**F\_AA\_225**

**FACULTAD DE INGENIERÍA DE SISTEMAS**

**CARRERA DE INGENIERÍA EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN**

**PLAN DE TRABAJO DE TITULACIÓN/TESIS**

**TIPO DE TRABAJO DE TITULACIÓN: PROYECTO INTEGRADOR**

|  |  |
| --- | --- |
| **I.- INFORMACIÓN BÁSICA** | |
| **PROPUESTO POR:**  Freddy Daniel Bazante Veloz | **LÍNEA DE INVESTIGACIÓN:**  Sistemas de Información |
| **AUSPICIADO POR:**  Dra. Myriam Hernández A.  Dra. Lorena Barona L. | **FECHA:**  26/06/2018 |
| **RELACIÓN:**  **Nombre del Proyecto de Investigación: N/A**  **Director del Proyecto de Investigación: N/A** | |
| **II.- INFORMACIÓN DEL TRABAJO DE TITULACIÓN** | |
| 1. **Título del Trabajo de Titulación**   ANÁLISIS DE CORRELACIÓN AUTOMÁTICA PARA DETECCIÓN DE ATAQUES RANSOMWARE EN AMBIENTE DE PRUEBAS. | |
| 1. **Planteamiento del Problema**   En la actualidad los diversos tipos de ataques a los sistemas de información han provocado un caos en numerosas instituciones, sean estas bancarias, de educación entre otras. Este problema se debe a la falta de controles y políticas de seguridad frente a posibles ataques.  En los últimos años se han encontrado un sin número de ataques, entre ellos varios tipos de malware, ransomware, denegación de servicios (DoS), como los más conocidos. Con la aparición de estos ataques también se han buscado métodos para protección de la información de los sistemas tales como antivirus, firewalls, sistemas de detección de intrusión o Intrusion Detection System en inglés (IDS), etc. Sin embargo, no son suficientes para saber cómo hacer un plan de contingencia frente a ellos.  El problema radica en que existen extensas bases de datos sobre malware y ransomware pero no se tiene una clasificación correcta de estos. Para ello usando herramientas de correlación automática a través de patrones y atributos se puede realizar una clasificación que ayudará a contrarrestar los posibles ataques y tener un plan de recuperación frente a incidentes. | |
| 1. **Justificación**   **3.1 Justificación Teórica**  Contrarrestar las tendencias de los ataques teniendo en cuenta los diferentes atributos filtrados para la presentación de amenazas relevantes. Para ello se ha visto la necesidad de realizar la recopilación de datos relacionados con ataques de ransomware mediante la implementación de un ambiente controlado, con lo cual se puede analizar muestras maliciosas que buscan hacer daño. Cabe destacar que cada tipo de malware y ransomware tienen atributos los cuales se identifican a través de ciertas especificaciones, como, por ejemplo, hashes.  Para dar un enfoque más claro frente a esta problemática cabe definir lo que es el análisis de ataques ransomware, como también el término ransomware. A continuación, se muestra una pequeña definición de lo antes expuesto:  El análisis de ataques ransomware se lo puede definir como la recopilación de información acerca de dicho malware, para ser más concretos se estudian atributos tales como patrones de encriptación o hashes (sha, md5 como ejemplos) y también su comportamiento en diferentes plataformas (Windows, Android, entre otros) [1].  Para poder definir ransomware se debe tomar en cuenta que es un tipo de software maicioso o malware. Entonces el ransomware (secuestro de información) es el término genérico para referirse a todo tipo de software malicioso que le exige al usuario del equipo el pago de un rescate. Al concretar la infección, puede bloquear el acceso al equipo o bien cifrar archivos para dejarlos inaccesibles. En el primer caso se trataría de un ransomware de bloqueo de pantalla o lockscreen; en el segundo, de un ransomware criptográfico o filecoder [2].  **3.2 Justificación Metodológica.**  Para el presente trabajo de investigación, se implementará un ambiente de pruebas controlado y un análisis de muestras de ransomware a través del filtrado de sus atributos, con los cuales se realizará una detección vía clasificación automática de ataques por ransomware. La detección oportuna permitirá respuestas más efectivas a ese tipo de ataques.  Con lo expuesto anteriormente se usará una metodología de análisis de malware en la cual se recopila las muestras del ransomware como también información acerca de sus atributos y comportamiento.  El uso de herramientas de correlación automática también ayudará en el proceso del análisis. EN este punto se usará la herramienta CUCKOO SANDBOX la cual es un sistema de análisis de malware automatizado de fuente abierta [4].  CUCKOO nos permitirá generar informes con diferentes características del ransomware que se analice.  **3.3 Justificación Práctica**  El análisis de ransomware en un ambiente controlado de pruebas, puede ser aplicado en diferentes empresas u organizaciones, que, con la detección temprana de ataques de este tipo, podrán diseñar planes de contingencia efectivos. De igual manera, con el análisis del comportamiento y patrones de logs asociados a ransomware, se podrá obtener información que ayude a prevenir pérdidas significativas a las organizaciones que pueden sufrir estas amenazas.  En vista de que el análisis ayudará notablemente, los beneficiarios serán la comunidad científica como también la comunidad estudiantil, es decir, toda la información recabada estará disponible para todo aquel que pertenezca a un ámbito científico y estudiantil. | |
| 1. **Hipótesis (Si aplica)**   N/A | |
| 1. **Objetivo General**   Implementar un ambiente controlado para análisis de ransomware. | |
| 1. **Objetivos Específicos**  * Simular ataques de ransomware a través de muestras de cryptolocker y wannacry en el ambiente de pruebas. * Filtrar atributos relevantes de los ataques ransomware para realizar análisis automático, usando clasificadores que apliquen machine learning. * Almacenar la información obtenida sobre patrones de comportamiento en logs de distintos tipos de ransomware, para que sirva de base en la detección temprana de ataques y que permita la implementación de planes de contingencia y recuperación frente a estas amenazas.   *.* | |
| 1. **Metodología**   Se emplearán métodos de extracción de la información de los patrones y de los atributos de ransomware en los logs y se realizará el respectivo filtrado de atributos para mantener solamente los relevantes para la fase de análisis. Se aplicará un tablero Kanban para realizar el seguimiento del estado de las actividades. Estas actividades tendrán 4 estados: pendiente, en desarrollo, en pruebas y finalizada. Con la información de los atributos en logs, se utilizarán métodos de correlación automática para clasificar y detectar en forma temprana este tipo de amenazas. Los patrones encontrados se presentarán como datos base y serán usados en los planes de contingencia y recuperación de ataques. Todo el proceso se lo dividirá en 4 fases.  En la primera fase se creará un ambiente seguro y controlado para analizar el ransomware con Oracle VirtualBox, que es una de las herramientas de virtualización más utilizadas. Bajo este ambiente se podrá supervisar y determinar las actividades del ransomware. A pesar de que con frecuencia el ransomware utiliza técnicas de evasión, al sospechar que está siendo  ejecutado bajo un ambiente virtual.  En la seguda fase, para realizar un análisis dinámico es necesario establecer un ambiente complejo, ya que se debe ejecutar el ransomware para observar su comportamiento. El ransomware se comporta de manera diferente dependiendo del sistema operativo y el entorno en el que se está ejecutando.  En la tercera fase es importante la configuración de la red donde se va a colocar el escenario,  debido a que algunos ransomware suelen ser auto-replicantes, otros utilizan el internet para  comunicarse con su servidor de malware autor.  En la fase cuatro, dentro del escenario virtual de CUCKOO SANDBOX, se contará con un equipo principal (host físico) que consiste en un software central de gestión bajo el sistema operativo Ubuntu 18.04, este se ocupa de las ejecuciones de muestras de ransomware y análisis, ya que es aquí donde se podrá visualizar los resultados de las muestras. También se encuentran las maquinas victimas (host virtualizados) que se conectan en red con el equipo principal, estas se componen de un software cliente bajo el sistema operativo windows7, son las maquinas que serán infectadas con las muestras de ransomware. | |
| 1. **Plan de Trabajo**   Las actividades planificadas para el desarrollo del proyecto son:   * 1. Realización del estado del arte sobre ransomware, técnicas de análisis de ransomware y herramientas para el análisis   2. Revisión del estado del arte por parte del director y codirector de tesis.   3. Realización de un marco metodológico en el cual constará la instalación de CUCKOO SANDBOX, configuración de CUCKO SANDBOX, obtención de las muestras de ransomware, colocación de muestras de ransomware en el sistema. Ejecución de pruebas y recolección de información del proceso de pruebas.   4. Análisis de la información para establecer patrones de detección temprana de ransomware.   5. Informe sobre los resultados obtenidos en el proceso de pruebas.   6. Proveer conclusiones y recomendaciones.   7. Presentación de documentos y anillados para la defensa.   8. Defensa del proyecto | |
| 1. **Bibliografía**   [1] Monika, P. Zavarski y D. Lindskog «Experimental Analysis of Ransomware on  Windows and Android Platforms: Evolution and Characterization, » 2016.  [En línea]. Available: https://www.sciencedirect.com/science/article/pii/S1877050916318221#! [Último acceso: 09 julio 2018].  [2] ESET, «TODO SOBRE EL RANSOMWARE:» 2016.  [En línea]. Available:  http://www.eset-la.com/pdf/kit-antiransomware/Guia-Todo\_Sobre\_Ransomware.pdf.  [Último acceso: 26 junio 2018].  [3] C. Guarnieri, «CUCKOO – Automated Malware Analysis,» 2017.  [En línea]. Available: https://cuckoo.sh/docs/ [Último acceso: 26 junio 2018].  [4] CUCKOO SANDBOX, «CUCKOO SANDBOX» 2017.  [En línea]. Available: https://cuckoosandbox.org/. [Último acceso: 26 junio 2018].  [5] CCN-CERT, «MEDIDAS DE SEGURIDAD CONTRA RANSOMWARE:» 2016.  [En línea]. Available:  https://www.uv.es/websiuv/documentos/seguretat/privado/recsegccncert.pdf  [Último acceso: 26 junio 2018].  [6] F. Carranza, «Seguridad Informática: virus ransomware, el Secuestro virtual de datos es Posible,» 2017. [En línea]. Available:https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/13925/ MEDINA%20 CARRANZA%20FACUNDO%20MARTIN.pdf?sequence=  1&isAllowed=y [Último acceso: 26 junio 2018].  [7] Github, «github,» 2018. [En línea]. Available: https://github.com/cuckoosandbox/cuckoo. [Último acceso: 10 julio 2018].  [8] B. Saleh, M. Aizaini y S. Modh «Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions,» 2018.  [En línea]. Available: https://www.sciencedirect.com/science/article/pii/S016740481830004X [Último acceso: 10 julio 2018].  [9] J. Gómez, L. Álvarez y P. García «R-Locker: Thwarting ransomware action through a honeyfile-based approach,» 2018. [En línea]. Available: https://www.sciencedirect.com/science/article/pii/S0167404817302560 [Último acceso: 10 julio 2018].  [10] Z. Asma y A Munam. «IoT Based Ransomware Growth Rate Evaluation and Detection Using Command and Control Blacklisting,» 2017. [En línea]. Available: https://ieeexplore.ieee.org/document/8082013/?reload=true [Último acceso: 10 julio 2018]. | |
| 1. Cronograma  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin | Predecesoras | responsable | | **Programada automáticamente** | **Proyecto Integrador** | **480 horas** | **lun 16/07/18** | **vie 05/10/18** |  |  | | Programada automáticamente | Realización del estado del arte sobre ransomware , técnicas de análisis de ransomware y herramientas para el análisis | 36 horas | lun 16/07/18 | vie 20/07/18 |  | Freddy Bazante | | Programada automáticamente | Revisión del estado del arte | 24 horas | vie 20/07/18 | mié 25/07/18 | 2 | Dra. Myriam Hernández y Dra. Lorena Barona | | **Programada automáticamente** | **Realización de un marco metodológico** | **368 horas** | **mié 25/07/18** | **jue 27/09/18** | **3** |  | | Programada automáticamente | Instalación de CUCKOO SANDBOX | 100 horas | mié 25/07/18 | vie 10/08/18 | 3 | Freddy Bazante | | Programada automáticamente | Configuración de CUCKOO SANDBOX | 70 horas | lun 13/08/18 | jue 23/08/18 | 5 | Freddy Bazante | | Programada automáticamente | Obtención de muestras de ransomware | 50 horas | jue 23/08/18 | vie 31/08/18 | 6 | Freddy Bazante | | Programada automáticamente | Colocación de muestras de ransomware en el sistema | 48 horas | lun 03/09/18 | lun 10/09/18 | 7 | Freddy Bazante | | Programada automáticamente | Ejecución de pruebas funcionales del sistema | 50 horas | mar 11/09/18 | mié 19/09/18 | 8 | Freddy Bazante | | Programada automáticamente | Recolección de información después del proceso de pruebas | 50 horas | mié 19/09/18 | jue 27/09/18 | 9 | Freddy Bazante | | Programada automáticamente | Realización de un informe de resultados obtenidos de las pruebas | 36 horas | jue 27/09/18 | mié 03/10/18 | 4 | Freddy Bazante | | Programada automáticamente | Análisis de la información para establecer patrones de detección temprana de ransomware | 10 horas | jue 27/09/18 | vie 28/09/18 | 4 | Freddy Bazante | | Programada automáticamente | Proveer conclusiones y recomendaciones | 10 horas | vie 28/09/18 | lun 01/10/18 | 12 | Freddy Bazante | | Programada automáticamente | Presentación de documentos y anillados para la defensa | 24 horas | mar 02/10/18 | jue 04/10/18 | 13 | Freddy Bazante | | Programada automáticamente | Defensa del proyecto | 8 horas | vie 05/10/18 | vie 05/10/18 | 14 | Freddy Bazante | | |

Firma

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Freddy Daniel Bazante Veloz |  |  |  |  |
| Proponente |  |  |  |  |
| Email: Freddy.bazante@epn.edu.ec  Telf.: 0987020787 |  |  |  |  |

Firma Firma

|  |  |  |
| --- | --- | --- |
| Dra. Myriam Beatriz Hernández Álvarez |  | Dra. Lorena Isabel Barona López |
| DIRECTOR |  | CODIRECTOR |
| Email: Myriam.hernandez@epn.edu.ec  Telf.: 0992715620 |  | Email: lorena.barona@epn.edu.ec  Telf.: 0987800285 |