Aplicación de técnicas de análisis de datos y de aprendizaje automático para la caracterización y detección de campañas de ransomware

26 de agosto de 2022

1. Nombre del Tutor del Proyecto

David Arroyo Guardeño

2. Nombre del Grupo de Investigación asociado a AI-HUB

Grupo de Investigación en Criptografía y Seguridad de la Información, Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo".

3. Ubicación del centro donde se disfrutrará la beca

C/Serrano nº 144, 2806 Madrid

4. Título del proyecto

Aplicación de técnicas de análisis de datos y de aprendizaje automático para la caracterización y detección de campañas de ransomware

5. Descripción del proyecto

La proliferación de ciberataques es una constante que preside nuestro día a día y que atenta contra la continuidad de nuestro modelo de sociedad. El 17 de julio de 2022 el Consejo Superior de Investigaciones Científicas sufrío un ataque de ransomware supuestamente atribuido al grupo de ciber-extorsión Vice Society. Esta incidencia y la respuesta desplegada por parte de la institución y

organismos involucrados en la investigación de este ciberataque pone de relieve la necesidad de desarrollar un protocolo de detección temprana de ciberamenazas. En el caso de ransomware, esto paso por analizar en profunidad los tipos de campañas que se han llevado a cabo en el pasado, tratando de inferir un conjuto base de recomendaciones de la respuesta desplegada por los organismos y actores afectados. El presente proyeto estudiará mediante técnicas de Procesamiento de Lenguaje Natural datasets extraídos de foros de discusión de grupos de ciberextorsión en la DeepWeb. Ese análisis estará orientado a determinar qué tipo de extorsión se pone en juego en cada tipo de grupo, al mismo tiempo que se extraerá un cronograma con la secuencia temporal de ataques de ransomware en el pasado. Este análisis se complementará con un análisis agregado de redes sociales online (fundamentalmente, Twitter) con objeto de anticipar posibles campañas de ciberextorsión. El trabajo comprenderá una revisión del estado del arte relativo a la ciber-extorsión de ransomware y las denominadas Amenazas Avanzadas Persistentes (Advanced Persistent Threats). En esa revisión, se estudiará cómo criptodivisas como Bitcoin son empleadas por los sistemas de ciber-extorsión para recibir el pago por parte de las víctimas de ataques de ransomware.

El plan de formación a llevar a cabo se centrará en la identificación y/o creación de conjunto de datos y en el entrenamiento/validación de técnicas de Procesamiento de Lenguaje Natural para la caracterización de foros de discusión en DeepWeb vinculados con ciberextorsión y ransomware. El equipo de trabajo encargado de supervisar el plan de formación ha formado parte del proyecto TRESCA y en la actualidad está involucrado en el proyecto XAI-Disinfodemics adscrito a la temática 18 ("Desinformación, engaños y noticias falsas a través de canales públicos y privados") de la convocatoria de proyectos en líneas estratégicas 2021 de la Agencia Estatal de Investigación. La herramienta MsW desarrollada en TRESCA y en fase de mejora en XAI-Disinfodemics será empleada para extraer los datasets de interés desde redes sociales online. La labor de formación estará centrada en ver cómo mejorar el MsW mediane la integración de herramientas de análisis de la DeepWeb. Dicho de otra forma, el plan de formación está adscrito al campo de la ciberinteligencia y la investigación de ciber-criminalidad mediate integración de fuentes abiertas de datos y datos procendentes de DeepWeb y de actividad de criptodivisas (en concreto, Bitcoin).