**Instituto Tecnológico de Santo Domingo**


**Nombres**

Desireé Larissa

**Apellidos**

Maríñez Jiménez

**ID**

1101374

**Asignatura**

ING202 - Algoritmos Maliciosos

**Profesor**

Harold Lawrence Marzan Mercado

**SANTO DOMINGO**

**REPÚBLICA DOMINICANA**

**Julio 2022**

**Proyecto Final [PF]**

**Virus informático Ransomware**

**Tabla de contenido**

## Introducción

A medida que pasa el tiempo, y el mundo progresa, nos adentramos todavía más en la Era de la Tecnología, donde nuevas herramientas salen a la luz cuyo propósito es el de traer beneficios y facilidad a la vida humana. Gracias a esto, han surgido numerosas aplicaciones y programas que han otorgado provecho al día a día del hombre. El mundo ha empezado a regirse por estas nuevas normas tecnológicas, por lo cual es pertinente adaptarse a ellas.

Sin embargo, el uso de estas aplicaciones no siempre provienen de ambientes inofensivos. El surgimiento de aplicaciones de contenido malicioso han circulado por la red del Internet desde comienzos de esta, pero no se habían tenido en cuenta sino hasta ahora, que tanto las tecnologías como las herramientas se han desarrollado a pasos gigantescos y novedosos. Hoy en día, cualquiera puede crear un algoritmo malintencionado, amenazando la seguridad del usuario.

Como usuarios de Internet, es cierto que debemos velar por nuestra propia seguridad, pero no siempre es tarea sencilla. Los virus informáticos suelen esconderse, pasando desapercibido de los programas antivirus que uno tenga instalado en su dispositivo. Por ese motivo, solo se debe confiar en fuentes confirmadas en ser seguras, e ignorar cualquier otro tipo de archivos o hipervínculo que carezca de dichas propiedades. Si se quiere acceder a estas, uno debe ser responsable de las consecuencias que sucedan, así como evitar infectar a otros usuarios.

De entre todos los tipos de algoritmos maliciosos que existe, la presente se enfocará en el virus informático de tipo Ransomware, explicando un poco sobre lo qué es uno, su historia, los casos más conocidos, para luego finalizar hablando sobre el ransomware que se

programó, incluyendo una explicación detallada del código de este. Cabe destacar que la misma se hizo con motivos de puntuación, y que no se espera su lanzamiento a la Internet. Su objetivo es abrir el camino a la encriptación de archivos, y su uso debe quedarse en la total individualidad.

## Desarrollo

### Descripción

Antes de comenzar a hablar de la historia de los ransomware, y cómo han evolucionado frente a las nuevas herramientas de programación —y las nuevas barreras de seguridad— del Internet, tenemos que explicar qué es un ransomware.

De la unión de los términos “ransom”, o rescate, y “ware”, de software, significa literalmente software de rescate, el cual se trata de la restricción momentánea o permanente, dependiendo del atacante, de los archivos de un dispositivo, el cual se le sucede un rescate, normalmente de pago, para recuperarlos. Este, como se puede ver, es familia de los malware, los cuales son softwares de contenido malicioso. A pesar de que algunos ransomware puedan ser inofensivos, como se explicará más adelante, en su mayoría resultan ser malignos para los usuarios infectados, debido a que el tipo de ransomware más programado son los de cifrado.

Los ransomware se dividen en tres tipos, abarcando desde los inofensivos hasta los perjudiciales. Los primeros en esta lista son los Scareware; los cuales se tratan de aquellos que aparecen como publicidad o anuncios falsos, pudiendo solamente irse a través del pago, como todos los ransomware. En segundo lugar, están los bloqueadores de pantallas, que como su nombre indica, bloquean las pantallas de los dispositivos infectados, normalmente

con mensajes alarmantes para que el usuario pague la recompensa rápido. Los últimos, pero no menos importantes —incluso se tratan de los ransomware más peligrosos— son los de cifrado, los cuales encriptan los datos de los archivos a los que infecta, pudiendo solamente recuperarse con una llave. Ningún software puede acudir a la ayuda de uno si le sucede este caso.

**Historia**

Los comienzos del ransomware comenzaron con el primer ransomware conocido, el cual fue PC Cyborg para el final de los años 80. Este cifraba todos los archivos que se encontraban dentro del directorio C:, exigiendo al usuario víctima la suma de 189 dólares para renovar la licencia. Como fue el primero de su tipo, este era fácil de descifrar, por lo que los informáticos lograban superar sus defensas y desencriptar los archivos ellos mismos.

Los siguientes años fueron los más evolutivos para los ransomware, siendo el 2004 donde comenzaron las verdadera amenazas de estos, cuando GpCode se desarrolló y causó un cifrado RSA débil para secuestrar información a cambio de dinero. Para el 2007, WinLock creó una nueva era de ransomware, al estos bloquear los dispositivos de los usuarios y mostrar imágenes de contenido sexual, exigiendo también un pago como rescate.

En el 2012, surgió la familia Reveton de programas de ransomware, creando los de tipo cuerpo policial falso. A las víctimas se les impedía el uso de sus dispositivos, y aparecía una página, presuntamente oficial, de los cuerpos policiales más importantes, tales como el FBI y la Interpol. Este denunciaba que la víctima había cometido actividades ilícitas, y debía pagar una multa para volver a utilizar sus ordenadores. A primera vista, asustaba a los

usuarios, quienes creían que se trataba de una asunto real, y cuestionando sus hechos les pagaban la recompensa.

Para finales del 2018, apareció Ryuk dentro de los ransomware, liderando varios ataques contra publicaciones de noticias estadounidenses. Los sistemas que fueron atacados fueron infectados con Emotet o Trickbot, dos troyanos ladrones de información. Ryuk operaba al infectar el sistema y marcarlo como un objetivo para el ransomware Emotet/TrickBot.

**Ransomwares Conocidos**

1. **CovidLock - 2020:** ocurriendo en plena pandemia por el coronavirus Covid-19, los piratas informáticos decidieron aprovechar las constantes actividades por el Internet de los usuarios que se quedaron en sus casas para atacar sus servidores y encriptar sus archivos a través de ficheros que hablaban sobre la enfermedad. Este encriptaba los archivos de los dispositivos Android, negándole el acceso a los usuarios, requiriendo un rescate de 100 dólares por dispositivo.

2. **Emotet - 2018:** fue calificado como el malware más peligroso y devastador, debido a que robaba información financiera, como los registros bancarios y las criptomonedas de los usuarios infectados, propagándose a través de correos electrónicos en forma de correo basura.

3. **WannaCry - 2017:** uno de los ransomwares más conocidos, este posee la peculiaridad de que se duplica sin modificar ningún documento y sin afectar al sector

de inicio una vez que se infiltra en un sistema, propagándose por medio de estafas por correo electrónico.

**Descripción y explicación del virus**

El virus que se creó como proyecto final fue un ransomware de tipo cifrado, programado en el lenguaje de programación Python, y el entorno donde se ejecuta es en los sistemas operativos de Microsoft Windows. Este utiliza varias librerías de Python, siendo estas cryptography.fernet, rsa —siendo estas dos las dos principales—, time, os y Courier; este último usándose para enviar llaves a un correo determinado.

Lo que hace este ransomware es encriptar los archivos que se encuentren del directorio que se pase, utilizando una llave simétrica que luego es encriptada por una asimétrica pública. Solamente se podrá desencriptar la llave con la que se encriptaron los archivos con una llave privada.

Sin embargo, al querer desencriptarlos, tendrá que pagar la cantidad que se le especifica, la cual deberá ser transferida a una billetera de Bitcoin. Finalizado este proceso, el atacante le suministrará una palabra clave para ingresar para que el proceso de desencriptar comience. Si el usuario no ingresa la palabra que es, sus archivos se eliminarán.

Así mismo, en el caso de que el usuario no quiera desencriptar sus archivos, estos también serán eliminados. La llave pública se agrega como archivo KEY en los ficheros del usuario, y se envía la llave privada al atacante a través de la mensajería de Courier.

Algo a tener en cuenta es que este ransomware utiliza tanto llaves asimétricas como simétricas. Se crea una llave simétrica, la cual es la que encripta los archivos, y está a su vez es encriptada por la llave pública, pudiendo solamente desencriptarse con la llave privada.

## Conclusión

Los virus informáticos de tipo ransomware, a pesar de presentar versiones inofensivas, causan grandes estragos a gran escala. Su ejecución y distribución aumentan las fallas de seguridad en la Internet, las cuales son bastantes en consideración.

Como usuario del Internet, nuestro deber es asegurarnos de evitar la expansión de estos, tomando medidas preventivas contra ransomwares y documentarnos sobre estos. Acceder a sitios asegurados y confiables, y utilizar programas antivirus en los dispositivos aumentan las posibilidades de evitar infectarse.

## Bibliografía

Kaspersky. (2022, 1 julio). *El ransomware: qué es, cómo se lo evita, cómo se elimina*. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/ransomware

Malwarebytes. (2019, 25 noviembre). *Ransomware: qué es y cómo eliminarlo*. https://es.malwarebytes.com/ransomware/#:%7E:text=El%20ransomware%20es%20una%20forma,an%C3%B3nimo%20para%20restaurar%20el%20acceso

Panduru, D. (2022, 23 febrero). *10 ejemplos de malware: Los más famosos y devastadores casos de la historia*. ATTACK Simulator.

https://attacksimulator.es/blog/10-ejemplos-de-malware-los-mas-famosos-y-devastadores-casos-de-la-historia/