Revista de I+D TECNOLÓGICO
Portal de revistas: http://revistas.utp.ac.pa

Revisión sobre propagación de *ransomware* en sistemas operativos Windows

Review on propagation of ransomware in windows operating systems

José Moreno[1*], Carlos Rodriguez[1], Isabel Leguias[2]

[1]*Facultad de Ingeniería en Sistemas Computacionales, Universidad Tecnológica de Panamá, Panamá*

[2]*Grupo de Investigación en alud Electrónica y Supercomputación, Universidad Tecnológica de Panamá, Panamá*

***Autor de correspondencia**: jose.moreno3@utp.ac.pa

RESUMEN- El *ransomware* es una de las nuevas amenazas a las que estamos expuestos, enfocándose principalmente en los sistemas operativos de escritorio Windows, sin dejar de lado a los dispositivos móviles y microcomputadores que también están expuestos de igual manera al robo, fuga de información y secuestro de los datos, poniendo en riesgo la seguridad personal. El *ransomware* ha evolucionado a través de la implementación de técnicas criptográficas que utilizan algoritmos de cifrado asimétrico. Además, utiliza la ingeniería social como principal método de propagación de *malware*, en este trabajo se presenta el análisis del *ransomware hidden tear*, los lineamientos de detección y prevención, además de buenas prácticas y recomendaciones.

Palabras claves– *Ransomware, Windows, ataques, ingeniería social, cibercrimen, cifrado, descifrado, fraude, extorsión.*

ABSTRACT– Ransomware is one of the new threats to which we are exposed, focusing mainly on Windows operating systems, without neglecting mobile devices and microcomputers that are also exposed in the same way to theft, Information and data hijacking, putting personal security at risk. Ransomware has evolved through the implementation of cryptographic techniques that use asymmetric encryption algorithms. In addition, it uses social engineering as the main method of propagating malware, in this paper is presented ransomware hidden tear analysis, detection and prevention guidelines, as well as best practices and recommendations.

Keywords– *Ransomware, Windows, attacks, social engineering, cybercrime, encrypt, decrypt, fraud, extortion.*

1. Introducción

El *ransomware* es un tipo de *malware* que impide el acceso a la información, cifrando los archivos con algoritmos criptográficos simétricos o asimétricos, solicitando una suma de dinero para recuperar la información cifrada, comúnmente utilizando algoritmo simétrico AES (Advanced Encryption Standard) de 256 bits.

AES o Estándar Avanzado de Seguridad es un esquema de cifrado por bloques adoptado como estándar de cifrado por el gobierno de los Estados Unidos [1].

El secuestro de los datos o pérdida de información pueden causar una falla de seguridad informática, generando problemas en la integridad y disponibilidad de los datos que pueden implicar sustanciales perjuicios a cualquier organización. Ejemplo de victimas del *ransomware* son: las PYMES, hospitales, usuarios comunes, que no cuentan con políticas definidas de seguridad informática, plan de recuperación de desastres, plan de pérdida de datos.

El presente artículo tiene como finalidad explicar el funcionamiento de los *ransomware* en los sistemas operativos Windows y Linux, adicionalmente trataremos la historia o inicios del *ransomware*, definición, métodos de propagación, métodos de detección, discusión y conclusión.

2. Trabajos relacionados

Los *ransomware* se clasifican de diversas formas: por su comportamiento, el cual bloquea el acceso al sistema operativo, a su vez cifra archivos y datos del sistema operativo infectado. Igualmente, según [3] su tecnología podemos clasificarlos de la siguiente manera:

- FAKEAV son *malware* que engañan a los usuarios a comprar falsos *antimalware*, por medio de mensajes falsos con resultados falsos.
- *Ransomware* de compresión, los cuales comprimen archivos de ciertos formatos como .DOC, .EXE, .DLL, .PPT, dejando una nota de la extorsión con la solicitud del pago.

Citación: J. Moreno, C. Rodriguez y I. Leguias, "Revisión sobre propagación de ransomware en sistemas operativos Windows", *Revista de I+D Tecnológico*, vol. 16, no. 1, pp. (39-45), 2020.
Tipo de artículo: Original. **Recibido:** 26 marzo de 2019. **Recibido con correcciones:** 26 de marzo de 2019. **Aceptado:** 2 diciembre de 2019
DOI.

- SMS *Ransomware* los cuales envían notificaciones continuamente mientras el usuario no efectué el pago.
- *Ransomware* cuyo objetivo es infectar el MBR de un sistema vulnerable el cual no permite que el sistema operativo se inicie y mostrando una notificación de la extorsión.
- Police *Ransomware* personifica las autoridades de policía local mostrando notificaciones y engañando a la víctima con avisos de actividades ilícitas [3].

La distribución de los *ransomware* ha cambiado desde sus inicios donde utilizaban *floppy disk* para su propagación, en la actualidad se distribuyen por medio de publicidad engañosa, a través de unidades de almacenamiento removible como *pendrives*, macros en documentos de textos, presentaciones, hojas de cálculos, ejecutables, entro otros. Estas nuevas técnicas de distribución han permitido la evolución de los métodos de pago de la extorsión, incluyendo pago por medio de paypal, tarjetas de débitos de diversos lugares (tarjetas de regalos de amazon, google play, etc.), pago con criptomonedas [4].

3. El *ransomware* en sus inicios

El *ransomware* se define como un: "Tipo de *malware*, que extorsiona a sus víctimas, cifrando los archivos"[5].

La historia del *ransomware* data de finales de los años 80 e inicios de los 90 con el primer *ransomware* denominado AIDS trojan, distribuido en un *floppy disk*, durante una conferencia internacional sobre SIDA, el cual cifraba el nombre de los archivos solamente, solicitando un pago a una cuenta bancaria localizada en Panamá [6].

Los algoritmos criptográficos utilizados para cifrar el acceso a los datos eran algoritmos simétricos, por lo que en sus inicios este tipo de cifrado no era rentable para los ciberdelincuentes, debido a su facilidad para ser descifrado; hasta que en el año 2005 en Rusia comenzaron a utilizar los algoritmos asimétricos. En 2012, los investigadores detectan una nueva variante de *ransomware* denominada Crypto Locker, el cual trataremos a continuación. [7].

4. ¿Cómo funciona?

Uno de los *ransomware* más conocidos es el Crypto Locker, el cual basa su cifrado en un algoritmo criptográfico asimétrico RSA (Rivest-Shamir-Adleman) para el cifrado de archivos y bloqueo de sistemas. Las últimas variantes de *ransomware* aplican una combinación de cifrado AES + Cifrado RSA [7], como se muestra en la figura 1.

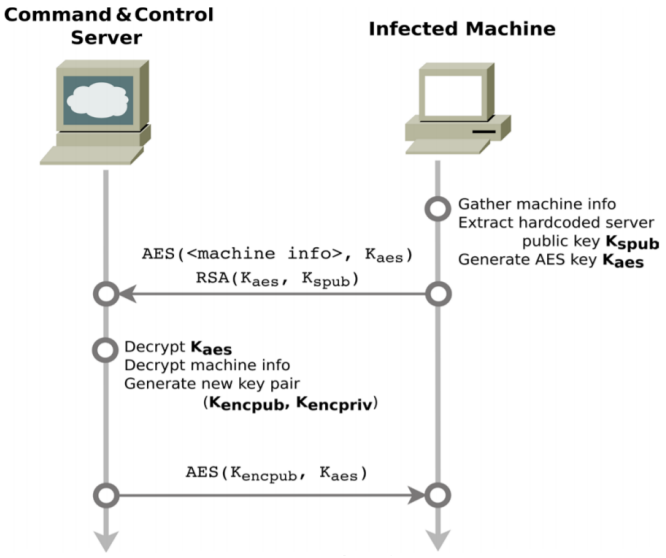

Figura 1. Funcionamiento Crypto Locker cifrado AES + RSA [7].

4.1 Análisis de *ransomware hidden tear*

Hidden tear es un *ransomware* de código abierto utilizado principalmente para propósito educativos, en agosto de 2015 fue liberado por su creador el experto en seguridad informática Utku Sen y se encuentra en el portal de *github*. Este *ramsomware* puede ejecutarse de dos formas: el modo *online*, que es el método que utilizan los actuales *ramsomware* y el método *offline*, el cual es demostrativo. [8] Su funcionamiento para el modo online es el siguiente:

Utiliza el algoritmo simétrico AES para cifrar los archivos.

- Envía la llave de cifrado a un servidor.
- Los archivos cifrados pueden ser descifrados con la llave para descifrarlos.
- Genera un archivo de texto con un mensaje en el Escritorio de la pc de la víctima.
- No es detectado por los antivirus.

4.2 Pasos para el análisis del *ransomware*

- Se prepara una máquina virtual con Windows 7.
- Se descarga el *malware* a la máquina virtual con Windows 7 desde el repositorio de *github*.
- Se crea una cuenta en el *hosting* gratuito *000webhost*, como se muestra en la figura 2.
- Se crea un sitio web falso para funcionar como mascara donde llegarán los datos del sistema

operativo infectado, como vemos en la figura 3 y figura 4.

- Se descarga Mono y Xamarin Studio, herramientas con la que se compila el código fuente del *hidden tear*. Como vemos en la figura 5,6 y 7 respetivamente.
- Desarrollo de la prueba de concepto, como se aprecia en las figuras 8,9,10 y 11.

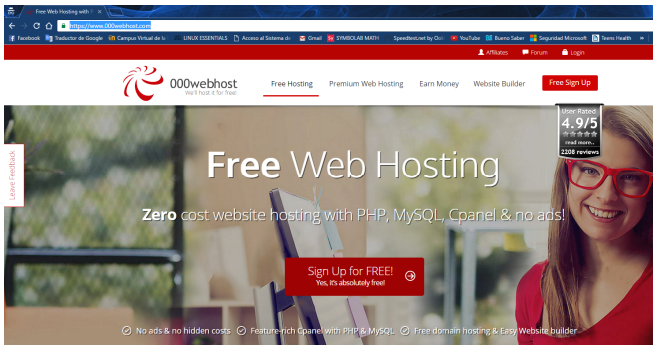

Figura 2. Creación cuenta en *000webhost*: Fuente Propia.

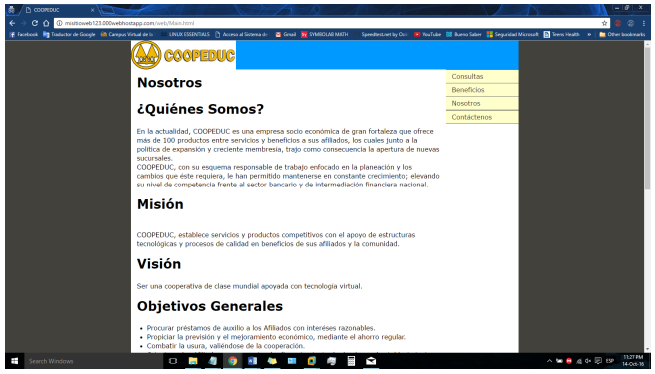

Figura 3. Sitio público utilizado para recibir las llaves generadas por el *ransomware*: Fuente Propia.

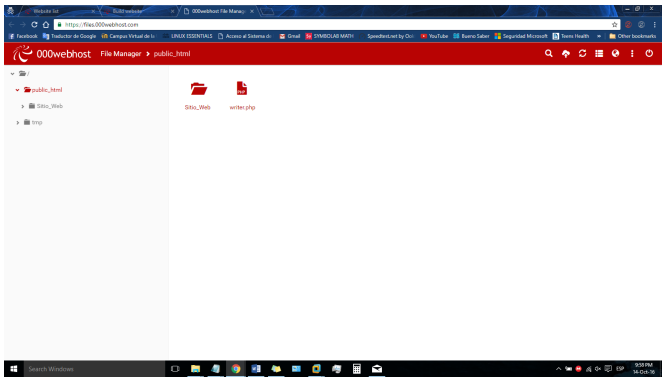

Figura 4. Creamos un archivo *writer.php* que nos permitirá guardar los datos enviados por el *ransomware* a nuestro servidor: Fuente Propia.

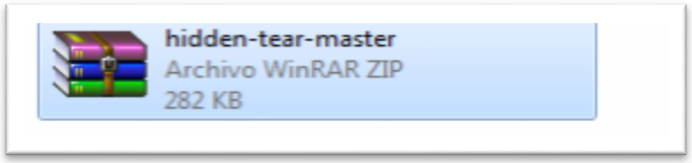

Figura 5. Código fuente del *ransomware* que vamos a compilar: Fuente Propia.

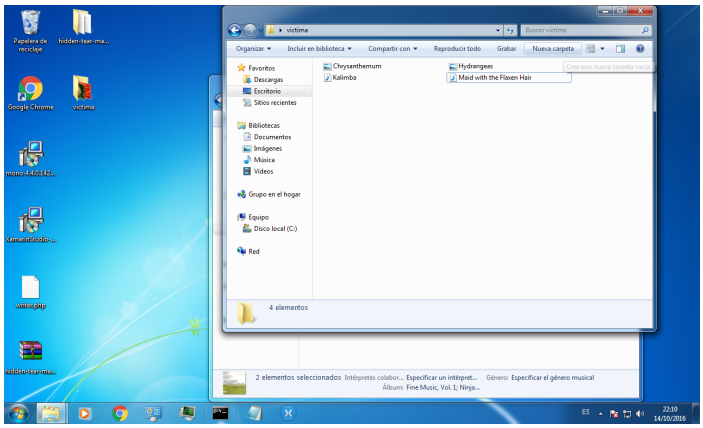

Figura 6. Directorio víctima donde vamos a encontrar unas imágenes y archivos para la prueba: Fuente Propia.

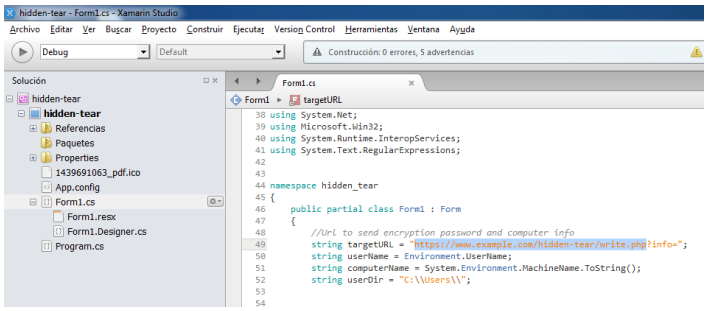

Figura 7. Cambiamos los datos de configuración por los datos de nuestro servidor web donde llegará la llave del *ransomware*: Fuente Propia.

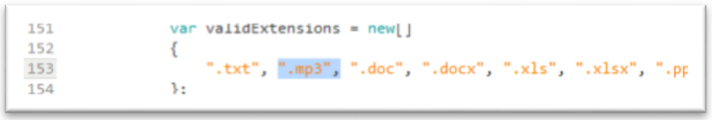

Figura 8. Definimos que extensiones de archivos queremos cifrar con el *ransomware hidden tear*: Fuente Propia.

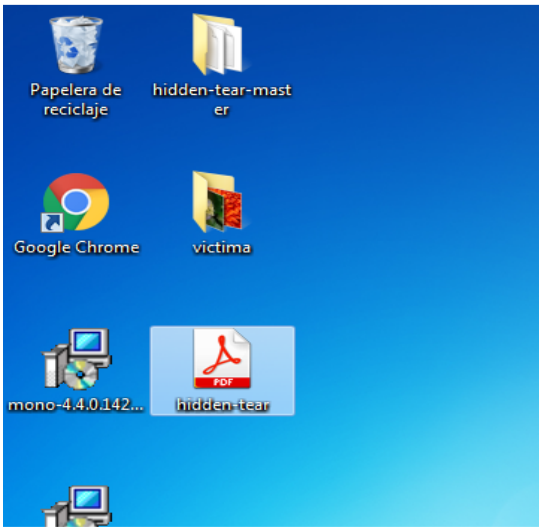

Figura 9. Luego de compilar se genera el ejecutable del *malware* aparentemente un archivo pdf: Fuente Propia.

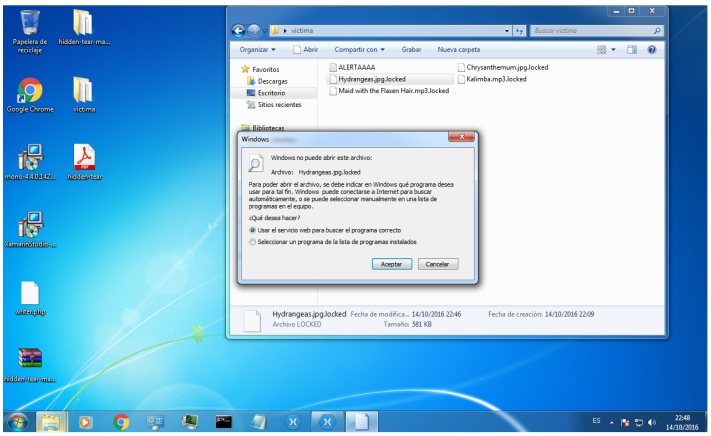

Figura 10. Se genera un mensaje de advertencia informando que hemos sido víctima de un *ransomware*: Fuente Propia**.**

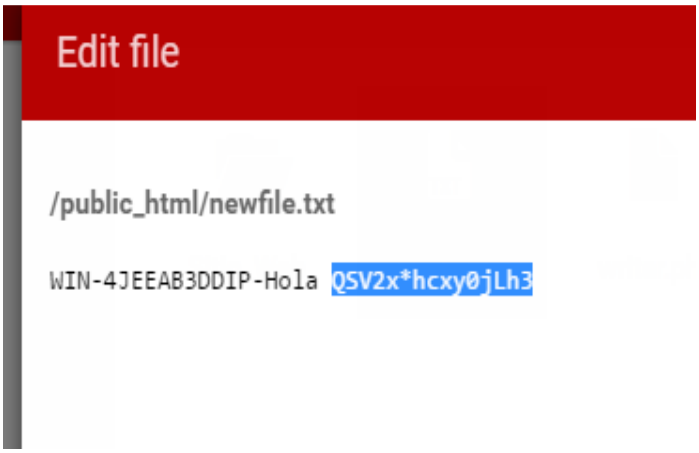

Figura 11. En el servidor web encontraremos un archivo con la llave para descifrar los archivos de la víctima: Fuente Propia.

5. Métodos de propagación

El método que utilizan los ciberdelincuentes para la propagación de *ransomware* es la ingeniería social; debido a que la víctima comúnmente es el eslabón más débil de la cadena, la mayoría de los *malware* por lo general provienen de correos de contactos que han sido infectados previamente con algún tipo de *malware*.

Los métodos de propagación son los siguientes [1]:

- **Redirección de tráfico**: método que engaña al usuario con publicidad engañosa redirigiendo al usuario a otro sitio donde se encuentra el *malware*. Procede de sitios pornográficos hacia sitios de juegos gratuitos o de aplicaciones gratuitas. Al descargar el *freeware* e instalarlo, se instala el *malware*, el cual explota las vulnerabilidades en el sistema operativo del usuario bloqueando el acceso al sistema y los archivos del usuario.
- **Adjuntos de correos**: este método utiliza los correos de fuentes confiables que han sido comprometidos, también pueden ser correos similares a la de fuentes confiables como facturas de servicios básicos, pago de impuestos, notificaciones legales o de la empresa. Dichos correos contienen archivos adjuntos o incitan al usuario a abrir un enlace a un sitio web que contiene el *ransomware*. Cuando el usuario abre el enlace o el archivo adjunto se propaga el *malware* en el sistema.
- ***Botnets***: Son distribuidos por medio de los sistemas comprometidos. Estos sistemas comprometidos proceden a descargar el *malware* en un segundo plano. Normalmente utilizando programas de descarga legítima que no contienen *malware*, sino que descargan el código malicioso en un paso posterior, utilizando un *crack* o *keygen*.
- **Ingeniería social**: es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos [9].
- **RAS (*Ransomware* as A *Service*, *Ransomware* como servicio)**: ataques de malware ofrecidos mediante servicios pagados, se ejecutan como un servicio de negocio en la nube.

En [10] describen otros métodos o técnicas de propagación que existen tales como:

- Sistema de distribución de tráfico.
- MALVERTISEMENT (publicidad maliciosa).
- Spam email (correo basura).

6. Detección y prevención

El *ransomware* utiliza algoritmos de cifrado asimétrico, que requiere una llave privada, que solo

conoce el cibercriminal [7] y como no hay solución para descifrar los archivos cifrados se toman ciertas medidas de prevención:

- Existen herramientas *antiransomware* con la capacidad de informar sobre algunos *malware* sospechosos. Se recomienda la instalación de antivirus confiables y de *firewall*, que puedan filtrar la amenaza antes que llegue a los archivos del sistema [7].
- Evitar hacer *click* sobre enlaces que vienen en correo electrónico. El *ransomware* ataca a través de estos enlaces, cuyos correos son considerados de correo de Phishing o Spam, los cuales son utilizados para robar dinero al usuario.
- Asegurarse de que, si se hace *click* sobre alguna fuente, esta sea de una fuente confiable.
- Como buena práctica de seguridad se debe realizar copias de seguridad o *backups* en intervalos regulares definidos por el usuario del equipo o el administrador del servidor, debido a que existe un *ransomware* capaz de borrar los sectores de arranque del disco duro, etc. Con lo cual los usuarios quedan despojados de acceso al sistema.

Existen también formas de detección que son herramientas de *software* capaz de emitir alertas o reportar comportamientos, como son el *antiransomware tool*, el cual detecta el *ramsonware* en etapas tempranas, antes que este afecte los archivos. Posee varias características útiles como son:

- Usa heurísticas e IA para realizar análisis.
- Es capaz de detectar ataques de día cero.
- Detecta la mayoría de las variantes de *ransomware*.
- Cada *ransomware* detectado es bloqueado.

Con esta utilidad como herramienta de detección se añade muchas ventajas en la protección contra el **ransomware** lo que permite realizar las correcciones a nuestro sistema/red [7].

7. Herramientas

Como primer paso para identificar el tipo de *ransomware* es utilizar alguna herramienta útil para la detección de este tipo de *malware*. A continuación, estas herramientas:

Virustotal [11]: Es un sitio *web online* que permite analizar las muestras del *ransomware* para identificar con cual variante del *malware* hemos sido infectados. Además, analiza enlaces web de dudosa procedencia, acortadores de url (bitly, goo.gl, tiny url, etc.) usados comúnmente para la descarga de archivos maliciosos.

Se sube una muestra del mensaje o archivo infectado en la siguiente url: www.virustotal.com. Si deseamos analizar una dirección web usamos la opción URL de la herramienta, como se muestra en la figura 12.

Figura 12. Herramienta virus total *online*: Fuente Propia.

Luego de finalizado el análisis de la muestra nos debe mostrar un resultado con la posible variante del *ransomware* con que hemos sido infectados, como se muestra en la figura 13.

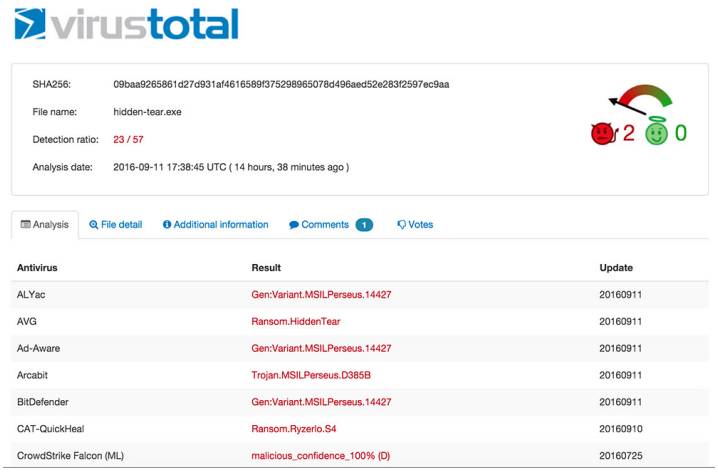

Figura 13. Análisis de un archivo infectado con *ransomware*: Fuente Propia.

Nodistribute [12]: Es una aplicación *online* que permite el análisis de archivos infectados con algún tipo de *ransomware* donde indica el posible *malware* o variante del *malware* usado para secuestrar el sistema operativo de la víctima.

De igual manera la muestra o la *url* sospechosa se sube en la dirección: www.nodistribute.com para su análisis, como se muestra en la figura 14.

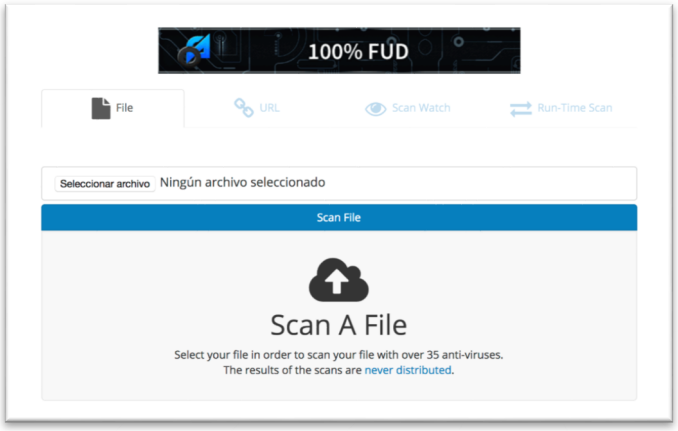

Figura 14. Página de inicio de nodistribute: Fuente Propia.

Nomoreransom: Herramienta de detección y análisis de muestras de archivos infectados, sin embargo, esta nos proporciona indicios de las posibles soluciones para descifrar la data secuestrada por el *ransomware* [13].

A través del navegador de su preferencia introduce la dirección www.nomoreransom.org donde se sube la muestra del archivo infectado o el mensaje o dirección la cual indica el *ransomware*, como se muestra en la figura 15.

Figura 15. Herramienta *online* Nomoreransom.

Telecrypt decryptor: Está herramienta permite descifrar archivos cifrados con *ransomware* Telecrypt. Este *ransomware* utiliza el protocolo de comunicación de la aplicación *Telegram* para enviar la llave de descifrado y mantenerse en contacto con la víctima. La herramienta funciona si se cumple con las siguientes condiciones:

- Si el usuario afectado cuenta en su sistema operativo con el programa .NET 4.0 en adelante (todos los sistemas operativos de Windows lo traen desde Windows xp).
- Si la víctima tiene al menos uno de los archivos infectados en su forma no descifrada.
- El usuario debe ejecutar el programa como administrador del sistema operativo. [14].

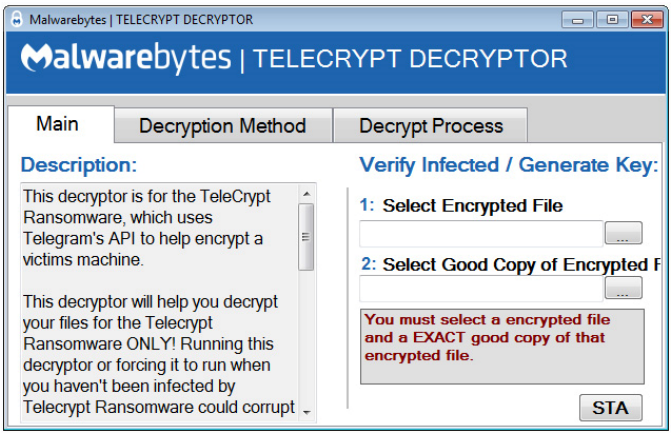

Figura 16. www.helpnetsecurity.com [15].

8. Discusión

Los resultados de la prueba realizada muestran que el *ransomware* utiliza los métodos criptográficos de algoritmo simétricos AES de 256 bits para secuestrar la información de las computadoras de sus víctimas. Este algoritmo es de los más utilizados debido al bajo consumo de recursos y la rapidez al momento del cifrado y descifrado.

Diferentes investigaciones han llegado a la conclusión de que el método de propagación más utilizado es la ingeniería social. Muchas personas ingenuamente caen víctimas de esta técnica que pueden ser: correos electrónicos, archivos maliciosos, ejecutables disfrazados de otros tipos de archivos como imágenes, entre otros.

9. Conclusiones

El *ransomware* se ha incrementado en los últimos años como un negocio rentable para los ciberdelincuentes, debido al desconocimiento de los usuarios del peligro que conlleva abrir archivos y enlaces de fuentes conocidas independientemente de la red social utilizada ya sea *facebook*, *twitter*, *instagram*, *snapchat*, aplicaciones de mensajería instantánea como *whatsapp* o servicios de red como e-mail.

De la investigación concluimos que el método de propagación más utilizado es la ingeniería social, debido a factores inherentemente humanos tales como la confianza, curiosidad, entre otros.

Para finalizar, cabe mencionar que uno de los métodos de prevención contra el *ransomware* es contar con copias de seguridad dado que en la mayoría de los casos no se suele recuperar la información, por lo que es imprescindible contar con un respaldo de la información crítica.

10. Referencias

[1] C. C. Lu and S. Y. Tseng, "Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter," Proc. Int. Conf. Appl. Syst. Archit. Process., vol. 2002–Janua, pp. 277–285, 2002.

[2] A. Bhardwaj, V. Avasthi, H. Sastry, and G. V. B. Subrahmanyam, "Ransomware Digital Extortion: A Rising New Age Threat," Indian J. Sci. Technol., 2016.

[3] P. B. Pathak and Y. M. Nanded, "A Dangerous Trend of Cybercrime: Ransomware Growing Challenge," vol. 5, no. 2, 2016.

[4] D. F. Sittig and H. Singh, "A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks," Appl Clin Inf., vol. 7, no. 7, pp. 624–632, 2016.

[5] A. Gazet, "Comparative analysis of various ransomware virii," J. Comput. Virol., vol. 6, no. 1, pp. 77–90, 2010.

[6] H. Orman, "Evil Offspring - Ransomware and Crypto Technology," IEEE Internet Comput., vol. 20, no. 5, pp. 89–94, 2016.

[7] D. Kansagra, M. Kumhar, and D. Jha, "Ransomware: A Threat to Cyber security," Comput. Sci. Electron. Journals, vol. 7, no. 1, pp. 224–227, 2015.

[8] H. A. Martínez-García, M. M. Medina, and L. B. C. Us, "Recuperación de datos cifrados mediante control de versiones en nube, una alternativa contra el ransomware: Caso de estudio," Adv. Eng. Innov., vol. 1, no. 1, pp. 21–31, 2017.

[9] I. Kotenko, M. Stepashkin, and E. Doynikova, "Security analysis of information systems taking into account social engineering attacks," Proc. - 19th Int. Euromicro Conf. Parallel, Distrib. Network-Based Process. PDP 2011, pp. 611–618, 2011.

[10] H. U. Salvi and R. V. Kerkar, "Ransomware: A Cyber Extortion," Asian J. Converg. Technol., vol. 2, no. 3, pp. 1–6, 2015.

[11] (2017) Virustotal [Online]. Disponible en: https://www.virustotal.com

[12] (2017) NoDistribute [Online]. Disponible en: https://www.virustotal.com

[13] (2016) Nomoreransom. [Online]. Disponible en: https://www https://www.nomoreransom.org/ /

[14] (2016) Helpnetsecuirty. [Online]. Disponible en: https://www.helpnetsecurity.com/2016/11/23/telecrypt-decryptor-ransomware/