PROTOCOLO DEL PROYECTO (CI-02/2023)

NOMBRE DE LA INSTITUCIÓN	Instituto Tecnológico de Morelia

Título del proyecto:

Modelo de detección temprano de ataques de malware en redes públicas, utilizando técnicas de machine learning para un sistema de predicción: Buenas prácticas anti Ransomware

1. DESCRIPCIÓN DEL PROYECTO

1.1 Resumen

La falta de seguridad, y las activiades de la delincuencia conocidos como ciberterroristas, son de los problemas más importantes que afronta México en la post pandemia del virus COVID-19, y el mundo digital. Los sistemas de vigilancia y monitoreo automatizados, al igual que los sistemas de prevención y contención de ataques de Malware (software malicioso), son una solución que presenta muchas ventajas para garantizar la seguridad de la información en las empresas.

Se desarrollará e implementará un prototipo de un sistema que detecte ataques de Malware en equipo de cómputo que son utilizados en redes públicas y en software vulnerable al secuestro de datos (conocido como ataque Ransomware). La utilización de Machine Learning (ML) que es una rama de la Inteligencia articificial (IA) permitirá la detección y el monitoreo utilizando técnicas de IA, para así prevenir y evitar problemas o incidentes de seguridad.

1.2 Introducción

Muchos sistemas y aplicaciones de software hoy en día usan una gran cantidad de dispositivos, componentes y equipo de cómputo (hosts) interconectados entre sí, los cuales, por sus configuraciones, un gran porcentaje no contemplan medidas de seguridad en sus servicios de interconexión o esta configuración es casi nula y pueden conllevar a un grave problema de seguridad al estar conectados en red, es decir, estos sistemas no cuentan con sistemas que detecten, alerten o contengan los posibles ciberataques de malware. “Ya no es novedad para las empresas y sus dirigentes que los ataques Ransomware son una amenaza latente, y que, de ser víctimas de este crimen, el impacto económico será de grandes dimensiones” (Consultek, 2022). Este tipo de ataques se lleva a cabo en cualquier tipo de sistema operativo y múltiples plataformas como dispositivos periféricos, almacenamiento externo, entornos virtuales y físicos.

Tomando en consideración las posibles afectaciones que se describen a continuación:
1. Pérdida de imagen y confianza.
2. Pérdida económica por interrupción del funcionamiento normal del negocio.
3. Robo y/o secuestro de datos.
4. Gasto por pago de la extorsión.
5. Daño o pérdida de datos, así como el mal funcionamiento de los sistemas y aplicaciones de software.
6. Costo por demandas o responsabilidades legales.
7. Gasto por la notificación y advertencia de nuestros usuarios y clientes.
8. Gestión de la crisis, recuperación de la información y puesta nuevamente en marcha de los sistemas.

“Es por esto que no sorprende observar a las grandes empresas, año tras año, asignando cada vez más presupuesto a sus sistemas de seguridad, ya que puede resultar mucho más costoso recuperarse de un ataque de Ransomware que prevenirlo. Además de la rectificación de los daños ocasionados, se presentan afectaciones en cuanto al tiempo de inactividad, horas de trabajo, costo de la red, dispositivos afectados y oportunidades comerciales perdidas. Cada día, es más costoso lidiar con los ciberataques. De hecho, uno de los sucesos más recordados al respecto fue el ciberataque global del Ransomware, a través del Malware WannaCry, que inició mediante la compañía Telefónica en España y terminó infectando a más de 300,000 computadoras a lo largo de 150 países. Esto significó un impacto económico de más de $1,000 millones de dólares americanos” (Consultek, 2022). De acuerdo con un sondeo realizado para el estudio ”El estado del ransomware 2022”, ordenado por la empresa de ciberseguridad Sophos, el 44% de las compañías hackeadas pagó el rescate de sus datos y en promedio, la cantidad de dinero destinada a ello fue de 480 mil dólares, es decir, alrededor de 9.6 millones de pesos.

“Evidentemente, el costo del rescate excede por mucho cualquier inversión en prevención, que de hecho, es la mejor práctica que se puede implementar. En promedio el costo financiero de un ataque ransomware, incluyendo lo invertido en el rescate, es de $133 000 dólares”.

Cabe hace notar que cualquiera puede ser objetivo de un ataque Ransomware, desde un país, una empresa, instituto público/privado, o bien, una persona. Esto porque la mayoría de los ataques de Ransomware continúan estando dirigidos a personas clave de las organizaciones o institutos, y a los equipos de trabajo que pueden contener información valiosa, o que a través de ellos se puede llegar a activos críticos.

El Ransomware es un malware especial que demanda un pago para recuperar la funcionalidad robada, principalmente de datos. Los vectores de ataque que más utilizan este tipo de troyanos extorsivos son: el protocolo de escritorio remoto RDP, las vulnerabilidades de software y los correos electrónicos engañosos (phishing). Existen varios tipos de Ransomware como los que se presentan a continuación:

- Locking: Bloquea el uso del computador / dificulta su interacción modificando su GUI o el navegador utilizado.
- Cripto: Cifran el disco duro / archivos y extorsiona a la víctima para recuperar los datos.
- MBR: Modifican el MBR (Master Boot Record) para evitar el arranque del sistema hasta que se pague el rescate.

Los ataques de Ransomware vienen en las más variadas formas y tamaños. El vector de ataque es siempre un factor que condiciona el tipo de Ransomware utilizado. Para estimar el tamaño o el alcance de un ataque, es necesario evaluar qué es lo que está en riesgo y qué clase de información podría desaparecer o quedar expuesta. Las estrategias para contener los efectos de un ataque son las mismas para todos los tipos de Ransomware: usar adecuadamente una solución de seguridad y contar con copias o respaldos de seguridad.

El 27% de los incidentes de malware notificado en 2020 fue atribuido al Ransomware, el cual de acuerdo con la consultora Gartner tiene un impacto mayor en una organización que una filtración de datos. Pronósticos de Cybersecurity Venture, apuntan que cada 11 segundos una empresa será víctima de un ataque de Ransomware a nivel mundial en 2021. Los atacantes del Ransomware están demostrando ser una amenaza continua para la ciberseguridad.

Una vez comprometida la computadora del usuario, el atacante se puede mover dentro de la red en busca de activos con información valiosa, como servidores de datos, etc. Por lo que es importante dar a conocer la importancia de la seguridad informática en las redes locales y públicas, especialmente en la implementación de sistemas de tipo Firewall, ya que nos permite tener un mayor control en el tráfico de los datos por medio de permisos para transitar en la red y que los datos no puedan fluir de manera libre y descontrolada.

Las redes y sistemas computaciones de la mayoría de los Institutos de Educación Superior Públicas actualmente no cuentan ni con esquemas de seguridad ni con un sistema que permita el filtrado de tráfico de red que contenga al Ransomware o ataques parecidos, por lo cual están vulnerable a ataques de este tipo.

Es por todo lo mencionado anteriormente, que se considera necesario realizar la creación e implantación de un sistema, que sea capaz de realizar una detección temprana en tiempo real de contenidos potenciales de Ransomware, en las redes de computadoras y sistemas de información de estos Institutos.

La detección temprana es clave, y más cuando el Ransomware puede costar a las empresas grandes sumas de dinero, por ello la importancia de lograr una detección rápida que permita actuar con rapidez y detener un ataque al inicio del proceso, antes de que se propague dentro de la red y afecte a las aplicaciones, información y servicios críticos.

Ahora bien, un sistema de detección de rasomware combinado con técnicas de Machine Learning, puede convertirse en un buen aliado para ir más allá de las firmas o comportamientos conocidos, y ser capaz así de encontrar patrones previamente desconocidos.

Machine Learning

El área de Inteligencia Artificial (IA) con el transcurso de los años ha desarrollado diversas técnicas de aprendizaje de máquina para múltiples aplicaciones en el mundo real. Una de ellas, es el Machine Learning (ML), que es una forma de la Inteligencia Artificial que permite a un sistema aprender de los datos, en lugar de aprender mediante la programación explícita. Sin embargo, machine learning no es un proceso sencillo. Conforme el algoritmo procesa datos de entrenamiento, es posible producir modelos más precisos basados en datos. Un modelo de machine learning es la salida

de información que se genera cuando entrena su algoritmo de machine learning con datos. Después del entrenamiento, al alimentar al modelo con una entrada, éste dará una salida. Por ejemplo, un algoritmo predictivo creará un modelo predictivo. A continuación, cuando se le proporcione al modelo predictivo datos, generará un pronóstico basado en los datos que entrenaron al modelo (A. D., 2020), (Apd R., 2020) y (Machine Learning, 2020).

Machine learning (ML) permite entrenar modelos con conjuntos de datos antes de ser llevados a producción. Algunos modelos de machine learning están online y son continuos. Este proceso iterativo de modelos online conduce a una mejora en los tipos de asociaciones hechas entre los elementos de datos. Debido a su complejidad y tamaño, estos patrones y asociaciones podrían haber sido fácilmente pasados por alto por la observación humana. Después de que un modelo ha sido entrenado, se puede utilizar en tiempo real para aprender de los datos. Las mejoras en la precisión son el resultado del proceso de entrenamiento y la automatización que forman parte del machine learning y del algortimo.

El uso de Machine Learning en la protección de datos, basado en el aprendizaje tomando como referencia un conjunto de datos, conocidos como DataSets, puede proporcionar lo siguiente:

- Detección de casi todo el nuevo malware sin necesidad de actualizaciones.
- Detección de vulnerabilidades de día cero en tiempo real de amenazas nuevas y emergentes.
- Necesidad reducida de actualizaciones puntuales.
- Protección contra la amplia gama de amenazas, ransomware, vulnerabilidades y ataques dirigidos.

Consideremos esto: a medida que se ejecuta un programa, existe un historial de lo que sucede en diferentes momentos. Al analizar lo que sucede en cada etapa, se aclara la actividad normal y se crea un modelo de referencia, es decir, un modelo de comportamiento normal. En el caso de un ataque de Ransomware, se inyectaría un nuevo código en este proceso, que se nota fácilmente comparado contra el comportamiento diario normal.

Las soluciones de software más sólidas utilizan ML que considera sólo los puntos de referencia más populares y excluye las aberraciones. Este enfoque refina o ajusta aún más el conocimiento de la máquina sobre el código bueno y el código malicioso, no sólo aumentando la precisión, sino también mejorando el rendimiento del software, ya que el modelo de aprendizaje automático consume muchos menos datos para ejecutarse.

El ML se utilizará para procesar, extraer y resumir las informaciones útiles que ayuden en la detección de los ataques ransomware al sistema. Es decir, se desarrollará un sistema prototipo que lleve a cabo un análisis de las posibles vulnerabilidades existentes en los hosts.

En resumen, se creará un prototipo que detecte ataques de malware a sistemas de cómputo que son utilizados en la industria 4.0 así como en redes públicas y en todo tipo de sistema vulnerable al ransomware. La utilización de Machine Learning (ML) permitirá el monitoreo utilizando técnicas de inteligencia artificial, y así prevenir, detectar y tratar de evitar problemas o incidentes de seguridad en ese tipo de sistemas.

1.3 Antecedentes

Aguilar Daniel y Guaita Franklin (2019), desarrollaron una investigación en la que se profundiza en la historia, caracterización, detección y mitigación del software malicioso Ransomware y sus variantes. Es así que, como mencionan, según información de la corporación Manage Engine, el ataque cibernético más grande fue registrado en el año 2017, el cual evidenció un ataque masivo a escala global provocado por un tipo de Ransomware llamado WannaCry que afectó a empresas de telecomunicaciones, hospitales y compañías de reparto. Sin embargo, otros Ransomware más sofisticados conocidos como Petya y Jigsaw han vulnerado la seguridad de otras organizaciones europeas. En el caso de Petya se dirige a computadoras con sistemas operativos Windows que no están actualizados a diferencia de WannaCry, los datos perdidos nunca se pueden recuperar. Por otro lado, Jigsaw otra variedad de Ransomware, es una infección seria que puede infiltrarse en el sistema e intentar forzar al usuario a pagar dinero, el inconveniente es que no hay garantías de que conseguirá una clave de desencriptación.

Es así que en el presente trabajo se pretende realiza una evaluación de algunos ataques Ransomware: WannaCry, Jigsaw, y Petya. Para lo cual se empleará un entorno virtual de red, que permite identificar el modo de operación de dichos ataques en la encriptación de información.

Como plataforma de experimentación se diseña una red híbrida con segmentación WAN, LAN y DMZ que permite

propagar el malware, encriptando la información de los endpoints. Para evaluar los tipos de ataques propuestos se usará un mecanismo de infección controlado a partir de un Ransomware de la web con fines educativos.

Detección de Ransomware con técnicas de Honeypot

Moore (2016) en la conferencia de Ciberseguridad y Cyberforensia, mencionó una investigación llamada “Detection Ransomware with Honeypot Techniques” [Detectando Ransomware con técnicas de Honeypot] en la cual investigó métodos para implementar un Honeypot para la detección de Ransomware. Moore (2016) comenzó este estudio ya que él notó que los ataques de Ransomware se están incrementando y que sobrepasa muchas soluciones técnicas aprovechándose de la ingeniería social.

También menciona que para poder detectarlo implementó una carpeta tipo Honeypot junto con los servicios de vigilancia de Windows, uno de estos servicios es EventSentry para manipular registros de seguridad, el otro es File Screening para controlar el acceso, y puede ser usada para bloquear la escritura de archivos no autorizados.

En su experimento puso la carpeta Honeypot en una computadora conectada a una red e infectó la máquina con Ransomware como resultado logró bloquear el servicio de Red para evitar que este se propague con un retraso de 6 segundos de la ejecución del Ransomware enviando un correo electrónico al administrador del sistema del registro indicando que muchos archivos habían sido atacados.

Al final resaltó que detectar Ransomware por medio de un firewall es muy difícil ya que tiene una naturaleza cambiante, pero cabe resaltar que a pesar de que tenga esa naturaleza el funcionamiento interno siempre es el mismo, ya que busca terminaciones de archivos y los encripta, y es por esto que se sugiere que se use un “canario minero” o una carpeta trampa para bloquear la escritura (encriptación) a archivos no autorizados.

1.4 Marco teórico

El Ransomware es un tipo de malware de extorsión mediante el cual los atacantes secuestran y cifran los archivos de la computadora de la víctima (TrendMicro, 2021). En este sentido, el propósito de un Ransomware es exigir un pago monetario, generalmente a través de bitcoins, para el rescate de los archivos. Varían según el tipo de Ransomware dependiendo del cobro de la extorsión donde incluyen opciones de pago alternativas, como las tarjetas de regalo de iTunes y Amazon o bitcoins. No obstante, el pago de un rescate por los datos no garantiza que los usuarios obtengan la clave de descifrado o la herramienta de desbloqueo necesarias para recuperar el acceso a los datos de la máquina infectada (Karpersky, 2021).

En general, el Ransomware explota las vulnerabilidades del sistema operativo y del usuario para introducirse en la computadora y encriptar todos sus archivos. De esta manera el atacante mantiene secuestrados los archivos de la víctima hasta que esta pague el rescate de los mismos. A pesar de las muchas variantes de Ransomware, se ha identificado que estos siguen un comportamiento similar. Primero, el malware busca ciertos archivos con extensiones como: .txt, .doc,. rft, .ppt, .chm, .cpp, .asm, .db, .db1, .dbx, .cgi, .dsw, .gzip, .zip, .jpg, .key, .mdb, .pgp y .pdf, entre otras (Orellana, 2018). Una vez identificados los archivos se inicia el proceso de cifrado (simétrico o asimétrico) de los mismos para limitar su acceso. A continuación, el atacante envía a la víctima una solicitud de rescate, bien sea por correo electrónico o usando una ventana emergente que exige la clave de cifrado que desbloquea los archivos congelados (Jatinder N.D. Gupta, 2008). Entre los ejemplos más conocidos de Ransomware que afectan a las computadoras de escritorio están WannaCry, Petya, XData, Reveton, CryptoLocker, CryptoWall y TeslaCrypt. Los que afectan las plataformas móviles incluyen Simplocker y LockerPin (Osorio-Sierra, 2020).

Tipos de Ransomware

Como se ha mencionado, existen diferentes variantes de Ransomware, sin embargo, estas pueden ser agrupadas en tres categorías o tipos (RansomwareEkans, 2020)): CryptoRansomware (CR), locker Ransomware o también conocidos como no criptográficos (NCR) y CryptoRansomware de llave privada. La empresa PCFORMAT (2021) e ICIBE-CERT (2021) plantean 2 definiciones Locker y CryptoRansomware(CR) este último tiene la misma funcionalidad del CryptoRansomwarede llave privada debido a que usan algoritmos de llaves públicas y privadas para cifrar la información, por este motivo y para efectos de la investigación tomaremos solo 2 definiciones:

1. CryptoRansomware

Los CryptoRansomware utilizan algoritmos criptográficos simétricos y asimétricos para cifrar los archivos, el malware comienza a cifrar los datos y archivos del usuario; una vez completado el cifrado, la víctima es informada de que todos sus datos están cifrados y sólo se pueden descifrar si paga el rescate. Las primeras versiones de CryptoRansomware almacenaban la clave de descifrado en el computador. Esto permitía recuperar dicha clave mediante ingeniería inversa. La evolución de este tipo de Ransomware se contactan con un servidor para enviar las llaves de cifrado. Algunos CryptoRansomware son más agresivos y no solo encriptan los datos, sino que también realizan otras acciones, por ejemplo, eliminar los archivos en el sistema infectado, si el pago no se realiza dentro de un plazo determinado (Cortés, 2021).

2. Locker Ransomware

Este tipo de Ransomware niega el acceso al dispositivo, es decir que bloquea la interfaz de usuario del dispositivo y luego solicita a la víctima el rescate. Esta variante de Ransomware deja a la víctima con muy pocas capacidades, por ejemplo, sólo le permite comunicarse con el atacante o realizar el pago del rescate.

A diferencia de los otros tipos de Ransomware, los locker no utilizan ninguna clase de cifrado. En su lugar, estos restringen por completo la interacción con el sistema operativo, bien sea bloqueando la pantalla, modificando el registro de arranque maestro (MBR) o la tabla de particiones del equipo infectado. Esta característica hace que los locker Ransomware sean considerados relativamente débiles porque el daño puede ser revertido sin pagar el rescate, es impotante entonces una detecciòn temprana (Panda Security, 2015).

Evolución de Ransomware

Aunque los conceptos teóricos iniciales fueron propuestos por Young y Yung en el año de 1996, el primer malware tipo Ransomware apareció en el año de 1989, cuando Joseph Popp creó un virus denominado AIDS, también conocido como PC Cyborg Trojan. Popp distribuyó dicho virus a través de 20000 diskettes que envió a investigadores del SIDA, a diferentes países del mundo. El atacante indicó a los investigadores que los diskettes contenían un programa que les ayudaría a analizar el riesgo que podía tener una persona para adquirir el virus del SIDA. Una vez instalado, el malware permanecía inactivo en los equipos y sólo se activaba después de que el equipo se encendiera 90 veces, punto en el cual exigía el pago de 180 dólares para permitir el acceso al equipo infectado. Dicho pago debía realizarse a una oficina de cobro en la ciudad de Panamá (Kharraz, A., et. al., 2015).

Más adelante, en el año 2005, apareció un virus denominado PGPCoder. Este malware infecta a los equipos a través de un archivo, llamado anketa.doc, que se adjuntaba a los correos electrónicos. El archivo contenía una macro maliciosa que cifraba todos los archivos con extensiones .doc, .xls, .pdf, .ppt, entre otras. Una vez encriptados los archivos, PGPCoder autodestruía el archivo infectado y creaba un nuevo archivo llamado readme.txt que proporcionaba la información sobre cómo contactarse con el atacante para recuperar los archivos cifrados (Kharraz, A., et. al., 2015).

En el año 2006, apareció Archiveus, el primer Ransomware que utiliza un cifrado asimétrico, junto con el algoritmo RSA para bloquear el acceso a los archivos de la máquina infectada. Para recuperar sus archivos, las víctimas tenían que comprar una contraseña de descifrado en ciertos sitios web específicos. Una particularidad de Archiveus es que sólo cifraba los archivos en la carpeta “Mis Documentos” en los equipos basados en Windows.

A partir de 2008, los Ransomware se convirtieron en un problema puesto que empezaron a engañar y a persuadir a los usuarios para que descargaran software falso, donde instalaba una copia del virus en la máquina. La cuestión con los falsos instaladores es que estos se veían y actuaban casi de la misma manera a como lo hacían sus contrapartes legítimas. No obstante, una vez se instalaba el virus, este solicitaba hasta 100 dólares para solucionar el problema en la máquina infectada (GitHub, 2021).

Para el año 2009 apareció el Ransomlock, el cual fue uno de los primeros Ransomware del tipo locker. Esta variante del malware tenía como objetivo bloquear el acceso al computador infectado hasta que se comprara un programa determinado o, se enviara un SMS (Servicio de Mensajes Cortos) a un número determinado que se proporcionaba en la pantalla de la máquina infectada.

Después, en el año 2012 surgió Reveton, un Ransomware basado en el troyano Citadel (Kharraz, A., et. al., 2015), que cifra los archivos del usuario y muestra un mensaje en la pantalla indicando que el computador ha sido usado para

actividades ilícitas, tales como descargas de software pirata o pornografía infantil. Con este mensaje, el virus hace creer al usuario que el remitente del mismo es una agencia del estado. Una vez el usuario accedía a los enlaces que se proporcionaban en el mensaje, este llevaba a sitios web comprometidos en los que se exigía el pago a través de tarjetas de pago (Kharraz, et. al., 2015).

Luego, con la creación del Bitcoin, en 2009, se abrió un método anónimo de extorsión que antes no estaba disponible para los atacantes. Esto llevó a que en el 2013 apareciera CryptoLocker, un Ransomware que se propagó rápidamente a través de sitios web comprometidos y archivos que llegaban mediante adjuntos de correos electrónicos maliciosos. CryptoLocker utilizó el algoritmo de cifrado AES-256 cifrando los archivos y documentos de equipos infectados mediante una central de comando donde realizaba ataques distribuidos a través de la red de Bots Zeus, además, distribuía las claves de descifrado usando la red TOR, cabe resaltar que fue el primero en usar TOR y cobrar en Bitcoins.

Para el año 2014, surgieron las primeras medidas contra los malware tipo Ransomware. Esto debido al incremento de ataques y a la aparición de variantes como CryptoWall, que se distribuían de forma masiva y generaron ingresos estimados de 325 millones de dólares para los ciberdelincuentes. También apareció CryptoDefense, que usaba encriptación RSA de 2048 bits pero dejaba la clave de desencriptación en texto plano en la computadora. CryptoWall empleaba kits de explotación y era más difícil de erradicar porque podía copiarse a sí mismo en las claves del registro y en las carpetas de inicio.

Para los años 2015 y 2016 aparecieron los primeros ataques a dispositivos móviles con el lanzamiento de LockerPin, un Ransomware que cambia el PIN de acceso de los teléfonos con el sistema operativo Android. Específicamente, este Ransomwar eexigía una suma de 500 dólares a las víctimas para desbloquear el dispositivo.

En estos mismos años también aparecieron los Ransomware diseñados para los usuarios de Linux. Encoder fue el primer Ransomware programado para atacar los sistemas de alojamiento web basados en Linux, bloqueando los directorios web y encriptando en el contenido aplicaciones como Magento y cPanel. Durante 2006 un Ransomware llamado Chimera tenía la particularidad de que no sólo encriptaba archivos, sino que también amenazaba con publicarlos en línea si no se pagaba el rescate, esta práctica es conocida como doxing.

El incremento de las variables de Ransomware consta de 32000 variantes nuevas y 337205 ataques generados por Ransomware. (Kaspersky Lab, 2016).

En el año 2017 se registró el primer ciberataque mundial con Ransomware mediante Wannacry, el cual infectó a más de 250.000 dispositivos utilizando técnicas de la herramienta de hacking EternalBlue filtrada por agentes de la NSA y una vulnerabilidad del protocolo SMB de Windows (Kharraz, et. al, 2015).

En años recientes se han desarrollado investigaciones con el propósito de identificar las técnicas y algoritmos de Machine Learning (ML) utilizadas para la detección y clasificación de las diferentes familias ransomware, así como las herramientas de software que se utilizan para la aplicación de estos algoritmos. Se han desarrollado metodologías para los algoritmos y técnicas de ML más utilizados como son: Random Forest (RF), Decisión Tree (DT), Long Short-Term Memory (LSTM), Support Vector Machine Learning (SVM) y Deep Neural Network (DNN). Muchos de estos trabajos están llegando a la conclusión que el ML permite detectar en las etapas iniciales, patrones de ataque de diferentes familias ransomware (Apd R., 2020), (A, D., 2020) y (Cumbicus Pineda, et. al., 2022).

1.5 Objetivos

Modelar e Implementar una metodología para la detección y contención de Ransomware utilizando herramientas de Machine Learning para generar un modelo de predicción y la mejora de la seguridad en redes públicas.

1. Identificar los distintos tipos del Ransomware y su impacto en redes públicas.
2. Investigar sobre Datasets para el modelo de entrenamiento
3. Limpiar y analizar el conjunto de datos para su procesamiento
4. Construir el modelo de predicción
5. Implementar el modelo de predicción en redes públicas
6. Aplicar la metodología para mejorar la seguridad en redes públicas
7. Implementación del sistema entrenado

1.6 Metas

PRODUCTOS ENTREGABLES	
Cantidad	**Tipo Entregable**
1	Tesis en desarrollo de Maestria
2	Alumnos residentes participantes en el proyecto
1	Artítulos de divulgación enviados
1	Registro de Software (INDAUTOR)

1.7 Impacto o beneficio en la solución a un problema relacionado con el sector productivo o la generación del conocimiento científico o tecnológico.

Detectar en etapas tempranas un ataque de Ransomware, en la mayoría de los ataques en redes públicas, utilizando un modelo de Machine Learning para evitar el cifrado de la información y el pago del ciber secuestro.

Cualquiera puede ser objetivo de un ataque Ransomware, desde un gobierno, una empresa, instituto o persona. Esto porque la mayoría de los ataques de Ransomware continúan estando dirigidos a personas clave de las organizaciones o institutos, y a los equipos de trabajo que pueden contener información valiosa, o que a través de ellos se puede llegar a activos críticos.

El Ransomware es un malware especial que demanda un pago para recuperar la funcionalidad robada, principalmente de datos. Los vectores de ataque que más utilizan los troyanos extorsivos son el protocolo de escritorio remoto RDP, las vulnerabilidades de software y los correos electrónicos engañosos (phishing).

Diseño del prototipo:

Se diseñará, modelará, entrenará e implementará un prototipo que detecte ataques de malware a sistemas de cómputo que son utilizados en redes públicas y en todo tipo de sistema vulnerable al ransomware. El modelo estará basado en Machine Learning (ML) permitiendo el monitoreo, utilizando técnicas de inteligencia artificial.

Resultados esperados:

- El modelo tenderá a prevenir, detectar y tratar de evitar problemas o incidentes de seguridad en ese tipo de sistemas.
- Se pretende que el modelo reduzca el secuestro y pago de rescate de la información.
- Beneficio a la comunidad académica, sector público y privado al contar con documentación y herramienta para la prevención de ransomware.
- Se documentará tanto las mejores prácticas como los resultados de las pruebas para ofrecer una guia de medidas anti-ransomware.

1.8 Metodología

En la fase inicial se analiza cómo detectar el malware en una red con solo observar el tráfico de red, también se comprende con qué tipo de malware se trabaja. La fase de entendimiento de los datos se comienza a analizar los datos iníciales e identificar los problemas de calidad de los datos; es decir si los datos son óptimos, pero para tener estos datos iníciales se trabajó en la obtención de los mismos, también se muestra cómo se capturo el flujo de trafico de red para luego almacenarla en una hoja de cálculo. En la fase de análisis se analiza los datos iníciales para luego almacenar en un DataSet, una vez almacenado se realizará un tratamiento a nuestro conjunto de datos con la finalidad de convertir en un Dataset limpio con el cual se pueda trabajar. Hasta esta fase se abarca la mayor parte del tiempo y esfuerzo para así tener un mejor resultado al momento de aplicar el modelado.

En el modelado se selecciona varios algoritmos para luego aplicar técnicas de modelado que sean pertinentes al problema, si las técnicas aplicadas no reaccionan como uno espera retornara a la fase de preparación de los datos con el fin de realizar un mejor tratamiento de los datos adaptados a las técnicas de modelado. En la etapa de evaluación se analiza la calidad del entrenamiento del modelo, es importante esta etapa para evaluar a fondo y revisar todo lo

ejecutado con el objetivo de obtener una decisión sobre los resultados del proceso de análisis de datos.

- Dataset de prueba

En esta fase de la metodología se trata de preparar los datos para adecuarlos a las técnicas de minería de datos que se van a emplear sobre ellos. Esto implica seleccionar el subconjunto de datos que se va a utilizar, limpiarlos para mejorar su calidad, añadir nuevos datos a partir de los existentes y darles el formato requerido por la herramienta de modelado.

Para que funcionen mejor muchos algoritmos de Machine Learning usados en Data Science, hay que normalizar las variables de entrada al algoritmo. Normalizar significa, en este caso, comprimir o extender los valores de la variable que estén en un rango definido. Sin embargo, una mala aplicación de la normalización, o una elección descuidada del método de normalización puede arruinar los datos y con ello el análisis.

- Modelado

En esta fase, se selecciona y aplica las técnicas de modelado que sean pertinentes al problema cuantas más sea mejor, y se calibran sus parámetros a valores óptimos. Típicamente hay varias técnicas para el mismo tipo de problema de minería de datos. Por lo tanto, casi siempre en cualquier proyecto se acaba volviendo a la fase de preparación de datos.

Una vez que se tiene normalizado nuestro Data se evalúa con varios algoritmos, para ver cómo se comportan cada uno con nuestros datos que tenemos. Algunos tal vez se acomoden a nuestras expectativas. Antes recordar que solo se aplicara los algoritmos, en la fase de evaluación se analizara con cual modelo se quedara para así finalizar el modelo.

- Evaluación

Comprender como un modelo se ajusta a los datos es muy importante para entender las causas de baja precisión en las predicciones. Un modelo va a estar sobre ajustado cuando vemos que se desempeña bien con los datos de entrenamiento, pero su precisión es notablemente más baja con los datos de evaluación, esto se debe a que el modelo ha memorizado los datos que ha visto y no pudo generalizar las reglas para predecir los datos que no ha visto. De aquí también la importancia de siempre contar con dos conjuntos de datos distintos, uno para entrenar el modelo y otro para evaluar su precisión; ya que, si se utiliza el mismo dataset para las dos tareas, no tendríamos forma de determinar como el modelo se comporta con datos que nunca ha visto

- Implementación

En esta fase se incluirá la identificación de los datos relevantes, la preparación de los datos para el entrenamiento del modelo, la selección del algoritmo de machine learning adecuado para el problema, el entrenamiento y el ajuste de los parámetros del modelo, la evaluación del rendimiento del modelo y la implementación del modelo para su uso.

- Fase de pruebas

- Documentar la pruebas y resultado

1.9 Programa de actividades, calendarización y presupuesto solicitado

No.	Actividad	Entregables	Periodo de realización	Monto solicitado
1	Construir un laboratorio con herramientas de virtualización, donde se instalara malware y particularmente ransomware para el analisis, identificación y estudio de los patrones de ataque	Estado del arte del malware, ransomware y medidas de seguridad de los sistemas operativos	Enero - Marzo	$ 32,000.00
2	Detección de tráfico malicioso y patrones de comportamiento y de propagación en redes tcp/ip. Preprocesamiento y limpieza de datasets. Investigar el uso de Machine Learning para detección de tráfico malicioso.	Datasets limpios, para comenzar analizar los distintos algoritmos de machine learning y seleccionar el mas adecuado a este tipo de patrones.	Marzo - Julio	$ 70,000.00

No.	Actividad	Entregables	Periodo de realización	Monto solicitado
3	Desarrollo de algoritmos para la detección temprana de ataques. Proponer y modelar un prototipo para elaborar un sistema de predicción, anti ransomware y envío de artículo a evento de divulgación	Algoritmo de detección de patrones de malware, que permita la anticipación del ataque, un artículo para evento de divulgación sobre los resultados logrados hasta ese momento.	Agosto - Octubre	$ 70,000.00
4	Implementar el modelo entrenado en prototipo para testear en una red pública y realización de pruebas del prototipo. Registro de Software e informe final del proyecto.	Registro ante indautor, informe del proyecto, asi como los resultados de las pruebas del prototipo en una red pública.	Noviembre - Diciembre	$ 28,000.00

1.10 Vinculación con el Sector Productivo

La metodología, así como el producto final, podría ser de utilidad a toda empresa de la región, e incluso a nivel nacional, para la seguridad en el uso de una plataforma de IoT.
Esta propuesta pretende apoyar en el monitoreo y control de la seguridad de las tecnologías utilizadas en domótica, así como en todo tipo de sistemas que estén basados en IoT.
Se pretende fomentar la cultura de la seguridad en soluciones de domótica para seguridad social, tanto en el sector educativo, científico como en el empresarial.
Al involucrar alumnos en el proyecto, éstos podrían participar en la elaboración o réplica de la metodología en otras empresas o instituciones, trasladando o transfiriendo la tecnología a nuevas entidades.
El producto de este proyecto se planea utilizar en las instalaciones del Instituto de Investigaciones en Ecosistemas y Sustentabilidad de la UNAM campus Morelia.

Con la empresa CTD NET (Consultoría en Transformación Digital, http://ctdint.com.mx/), es una organización enfocada a proveer soporte y consultoría a los clientes finales, mediante el desarrollo de una Cadena de Valor que convine lo mejor de las competencias de los diferentes integrantes de la Cadena de Valor, esto está reflejado en lo que somos, nuestra visión y misión.

1.11 Referencias

- 1. A, D. (2020). El aumento de gradiente es un conjunto de algoritmos de árboles de. Top Big Data. Retrieved December 13, 2022, from https://topbigdata.es/conjuntos-de-aumento-de-gradiente-basados-%E2%80%8B%E2%80%8Ben-histogramas-en-python/
- 2. Apd R. (2020). ¿Cuáles son los tipos de algoritmos del Machine Learning? APD España, constaldo de https://www.apd.es/algoritmos-del-machine-learning/
- 3 Consultek (2022) Recuperado en diciembre de 2022, de https://blog.conzultek.com/ciberseguridad/costo-financiero-ataques-ransomware.
- 4. Cortés, M. (2021). Cuatro técnicas para la detección temprana del Ransomware. CIO MX. https://cio.com.mx/cuatro-tecnicas-para-la-deteccion-temprana-del-Ransomware/
- 5. Cumbicus Pineda, O. M., Ludeña Preciado, P. V., & Neyra Romero, L. A. (2022). Técnicas de machine Learning para la detección de Ransomware: Revisión sistemática de Literatura. Journal of Science and Research, 7(3), 32–60. Recuperado a partir de https://revistas.utb.edu.ec/index.php/sr/article/view/2684
- 6. GitHub (2021). Consultado de chihebchebbi/Mastering-Machine-Learning-for-Penetration-Testing: Mastering Machine Learning for Penetration Testing, published by Packt. GitHub. Retrieved December 13, 2022, from https://github.com/chihebchebbi/Mastering-Machine-Learning-for-Penetration-Testing
- 7. ICIBE-CERT (2021). Ransomware: medidas de detección INCIBE-CERT. https://www.incibe-cert.es/blog/Ransomware-medidas-deteccion
- 8. Kaspersky (2021). Eliminación de Ransomware| Descifrar los datos: cómo eliminar el virus. www.kaspersky.es. https://www.kaspersky.es/resource-center/preemptive-safety/Ransomware-removal
- 9. Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E. (2015). Cutting the Gordian Knot: A Look Under the Hood of RansomwareAttacks. In: Almgren, M., Gulisano, V., Maggi, F. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science(), vol 9148. Springer, Cham. https://doi.org/10.1007/978-3-319-20550-2?
- 10. Machine Learning (2020). Consultado de https://www.ibm.com/mx-es/analytics/machine-learning

- 11. Orellana, R. F. J. (2018). Repositorio Institucional de la Universidad Politécnica Salesiana: Evaluación de tres ataques Ransomwareutilizando escenarios virtuales como plataforma experimental. Evaluación de Tres Ataques RansomwareUtilizando Escenarios Virtuales Como Plataforma Experimental. https://dspace.ups.edu.ec/handle/123456789/15919
- 12. Osorio-Sierra, A. F. (2020). Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. Proceso Para La Identificación, Clasificación y Control Del Comportamiento de Familias Ransomware. https://www.redalyc.org/journal/5537/553768212016/html/
- 13. PCFORMAT (2021). Imparable el Ransomware: Cuatro Técnicas para su Detección Temprana. https://pcformat.mx/2021/03/18/imparable-el-Ransomware-cuatro-tecnicas-para-su-deteccion-temprana/
- 14. Panda Security (2015). El reto de la detección temprana de ciberamenazas. Panda Security Mediacenter. Consultado en noviembre 2022 de https://www.pandasecurity.com/es/mediacenter/seguridad/reto-deteccion-temprana-ciberamenazas/
- 15. RansomwareEkans (2020). Prevención, detección y respuesta. INCIBE-CERT. https://www.incibe-cert.es/blog/Ransomware-ekans-prevencion-deteccion-y-respuesta
- 16. Trend Micro (2021). Cómo Prevenir el Ransomware.Consultado en enero 2022 de: https://www.trendmicro.com/es_mx/what-is/Ransomware/how-to-prevent.html

2. LUGAR(ES) EN DONDE SE VA A DESARROLLAR EL PROYECTO

En las instalaciones del Instituto Tecnológico de Morelia, en el laboratorio de seguridad y administración de la seguridad de la información del posgrado en sistemas computacionales, localizado en el departamento de sistemas y computación, edificio I, en el Tecnológico de Morelia, con domicilio: Av. Tecnológico #1500, Col. Lomas de Santiaguito, Morelia Michoacán, México, C.P. 58120

3. INFRAESTRUCTURA

Servidor HP Proliant, laptops con GPU, para análisis de machine learning, dispositivos móviles y prototipos de red virtualizados, así como computadoras ubicadas en el laboratorio de seguridad y administración de la información. En los cuales se desarrollarán las pruebas y el análisis de datos para el aprendizaje automático, además de la infraestructura que el instituto tecnológico de Morelia nos facilite, también se cuenta con equipo de computo facilitado por la unidad de TIC'S de la UNAM Morelia.

Profesor-Investigador Responsable
Nombre y Firma

<u>Se deberá proporcionar el informe final, en donde se incluya el cumplimiento de las metas comprometidas en función de los productos entregables. El cual será un criterio de evaluación para apoyos posteriores.</u>