en Sistemas Informáticos y de Computación: "*Análisis de correlación automática para detección de ataques ransomware en ambiente de pruebas*"; Bazante Veloz Freddy Daniel; https://bibdigital.epn.edu.ec/handle/15000/20121; marzo 2019.

- Conferencia: "*Dataset de Ransomware basado en análisis dinámico*"; Hernández Myriam; I Congreso de Ciencia de la Computación, Electrónica e Industrial CSEI 2019 (Scopus), Ecuador, Ambato; octubre 2019.

4. LIQUIDACIÓN ECONÓMICA:

El monto asignado al Proyecto Interno PII-17-14 fue de $ 4.998,53 USD (cuatro mil novecientos noventaiocho dólares americanos, con 53/100), y se ejecutaron $ 4.722,00 USD (cuatro mil setecientos veintidós dólares americanos, con 00/100), conforme al detalle emitido por la Unidad de Gestión de

Vicerrectorado de Investigación, Innovación y Vinculación
Campus Politécnico "J. Rubén Orellana R / Av. Ladrón de Guevara E11-253 y Andalucía/ Teléfono: 2976300 Ext. 1050
Quito-Ecuador

Investigación y Proyección Social del Vicerrectorado de Investigación, Innovación y Vinculación, que se adjunta a la presente Acta y forma parte integrante de la misma.

5. FINALIZACIÓN:

Con la presente Acta se declara finalizado y cerrado el Proyecto Interno PII-17-14 "*Detección de Ransomware a gran escala por medio de seguridad cognitiva*".

Para constancia de lo ejecutado y por estar de acuerdo con el contenido de la presente Acta, las partes libre y voluntariamente suscriben la misma, en tres ejemplares de igual contenido, tenor y valor legal.

Dado en la ciudad de Quito, D.M. a los tres días del mes de febrero del año dos mil veinte.

ESCUELA POLITÉCNICA NACIONAL
VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y VINCULACIÓN

Ph.D. Alexandra Alvarado
Vicerrectora de Investigación, Innovación y Vinculación

Ph.D. Myriam Hernández
Directora del Proyecto PII-17-14

sp/cr

Recibido
11/02/2020

Vicerrectorado de Investigación, Innovación y Vinculación
Campus Politécnico "J. Rubén Orellana R / Av. Ladrón de Guevara E11-253 y Andalucía/ Teléfono: 2976300 Ext. 1050
Quito-Ecuador