Instituto Tecnológico de Santo Domingo

Carrera: Ingeniería de Software

Asignatura: Algoritmos Maliciosos

Profesor: Harold Marzán

Nombre: **Juan Avila**

Matrícula/ID: 1100378

Ensayo/Informe: Ransomware

Julio 2022

Contenido

1 Introducción

El ransomware es un tipo de ataque malicioso muy común hoy en día. Presenta un grave riesgo de seguridad para los ordenadores y datos de usuarios en todo el mundo, pues los hackers que hacen uso de este tipo de ataque han sabido aprovechar el desarrollo tecnológico en pos de crear virus computacionales que son fáciles de transmitir y difíciles de detectar. Por ello, el presente ensayo contiene una serie de definiciones acerca de este tipo de metodología de ataque o diseño de algoritmo malicioso, un breve repaso por su historia, y lo grave que puede llegar a ser este tipo de vulnerabilidad, mencionado casos mediáticamente relevantes de este tipo de malware.

Así mismo, pretendo que el presente documento plasme de forma clara los riesgos y daños que puede causar un ransomware, pues creo que es importante concientizar a las personas de que este tipo de infección existe, ya que solo de esta manera minimizaremos las víctimas de este tipo de ataques.

2 Desarrollo

Un ransomware es un tipo de virus computacional que bloquea archivos o secciones del sistema de la víctima, requiriendo típicamente un rescate para desbloquear los elementos afectados. Las variantes más actuales de ransomware basan su ataque en algoritmos de encriptado, que dejan al usuario sin acceso a sus preciados archivos o incluso el sistema, y esto es interesante para el atacante pues precisamente infectar de esta forma ha permitido que, al ser el ataque reversible, se pueda monetizar el virus. Teniendo esto en cuenta, no resulta extraña su popularidad en los últimos tiempos, ya que codear un ransomware sencillo no es una tarea tan complicada, y al dejar un rédito económico tan jugoso, personas poco éticas se ven tentadas a crear programas maliciosos de esta índole.

2.1 Inicios

El primer ransomware conocido data de 1989, cuando Joseph Popp distribuyó mediante floppy disks su virus PCCyborg, que iniciaba su ataque tras 90 boots de sistema. Como puede esperarse, su alcance fue limitado principalmente por su método de transmisión, que a su vez se encuentra íntimamente relacionado a la tecnología disponible en la época. Teniendo esto en cuenta, es evidente que la evolución tecnológica ha traído consigo nuevos canales de comunicación, como el correo electrónico, que permiten la proliferación de este tipo de malware de forma masiva, como en el caso del notable WannaCry, uno de los ransomware más notorios jamás creados.

2.2 Infecciones destacadas

Entre los ataques de ransomware más destacados se encuentran Ryuk, el cual provocó más de 60 millones de dólares en daños. Pedía hasta 300.000 mil dólares como rescate, y se proliferó mediante links y emails maliciosos. También esta SamSam, cuya infección masiva en Atlanta, el departamento de transporte de Colorado y el puerto de San Diego provocó pérdidas de 30 millones de dólares. También está el anteriormente mencionado WannaCry, que provocó 4 mil millones de dólares en pérdidas, y se transmitía con el uso de phishing en correo electrónico, llegando a afectar compañías de la talla de FedEx, Telefónica, Nissan y Renault.

Cabe destacar además el reciente ataque sufrido por Bandai Namco, uno de los publishers de videojuegos más grandes de la industria. El ataque se encuentra atribuido al grupo BlackCat (a veces también referenciado como ALPHV), y se menciona que han secuestrado archivos confidenciales de la empresa, y quizá incluso datos personales de los clientes de Bandai.

Lo mencionado en esta subsección debería dejar en claro que incluso tomando medidas de seguridad podemos ser víctimas de los ataques ransomware, así como que pueden llegar a causar daños devastadores.

2.3 Prevención

A nivel personal es quizá un poco más sencillo controlar la infección de este tipo de amenaza, pues solo con tener especial cuidado con las fuentes de donde obtenemos archivos, y no hacer click ni abrir enlaces/emails sospechosos, podemos eliminar el riesgo de infectarnos de ransomware en una gran cantidad. Sin embargo, las técnicas de ingeniería social aplicadas por los atacantes más hábiles suelen crear engaños muy convincentes, casos para los cuales hay que tener especial ojo en quien nos está contactando si se trata de un correo electrónico, comparar hash del archivo descargado con el original si es posible etc.

3 Conclusión

Los contenidos presentados en el ensayo dejan bien en claro lo que es un ransomware, y espero que entonces el lector pueda saber identificar de mejor manera infecciones de este tipo tras haber leído este ensayo. Además, considero que el texto logra crear ese sentimiento de preocupación necesario para crear concienciación que lleve a una menor tasa de infección, pues a través de la mención de casos importantes de ransomware, que piden grandes sumas monetarias como rescate o afectan empresas gigantes, creo que el lector se da cuenta de que esto no es un juego, y más vale ser precavidos al obtener archivos de internet.

Siguiendo con esta idea, creo que las prevenciones mencionadas si bien no gozan de elegantes tecnicismos, son suficientes para minimizar en la medida de lo posible el riesgo de infección. Esto ya que una buena educación en el tema, así como conocer los mecanismos de engaño comúnmente utilizados por los atacantes, permiten identificar rápidamente si se trata de un scam o no. Teniendo esto en cuenta, me gustaría cerrar el ensayo con la siguiente frase: “El sentido común nunca dejará de ser el mejor antivirus”.

4 Bibliografía

A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time. (2022, 4 abril). Digital Guardian. https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#:%7E:text=The%20First%20Ransomware%20Attack,-While%20ransomware%20has&text=According%20to%20Becker's%20Hospital%20Review,PC%20CYBORG%20advisory%20from%201989.

Stanton, R. (2022, 12 julio). *Bandai Namco reportedly hacked by ransomware group*. Pcgamer. Recuperado 16 de julio de 2022, de https://www.pcgamer.com/bandai-namco-reportedly-hacked-by-ransomware-group/