UNIVERSIDAD DE COSTA RICA

FACULTAD DE INGENIERÍA

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN E INFORMÁTICA

SEGURIDAD DE SISTEMAS COMPUTACIONALES

Prof. Ricardo Villalón

Tarea/Investigación Corta

Análisis de seguridad de la Película: Algorithm: The Hacker Movie

Elaborado por:

B71146 Gabriel Bogantes Armijo

B78292 Rodrigo Antonio Vilchez Ulloa

B92911 Eduardo Fernández Baldizón

Investigación Preliminar

El uso de la tecnología ha crecido exponencialmente en paralelo a su desarrollo. Hoy en día, cualquier aparato tiene acceso al internet y con esto a sus vulnerabilidades. Las personas tienden a desconocer las potenciales amenazas a su información personal y sus datos. Como previamente se menciona, el uso del internet se ha vuelto algo del día a día para la mayoría de las personas, asimismo esto trae muchos beneficios y facilidades para la sociedad. También, es importante mencionar que se ha utilizado la tecnología para afrontar grandes retos como el Covid-19.

Según los datos de S21sec, desde el inicio de la pandemia la frecuencia en ataques a la seguridad de los sistemas computacionales ha aumentado en un 300%. Esto ya que la virtualidad ha pasado a ser la norma en muchos contextos (laborales, educativos y sociales). Gracias a esto, las empresas de ciberseguridad han puesto en práctica sus modelos para protección y mitigación de ataques.

Entre los pasos a seguir más importantes relacionados a la seguridad se encuentran:

- Identificar: Es importante tener indicadores para llevar un control de los incidentes encontrados. Además, el hecho de reportar diariamente mediante un *backlog* puede facilitar la fluidez del sistema en temas de seguridad.
- Proteger: Se recomienda el uso de la protección por capas además de la gestión de identidades y endpoint. Asimismo, el uso de la nube puede llegar a ser de gran uso gracias a su enorme elasticidad, visibilidad, protección y resistencia para los activos digitales.
- Detectar: Hacer *tuning* de las herramientas para la seguridad siempre y cuando se priorice de acuerdo al riesgo. También, es sugerido fomentar la vigilancia digital no cibernética y la redirección de costes hacia la protección.
- Responder: Se busca considerar el “Ciberseguro” como una forma de cubrir necesidades efectivamente en caso de incidentes. Por otro lado, para responder las situaciones se recomienda subcontratar un modelo pago por uso con un tercero que tenga acceso a un *snapshot* actualizado del sistema a proteger.

- Recuperar: Para la recuperación de datos e información se recomienda confiar en soluciones híbridas (onpremise-nube) para el almacenamiento que proporcionan la misma o mejor respuesta a los esquemas básicos.

Análisis de la película

En la película *Algorithm: The Hacker Movie*, el protagonista (LUser) es muy consciente de las vulnerabilidades de seguridad más comunes, a las que se exponen la mayoría de usuarios de dispositivos con conexión a internet. Él se aprovecha de estas vulnerabilidades para obtener información, tomando en cuenta que es un experto en el tema. De esta manera se contrasta a un experto en seguridad, con la mayoría de usuarios, que ni siquiera saben que sus dispositivos son vulnerables, y que por lo tanto no toman las medidas necesarias para aumentar su seguridad, y reducir el riesgo de ser víctimas de alguien como el protagonista. A través del protagonista, sus amigos, y el programa Shepherd, la película pone en escena una serie de prácticas de seguridad, así como vulnerabilidades y amenazas.

Informe de Seguridad

Datos personales y privacidad

La seguridad de los datos personales de los usuarios de internet está altamente relacionada con la forma como estos manejan su privacidad en internet. La mayoría de personas que utilizan redes sociales (por ejemplo), comparten mucha información personal, la cual puede ser recolectada y utilizada por personas con malas intenciones.

Existe la concepción equivocada de que si un usuario no hace nada incorrecto, no debe preocuparse por su privacidad, lo cual no es cierto ya que un mal manejo de la privacidad puede convertirse en una vulnerabilidad de seguridad. Una manera de minimizar este riesgo es ser cuidadoso con la información que se comparte y con cuáles usuarios se comparte.

Contraseñas

Las contraseñas, en el mundo digital, dan acceso a mucha información de los usuarios o de grupos más grandes como corporaciones. En muchas ocasiones esos datos son personales o sensibles y podrían perjudicar a cualquier persona en caso de que la información quede en manos equivocadas y maliciosas. Utilizar una contraseña es la primera forma de poner un obstáculo al acceso a esta información, es por eso que esta debe ser difícil de adivinar.

En la película se expone el hecho de que la mayoría de usuarios forman sus contraseñas con palabras o frases que involucren aspectos de su vida personal y que, en ocasiones, las personas sobreexponen su vida privada en redes, lo que da ventaja o información a aquellos que quieran obtener las contraseñas de los demás. También expone el hecho de que las contraseñas que dan acceso a sistemas con información sensible, como Shepherd, son conformadas con poca seriedad y que eventualmente no terminan protegiendo al sistema, como es el caso de la contraseña para obtener acceso a Shepherd.

Las recomendaciones actuales son: elaborar una contraseña que involucre caracteres en mayúsculas y minúsculas, con combinación de símbolos, números y preferiblemente con una longitud de caracteres mínima, que suele ser de ocho caracteres.

Rastreo

En la película, quizá la preocupación más grande de los personajes es el rastreo que pueden llegar a tener. En múltiples ocasiones los protagonistas toman las precauciones del caso y en algunos casos hasta lo mencionan explícitamente, tienen miedo a ser rastreados. Esto se ve presente en gran parte de la película pero explícitamente en tres escenas es donde más se ejemplifica:

1. En esta escena el personaje principal LUser explica que únicamente teniendo acceso a la red pública de una cafetería puede adueñarse de todos los datos de las personas conectadas a la misma. Básicamente “le pertenecen” todas estas personas, más específicamente su información personal.
2. No solo se puede rastrear personas mediante redes públicas de Wifi, sino también mediante su tarjeta SIM. LUser en múltiples ocasiones ejemplifica esta amenaza a su plan ya que se deshace de su tarjeta SIM en el teléfono periódicamente ya que esta es fácil de rastrear por parte de las autoridades o inclusive otros hackers.
3. En una escena curiosa, el personaje principal menciona que al conectarse a cierta red, su seguridad se encontraba “expuesta”. Entonces, decide forrar las paredes de un cuarto de papel aluminio. Él explica que funciona similar a un espejo ya que los datos pueden salir pero rebotan con el papel aluminio. Esto hace que evite que sea rastreado.

Personajes

LUser: Desde el principio se nos da a entender que es experto en obtener acceso a computadoras e información de otros usuarios. En una escena utiliza la técnica conocida como *phishing* para obtener acceso a una computadora (envía un correo electrónico con una imagen, que trae oculto un programa malicioso). El protagonista se describe a sí mismo como alguien que intenta tomar todas las medidas de seguridad posibles, incluso algunas un poco excesivas, como cambiar la tarjeta SIM de su teléfono constantemente.

- Objetivo de seguridad: no ser detectado, superando todas las medidas de seguridad de sus víctimas. Por esto mismo es que varias veces en la película menciona que se conecta a redes wifi de los vecinos, y que utiliza la computadora de la biblioteca, de manera que evita que sus actividades se puedan relacionar con sus propios dispositivos, y finalmente con su persona.

Hash: Amigo del protagonista. Por ser mejor para leer código, este le pide que le ayude a revisar Shepherd.

- Objetivo de seguridad: Al igual que LUser, su prioridad en teoría era no ser descubierto. Por esto es que le pregunta a LUser si apagó el wifi en su laptop, antes de correr el programa, considerando la posibilidad de ser rastreado a través del wifi. Igualmente comete un error, al no tomar en cuenta que podía ser grabado al hacer esto en público.
- Vulnerabilidad: Correr shepherd en público
- Amenaza: Que lo graben

Decimate: Un conocido del protagonista, que desde el principio de la película, da señas de ser más habilidoso que él. Más tarde se revela que trabaja para el gobierno. Este personaje se caracteriza por tomar muchas precauciones y ser cauteloso, prefería no arriesgarse ni involucrarse. Esto a pesar de que ya había hackeado al gobierno y tenía acceso a todo lo que buscaba LUser de antemano. Esta entidad (Shepherd) únicamente tenía una plataforma de ingreso básica y la contraseña era ridícula. Al final de la cinta, y como parte de su plan decide entregar a los otros personajes a la policía para “ayudarlos” posteriormente.

- Objetivo de seguridad: pasar desapercibido, no ser detectado y realizar sus “ataques” con mucha cautela.
- Vulnerabilidad: sus amigos/compañeros que lo pueden involucrar en acciones que lo descubran.

- Amenaza: que se descubra su identidad.

Shepherd: Después de descubrir la existencia de Shepherd y correr el programa, el protagonista descubre dos cosas: hace llamadas a un servidor, y presenta una pantalla de inicio de sesión. Luego, cuando Decimate le da la contraseña a LUser, nos damos cuenta que esta es bastante sencilla (11 caracteres), tomando en cuenta la importancia del programa. Igualmente, nos damos cuenta de una gran vulnerabilidad por parte de este programa, que es que solo utiliza la contraseña como un único método de autenticación. De un programa tan secreto y peligroso como este, se esperaría que utilizaran *Two Factor Authentication*, y/o algún factor biométrico, en combinación con el nombre de usuario y contraseña.

- Objetivo de seguridad: confidencialidad, que solo pueda ser accedido por personas con permiso.
- Vulnerabilidad: pocas medidas de autenticación
- Amenaza: que alguien no autorizado logre conseguir un nombre de usuario y contraseña, y obtenga acceso al sistema.

Computadora de Sam Novak: CTO del contratista gubernamental Emergent See, probablemente sea la computadora que dé acceso a mucha de la información confidencial de la compañía, gracias a la cual LUser es capaz de obtener inicialmente información acerca de Shepherd.

- Objetivo de seguridad: mantener la información y datos de la compañía seguros y lejos de terceros.
- Vulnerabilidad: el usuario (Sam Novak) desconoce de métodos de ataques con virus por el hecho de hacer click en links desconocidos (la imagen).
- Amenaza: acceso de terceros a la información que esté dentro de la computadora.

Red local de la casa de Mr. Dempsey: red a la cual LUser debe obtener acceso para poder controlar los dispositivos conectados a ella, para poder averiguar si la esposa del señor Dempsey le está siendo infiel, tal y como él le pide al momento de pagarle (a LUser) para obtener esa información.

- Objetivo de seguridad: mantener seguros los dispositivos conectados a la red.
- Vulnerabilidad: acceso a la señal desde fuera de la casa, dispositivos conectados a la red local sin el software actualizado, defectos de fábrica del router/módem.
- Amenaza: control total de los dispositivos por parte de un tercero.