MONTAJE DE UN AMBIENTE CONTROLADO UTILIZANDO RANSOMWARE Y APLICANDO HERRAMIENTAS DE SEGURIDAD QUE PERMITAN DETECTAR LAS VULNERABILIDADES DE LA INFORMACIÓN IMPLICADA.

ESTEBAN DAVID MOLANO ARTUNDUAGA

EDGAR VERNAZA ARBOLEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2021

MONTAJE DE UN AMBIENTE CONTROLADO UTILIZANDO RANSOMWARE Y APLICANDO HERRAMIENTAS DE SEGURIDAD QUE PERMITAN DETECTAR LAS VULNERABILIDADES DE LA INFORMACIÓN IMPLICADA.

ESTEBAN DAVID MOLANO ARTUNDUAGA

EDGAR VERNAZA ARBOLEDA

Proyecto para optar por el título de:

Especialista en seguridad informática

Director

Alexander Larrahondo Núñez

Máster en Seguridad de las Tecnologías de la Información y de las Comunicaciones

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2021

CONTENIDO

LISTA DE IMAGENES

RESUMEN

Este proyecto de grado se desarrolla con el objetivo de analizar el comportamiento de un Ransomware dentro de un sistema operativo Windows, que permita determinar cuáles son las vulnerabilidades más latentes de dicho sistema infectado, y asimismo, proponer políticas y medidas mínimas de seguridad informática a tener en cuenta en ambientes empresariales, para prevenir este tipo de ataques, o en su defecto disminuir las consecuencias que puedan ser ocasionadas.

En primera instancia se da a conocer el concepto de Ransomware y asimismo se expone la evolución que ha tenido el mismo a través del tiempo. Por otro lado, se describen los diferentes tipos de Ransomware, tales como: Locker Ransomware, Crypto Ransomware, Bad Rabbit, Goldeneye, Jiwsaw, Lockergoga, Locky y Petya; de los cuales se selecciona este último para llevar a cabo el desarrollo del laboratorio en un ambiente virtualizado. Posterior a esto se describen los diversos mecanismos de infección que son utilizados por los ciberdelincuentes para poner en riesgo la información de las organizaciones y asimismo se detallan los diversos mecanismos de prevención para evitarlos.

Por último, y como objetivo principal del proyecto se desarrolla el laboratorio de Petya, en el que se simula en un ambiente virtualizado, el envío de un archivo infectado a un correo. Dicho archivo es analizado con una serie de herramientas forenses (Valkyrie y Portal VirusTotal), con el propósito de determinar el origen y el nivel de amenaza que representa el mismo. De acuerdo con los resultados obtenidos se formulan varias recomendaciones a nivel organizacional para prevenir la infección por Ransomware.

Palabras clave: Ransomware, seguridad informática, sistema operativo Windows, Locker Ransomware, Crypto Ransomware, Bad Rabbit, Goldeneye, Jiwsaw,

Lockergoga, Locky, Petya, ambiente virtual, Valkyrie, Portal VirusTotal, amenaza, vulnerabilidad, infección, ciberdelincuentes.

1 INTRODUCCIÓN

En la actualidad las empresas involucran en la mayoría de sus procesos sistemas de información y tecnología que han permitido mayor productividad, eficacia y eficiencia en sus líneas productivas. El beneficio de rentabilidad y producción se ven en los resultados obtenidos cuando se aplica este tipo de procesos y nuevas tecnologías.

Los sistemas de información cumplen un papel muy importante en las empresas, permitiendo que la disponibilidad y el acceso a los datos sea más rápido y oportuno, junto con ello también paralelamente se ha tenido que avanzar y proponer seguridad en la información y los datos, siendo estos los objetivos de ataques informáticos tanto externamente a la red de la empresa como internamente.

La seguridad de la información plantea salvaguardar los tres pilares: confidencialidad, integridad y disponibilidad. Los ataques a sistemas de información y los actores que los producen se han convertido en un elemento más de estudio y cuidado por parte del área de TI. Estos procesos han conllevado que la producción se vea afectada la información y los datos sea vulnerada, modificada y eliminada causando en algunos casos a la perdida en su totalidad de la producción. Los ataques tienen dos objetivos encontrar debilidad y fallos de seguridad para ser corregidos y otro de sus objetivos es causar daño irreversible con pérdidas de información o beneficios económicos. Uno de estos ataques que actualmente se implementan son los ransomware, en otras palabras, pagar por un rescate de dato.

Prevenir estos riesgos e incidentes para la seguridad de la información en las empresas, se ha convertido en una tarea dentro de las actividades de la empresa

para ser implementada, las formas de realizarlo son a través de planes de contingencia, aplicando controles de seguridad, implementando políticas de seguridad y realizando Ethical Hacking o test de penetración.

Un ambiente controlado utilizando Ransomware y aplicando herramientas de seguridad que permitan detectar los fallos de seguridad de la información implicada se presenta como opción donde se realizarán pruebas que permitan constatar las vulnerabilidades encontradas y como actúa con respecto a la seguridad antes y después de implementar diferentes test de penetración y herramientas de seguridad.

Asegurar un sistema requiere deshabilitar servicios, realizar cambios en hardware y software, implementar códigos de seguridad utilizar herramientas de seguridad realizar bloqueos de aplicaciones y a los recursos en la red, el desarrollo de este ambiente pretende unificar aplicaciones de seguridad y configuraciones que permiten mitigar y contrarrestar este tipo de ataque por ello la importancia de tener un ambiente aislado donde se realizan las pruebas y se contrarrestan en la compañía ya implementándola.

2 DESCRIPCIÓN DEL PROBLEMA

Son varias las organizaciones que pasan por alto las medidas de seguridad requeridas que deben tener, para estar a la vanguardia de las nuevas amenazas informáticas, que suponen un gran riesgo en cuanto a los activos de información.

Desde las pymes que no consideran un sistema de seguridad, hasta las grandes empresas que no desean invertir en costos que creen innecesarios. En un alto porcentaje las pymes creen no necesitar un sistema de seguridad y en menor porcentaje general no cuentan con un sistema de seguridad confiable, desde cualquier punto de vista. Aún más, teniendo en cuenta que los ataques informáticos son más comunes de lo que se cree y se expanden con gran facilidad.

Por tanto, se hace evidente la necesidad de implementar y estructurar sistemas informáticos seguros, para proteger y conservar la información almacenada en medios informáticos.

Las investigaciones llevadas a cabo por Kaspersky lab, empresa dedicada a la seguridad informática y con presencia internacional en 200 países, revela cifras preocupantes en una encuesta realizada a más de 4000 empresas del mundo.

3 PLANTEAMIENTO DEL PROBLEMA

Debido al creciente flujo de información que se maneja en la actualidad por todos los medios tecnológicos que existen, hoy en día nace la necesidad de vincular el concepto de seguridad informática a todos los escenarios del ambiente personal y por supuesto empresarial, como medida de prevención y de control ante todos los nuevos ataques que se han venido desarrollando en el mundo informático para robar o alterar negativamente el activo más importante de cualquier organización: La información. La aparición de nuevos virus informáticos, códigos maliciosos, secuestros de la información, suplantación de información, perdida de información, alteración en los sistemas de información, entre otros siniestros, han convertido a los datos y/o información en un preciado tesoro que debe ser resguardado seriamente bajo un plan maestro de seguridad.

Eset (enjoy safer tecnology) sobre el documento informe de tendencias ciberseguridad 2019 el jefe de laboratorio de investigación de ESET Latinoamérica comento “los ciberataques, las fugas de datos y los casos en que se reportaron fallos de control en el control de la privacidad de clientes y usuarios ocurridos durante el 2018, dejan en claro el desafío de asegurar la protección de los activos. Por lo tanto, los objetivos prácticos de la seguridad de información deberán estar enfocados en salvaguardar la confidencialidad, integridad y disponibilidad de los sistemas informáticos y los datos” [1]

Tener un ambiente de pruebas o poner a la merced una zona libre de los sistemas de información sería de gran utilidad para comprobar y detectar cómo estas amenazas actúan, además de ser una guía para crear controles, políticas de

[1] ESET. “Tendencias en seguridad informática para el 2019”. {En línea}. {10 diciembre 2018} disponible en: (https://www.eset.com).

seguridad y utilizar planes de contingencia o respaldo de la información y así poder corregir la falla de seguridad por donde atacan el punto más vulnerable del sistema de información. Por ello, se plantea la siguiente formulación:

¿Cuáles son los riesgos de seguridad sobre la información implicada, al ejecutar un Ransomware (rescate por software) en un sistema Operativo Windows y utilizar herramientas de seguridad informática que conlleven a proponer políticas de seguridad que ayuden a mitigar y controlar las amenazas que se generan, haciendo uso de un ambiente de pruebas controlado?

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Detectar y diagnosticar vulnerabilidades en un sistema operativo Windows infectado con Ransomware en un ambiente de prueba haciendo uso de herramientas de seguridad.

4.2 OBJETIVOS ESPECÍFICOS

1. Identificar y proponer herramientas de seguridad que permitan prevenir el desarrollo y actuación del Ransomware en un sistema de información.

2. Identificar información que permita a las organizaciones socializar y capacitar al personal en el manejo de situaciones relacionadas con Ransomware para reducir su impacto con una serie de recomendaciones o sugerencias.

3. Implementar un ambiente virtual controlado para realizar las pruebas que permitan reflejar el funcionamiento del Ransomware en escalas reales.

5 JUSTIFICACIÓN

Para nadie es un secreto que a diario las organizaciones son víctimas de ciberataques que se manifiestan de diversas maneras, dependiendo del tipo de amenaza o del software malicioso que se es enviado con el objetivo de robar, modificar y corromper información o en el peor de los casos la eliminación de archivos.

Dentro del conjunto de programas maliciosos, se encuentra el Ransomware, un peligroso programa que restringe el acceso de manera no autorizada a los archivos y carpetas donde se aloja a cambio de una recompensa, son varios los casos reportados en organizaciones con este problema y sigue extendiéndose con mucha efectividad. Es por esta razón que surge la idea realizar una investigación pertinente para abordar todos los puntos importantes al momento de crear e implementar normas y políticas de seguridad en sistemas de información.

Lo que se propone es que la seguridad de la información sea abordada desde el punto de vista más importante, no solo como un activo más que se implementa en toda la organización, sino como una herramienta para encontrar las falencias que hacen que este tipo de ataques o software malintencionados ejerzan control y realicen cambios en la información obteniendo un beneficio con ánimo de lucro y perdida de información.

Por ende, el desarrollo de este proyecto cobra gran importancia, al pretender tener un ambiente con controles y herramientas de seguridad que permitan identificar oportunamente el ataque y restringir su actuación en el sistema de información.

Según Sánchez, “Cada entrada tiene un origen en común: cumplir los objetivos del negocio; deben basarse en una política de seguridad institucional e incluso tener un tratamiento diferente y ejecutarse en tiempos distintos ¿A qué me refiero con esto?, antes de salir a producción, cualquier sistema debería pasar por un proceso de fortalecimiento que le permita cumplir con las líneas base de seguridad establecidas de acuerdo con su tipo. Tiempo después es fundamental que la organización mida si esta línea base de seguridad sigue cumpliendo con su objetivo primordial y para ello puede ejecutar estudios de análisis de vulnerabilidades, los cuales alimentan tanto el proceso de remediación como el proceso de fortalecimiento y la actualización de la línea base de seguridad.”[2]

De lo anterior se concluye cuán importante es para una organización, tener un esquema controlado de pruebas de seguridad que permita poner en función a los sistemas de información antes de ser utilizados.

Al considerar un ambiente controlado de pruebas de seguridad como un elemento necesario para reducir todo tipo de malware, ransomware entre otras amenazas informáticas trae como beneficio evitar que la operación de los sistemas sea afectada ante un eventual incidente con el fin de ejecutar estas aplicaciones maliciosas o abrir correos sospechosos.

Al tener un ambiente virtualizado y controlado de seguridad también nos permite realizar todo tipo de prueba y disminuir el riesgo informático para contrarrestar su actuar en los sistemas dando lugar a implementar nuevos cambios o actualizaciones en el software para protegerse ante un eventual ataque y encontrar los fallos se seguridad que presenta el sistema.

[2] SÁNCHEZ, Eduardo Patricio. “Hardening”. {En línea}. {14 de enero de 2015} disponible en: (http://www.magazcitum.com.mx/ ?p=2109#.ViUM_n4veM8)

6 DELIMITACIÓN Y ALCANCE

El proyecto en desarrollo tiene como alcance estudiar un ambiente virtual de prueba controlado en un sistema operativo Windows para ejecutar un tipo de software malicioso en este caso un Ransomware e identificar cómo actúa, y cómo controlarlo utilizando herramientas de seguridad libres para prevenir la amenaza.

Los aspectos puntuales que comprende la investigación están referidos a:

Investigación acerca de los Ransomware y su funcionalidad, instalación y configuración del ambiente virtual utilizando máquinas virtuales en sistemas operativos Windows, ejecución de un Ransomware tipo bloqueador y cifrado, identificación, configuración e instalación de herramientas de seguridad informática que le permitan a las compañías identificar y controlar este malware y saber cómo protegerse de este tipo de ataques.

No se ejecutarán todos los tipos de Ransomware, ni se crearán malwares con esta funcionalidad. El objeto del trabajo es trazado bajo el funcionamiento actual del Ransomware.

7 MARCO REFERENCIAL

7.1 MARCO TEORICO

Nunca en la historia de la humanidad, las personas de todo el mundo han sido sometidas a extorsiones a gran escala como lo son hoy[3]. En los últimos años, el uso personal de las computadoras e Internet ha explotado y, junto con este crecimiento masivo, han surgido delincuentes cibernéticos para alimentarse de este floreciente mercado, dirigido a usuarios inocentes con una amplia gama de malware. La gran mayoría de estas amenazas tienen como objetivo ganar dinero directa o indirectamente de las víctimas. Hoy, el Ransomware se ha convertido en una de las categorías de malware más problemáticas de este tiempo.

El primer ataque conocido fue iniciado en 1989 por Joseph Popp, PhD, un investigador del SIDA, quien llevó a cabo el ataque distribuyendo 20,000 disquetes a investigadores del SIDA en más de 90 países, alegando que los discos contenían un programa que analizaba el riesgo de un individuo de adquirir el SIDA mediante el uso de un cuestionario. Sin embargo, el disco también contenía un programa de malware que inicialmente permaneció inactivo en las computadoras, y solo se activó después de que una computadora se encendió 90 veces. Después de alcanzar el umbral de inicio de 90, el malware mostró un mensaje que exigía un pago de $ 189 y otros $ 378 por un contrato de arrendamiento de software. Este ataque de Ransomware se conoció como el troyano del SIDA, o el PC Cyborg.

Si bien la aparición del troyano del SIDA estableció la amenaza del ransomware, este tipo de malware no se usó ampliamente en el cibercrimen hasta muchos años

[3] TIDY, Joe. “Coronavirus: cómo los piratas informáticos están usando el miedo a la enfermedad covid-19 para difundir virus informáticos”. {En línea}. {13 de marzo de 2020}. En BBC News Mundo disponible en: (https://www.bbc.com/mundo/noticias-51853454).

después. El panorama de amenazas era considerablemente diferente en los años ochenta y principios de los noventa. La evolución del ransomware, particularmente el cripto Ransomware, se aceleró en los últimos años a medida que más empresas criminales imitatorias saltaron a la arena para aprovechar el éxito de los demás.

La primera ola de aplicaciones engañosas hizo su aparición en el año 2005. Las aplicaciones se hicieron pasar por herramientas falsas de eliminación de spyware, como SpySherriff, o herramientas de mejora del rendimiento, como PerformanceOptimizer y RegistryCare. Estas herramientas falsas afectaron principalmente a las computadoras con Windows, pero también se dirigieron a las computadoras Mac OS X. Por lo general, exageraron el impacto de los problemas en la computadora, como las entradas de registro no utilizadas y los archivos corruptos, y dijeron que resolverían estos problemas si el usuario pagaba entre 30 y 90 dólares por una licencia. En realidad, muchos de ellos no arreglaron nada.

La familia Trojan.Gpcoder surgió en mayo de 2005, inicialmente utilizando técnicas de cifrado personalizadas que eran débiles y fáciles de superar. También utilizaron algoritmos de cifrado simétricos, lo que significaba que se usaba la misma clave tanto para el cifrado como para el descifrado. A pesar de las fallas iniciales, los autores del malware no se dieron por vencidos y continuaron creando versiones más nuevas de la amenaza.

A principios de 2006, el concepto de crypto ransomware comenzó a ganar fuerza a medida que los atacantes comenzaron a experimentar con la idea. El crypto ransomware condujo a la aparición de amenazas como Trojan.Cryzip en marzo de 2006. Cryzip copió archivos de datos en archivos individuales protegidos por contraseña y luego eliminó los originales. Sin embargo, la contraseña estaba

incrustada en el código del troyano, lo que facilito la recuperación de la contraseña.

Trojan.Archiveus también surgió en 2006. Al igual que Cryzip, Archiveus utilizó archivos de almacenamiento protegidos con contraseña, pero en un extraño giro, el malware no solicitó el pago en efectivo. En cambio, le pidió a la víctima que comprara medicamentos por Internet utilizando ciertas URL de farmacias en línea. Luego, la víctima necesitaba enviar la identificación de la orden para obtener la contraseña para descifrar los archivos. De esta manera, los atacantes podrían haber obtenido una comisión de la compra, que luego se consideró como un pago de rescate.

El siguiente punto crucial ocurrió entre 2008 y 2009, cuando los ciberdelincuentes cambiaron a usar programas antivirus falsos, una subcategoría más agresiva de aplicaciones engañosas. Las herramientas imitaron la apariencia y la funcionalidad del software de seguridad legítimo y realizaron escaneos simulados, alegando encontrar grandes cantidades de amenazas y problemas de seguridad en la computadora. Luego se le pidió al usuario que pagara una tarifa de entre US $ 40 y US $ 100 para solucionar los problemas falsos. También es posible que se les haya pedido que pagaran por servicios de soporte de varios años falsos.

De 2011 a 2012, los atacantes hicieron la transición de herramientas de antivirus falsas a una forma de extorsión más disruptiva. Esta vez, los ciberdelincuentes deshabilitaron el acceso y el control de la computadora, bloqueando efectivamente la computadora del uso.

A medida que se refinó el Ransomware de los casilleros, pasó de simplemente informar errores inexistentes a comenzar a introducir errores y problemas.

Finalmente, dejó de fingir ser una herramienta útil para mostrar una solicitud de pago evidente para restablecer el acceso a la computadora. Esto se debe a que, en los primeros días, los atacantes engañaron a las víctimas para que descargaran herramientas falsas para solucionar sus problemas informáticos.

Hoy en día, el Ransomware puede instalarse sin ninguna interacción del usuario a través de ataques como descargas automáticas. A pesar de esto, los creadores de Ransomware Lockers continuaron utilizando técnicas de ingeniería social para convencer a los usuarios de que pagaran el rescate. Las amenazas comenzaron a hacerse pasar por avisos policiales en lugar de software antivirus y herramientas de rendimiento del sistema. Por lo general, afirmaron que el usuario había infringido la ley al descargar materiales con derechos de autor, como música pirateada, películas o software (una ocurrencia común de acuerdo con diversas estadísticas de la industria), o al ver otros materiales digitales ilegales, como imágenes pornográficas que representan menores o animales.

Desde 2013 hasta la actualidad, ha habido un pivote de regreso al crypto ransomware. Crypto ransomware tiende a no usar ingeniería social; en cambio, es sincero acerca de sus intenciones y demandas. Las amenazas suelen mostrar un mensaje de extorsión, que ofrece devolver datos tras el pago de rescates considerables. Crypto ransomware ha elevado la barra de cantidades de rescate a un nuevo nivel. Una amenaza típica de crypto ransomware solicita un pago de alrededor de US $ 300 por una sola computadora. Las amenazas actuales de crypto ransomware son mucho más capaces que sus predecesores, con procedimientos operativos y de cifrado más sólidos.

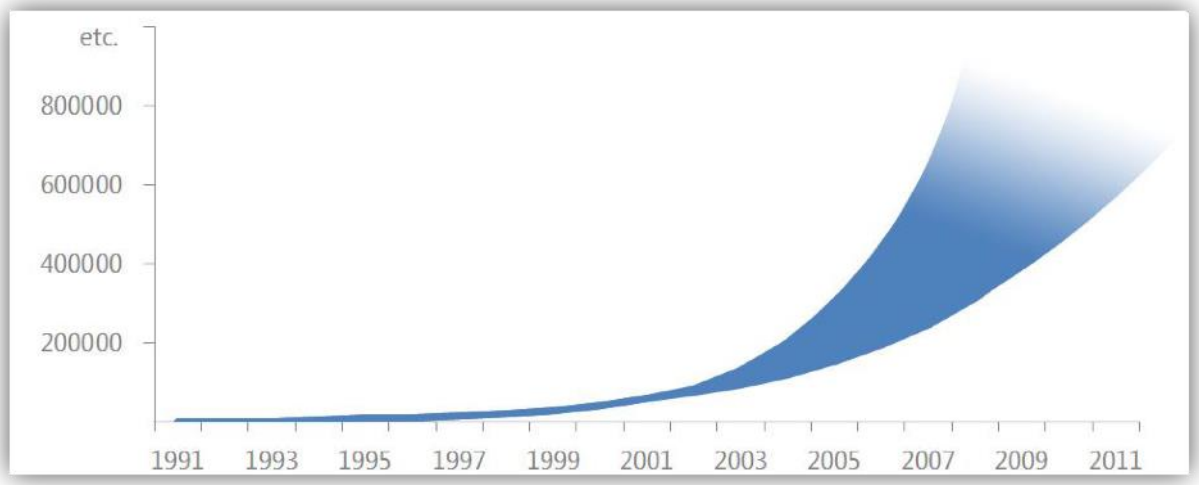
Petya existe desde 2016, y se diferencia del ransomware típico, ya que no solo encripta archivos, sino que también sobrescribe y encripta el registro de arranque maestro (MBR). El ransomware Petya ataca las redes mediante la explotación de

una falla de seguridad en el sistema operativo Windows de Microsoft que fue utilizada originalmente por la Agencia de Seguridad Nacional (NSA). La vulnerabilidad, conocida como EternalBlue.

El primer ataque del Petya fue en Ucrania, ha infectado sistemas en España, Alemania, Israel, el Reino Unido, los Países Bajos y los Estados Unidos. Las grandes corporaciones se han visto afectadas Maersk, el gigante petrolero ruso Rosneft e instituciones públicas y privadas en Ucrania. Incluso el reactor nuclear de Chernobyl informó casos de Petya.

Microsoft estima que más de 12,000 máquinas han sido afectadas por el Petya y la mayoría de las empresas afectadas por esta amenaza aún están evaluando el impacto y tomando medidas de emergencia para contener el ataque mientras continúan las investigaciones.

Ilustración 1 Aumento aproximado del malware desde 1991



Illustracion *Aumento aproximado Del malware* ***Fuente:*** *Microsoft Security Intelligent Report* ***Tomado de:*** *Microsoft_Security_Intelligence_Report_Special_Edition_10_Year_Review_Spanish.pdf*

A través de la historia se puede observar que constantemente se usan métodos distintos para acceder a la información digital de diversas maneras; uno de los más frecuentados es a través del Ransomware, un malware que desde el 2009 ha ido creciendo rápidamente y se ha expandido por todo el globo terráqueo. La distribución de este malware lo hace un delincuente cibernético con fines delictivos.

Actualmente se pueden encontrar en el mundo diferentes tipos de Ransomware que se enfocan en el secuestro de información, entre ellos uno muy conocido a nivel mundial es el “Fake police Ransomware”. Este Ransomware se enfoca principalmente en el defacing de un portal de la policía o FBI, para recaudar dinero a cambio de la información “legalmente” confiscada. Además de las posibles variaciones de este malware, desarrollo un método de propagación vía spam por email, el cual valida en un servidor el idioma y región de la víctima para traducir el mensaje por completo.

7.2 IDENTIFICACIÓN DE HERRAMIENTAS PARA PROTEGERSE FRENTE A LOS MALWARE.

7.2.1 MALWAREBYTES

Anteriormente conocido como Malwarebytes Anti-Malware, funciona junto con cualquier programa antivirus, incluido Windows Defender, y encuentra amenazas que podrían haberse filtrado. Funciona más como una capa adicional de protección, especialmente contra Malwares haciendo uso de diferentes scanners , en sus versiones más recientes cuenta con un scanner para la detección de ransomware.

Ilustración 2 Malwarebytes

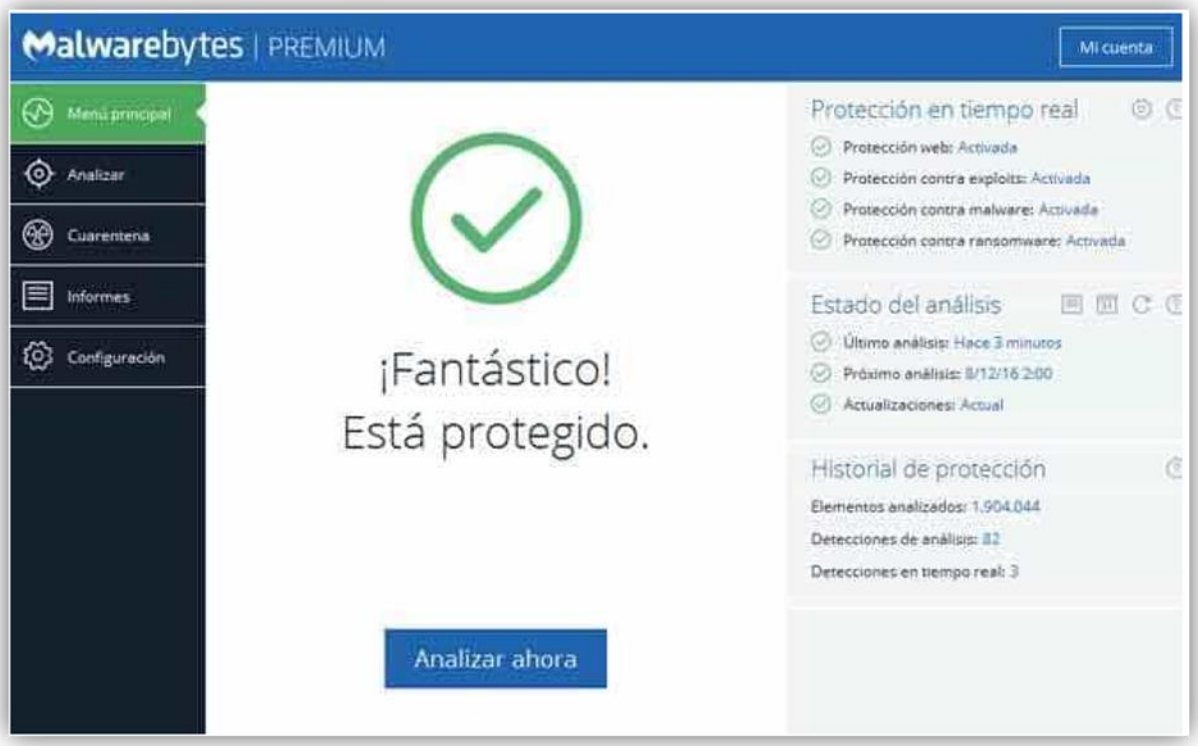


***Ilustración** MalwareBytes **Fuente:** los 7 mejores antimalware del 2020, la tienda de la licencias Tomado **de:** https://blog.latiendadelaslicencias.com/mejores-antimalware/*

Cabe mencionar que cuenta con una versión free y otra de pago, la cual cuenta con diversas características de la que carece la versión free.

Ilustración 3 Microsoft Malicious Software

***Ilustración** Microsoft Malicious Software **Fuente:** los 7 mejores antimalware del 2020, la tienda de las licencias **Tomado de:** https://blog.latiendadelaslicencias.com/mejores-antimalware/:*

La Herramienta de eliminación de software malintencionado de Windows (MSRT) de Microsoft es un programa gratuito que elimina todo el host del software malicioso (malware) más popular. Muchos usuarios de Windows lo tienen instalado y lo ejecutan mensualmente, pero no son conscientes de su existencia. Es un programa de sigilo, cuando las cosas funcionan normalmente no lo ves.

Se actualiza silenciosamente como parte de Windows Update, se ejecuta en lo que la compañía denomina "modo silencioso", lo que significa que no genera alertas al usuario, al menos mientras no encuentre ningún malware para eliminar.

Ilustración 4 Dr.Web CureIt!

Ilustración *Dr. Web CureIt* ***Fuente:*** *los 7 mejores antimalware del 2020, la tienda de las licencias Tomando* ***de:*** *https://blog.latiendadelaslicencias.com/mejores-antimalware/*

Es una solución rápida a sus problemas de seguridad pendientes. El escáner proporciona una excelente solución para buscar y eliminar virus, malware y spyware de su computadora. No requiere instalación; Es extremadamente fácil de usar; solo toma 20 minutos en promedio ejecutar un análisis completo y completo, es gratis.

Las definiciones de virus reciben actualizaciones varias veces al día, así que cada vez que ejecute un análisis, asegúrese de descargar la última versión del escáner.

7.2.2 COMBOFIX

Es un programa, creado por sUB, que escanea su computadora en busca de malware y luego procede a limpiar estas infecciones automáticamente si es posible.

Además de poder eliminar una gran cantidad del malware, ComboFix también muestra un informe que puede ser utilizado por ayudantes capacitados para eliminar el malware que el programa no elimina automáticamente.

Ilustración 5 AdwCleaner

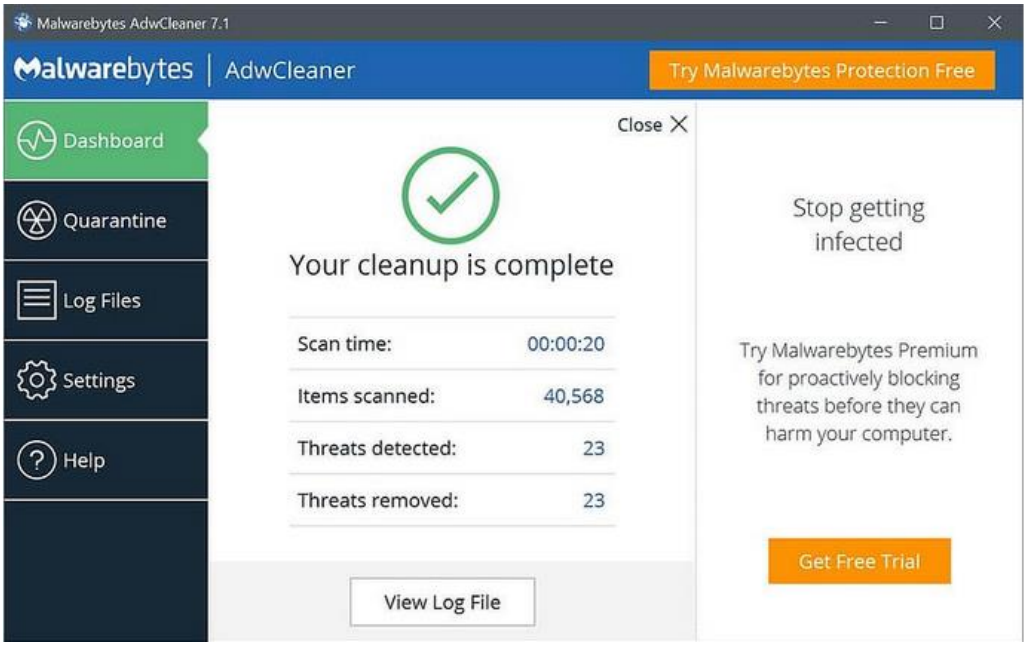


***Ilustración** AdwClearner **Fuente:** los 7 mejores antimalware 2020, la tienda de las licencias, **Tomado de:** https://blog.latiendadelaslicencias.com/mejores-antimalware/*

Es un programa gratuito anti-adware desarrollado por Malwarebytes.fue desarrollado por el equipo de desarrollo de Xplode. El usuario puede escanear el sistema en busca de accesos directos, claves de registro y extensiones de navegador maliciosas. También puede detectar bloatware y otros PUP como enlaces de Ebay en el escritorio.

Ilustración 6 Virus Total

Ilustración: *Virus total* ***Fuente:*** *los 7 mejores antimalware del 2020, la tienda de las licencias* ***Tomado de:*** *https://blog.latiendadelaslicencias.com/mejores-antimalware/*

Es el mejor escáner de virus en línea ya que no solo se encarga de escanear URL, direcciones IP y archivos contra varios motores de antivirus diferentes, sino que también se puede usar por correo electrónico o desde un escritorio para escanear procesos en ejecución.

Se utilizan docenas de diferentes motores antivirus para analizar los archivos enviados a VirusTotal, lo que significa que se utilizan varias perspectivas diferentes para determinar si un archivo es malicioso o no.

7.2.3 PROPUESTA DE HERRAMIENTAS DE SEGURIDAD

Privacy Manager

Bloqueadores de JavaScript para los navegadores web, que impiden la ejecución de todos aquellos scripts que puedan ser identificados como dañinos y reducción de la infección desde la web.

Anti Ransom

Bloquea el proceso de cifrado de un ransomware (monitorizando “honey files”) , también realiza un dump de la memoria del código dañino en el momento de su ejecución en el que con suerte se hallara la clave del cifrado simétrico que estuviera empleándose.

Máquinas virtuales

Se evita el alto contagio de ransomware debido a las técnicas anti-debug y anti virtualización comúnmente presente en este tipo de código dañino y se ha demostrado que en un entorno virtualizado su acción no llega materializarse

EMET

Herramienta que permite mitigar exploits, utilizando técnicas de mitigación específicas como la prevención de la ejecución de los datos, el filtrado de acceso a tablas de dirección de exportación, la protección de la sobre escritura de manejadores de excepciones estructurados.

Applocker

La utilidad principal de esta herramienta es por tanto limitar la instalación de malwares e impedir la instalación de software no normalizado o que necesita una licencia que no posee, impedir la ejecución de ficheros desde directorios comunes utilizados por el ransoware.

Crytoprevent

Esta herramienta es un complemento de software antivirus/ antimalware que previene infección de ransoware su método de protección creado con reglas “SRP” (también conocidas como políticas de restricción de software) impidiendo la ejecución del malware.

7.3 MARCO CONTEXTUAL

Se realizará una investigación acerca del Ransomware actualmente utilizado para la realización de ataques a las organizaciones, donde la investigación arrojará resultados muy importantes para la evaluación del malware en cada fase del desarrollo del trabajo.

Los problemas más frecuentes que se encuentran en la infección del Ransomware, son el secuestro de información y la extorsión por parte del delincuente cibernético.

Por otra parte, se corre el riesgo de perder toda la información si no se paga el rescate o se desencripta los archivos en el tiempo estipulado, el cual suele rondar los 3 días.

Conforme a lo anterior los problemas están vinculados y asociados a la falta de prevención y seguridad en los procesos diarios que se realizan en las empresas los cuales se ven expuestos a ser víctimas de acciones ilícitas.

7.4 MARCO DE ANTECEDENTES

Dentro de las diferentes investigaciones en esta área se encuentra la del Ransomware Digital Extortion: A Rising New Age Threat (Akashdeep Bhardwaj, 2016), en la que se presenta al ransomware explicando qué es y cómo se propaga, pero además recopila soluciones para contrarrestar el malware. Proponen un ambiente de detección de malware en la nube con tres diferentes ambientes de análisis, con lo que, según la investigación, se consigue detectar más rápido el malware. El malware cuando es detectado ya no puede ingresar a otros huéspedes que tengan esta solución instalada, ya que por medio de la utilización de la nube como medio de comunicación y recopilación de información se evita su propagación.

Por otro lado, se encuentra la investigación realizada en Quito - Perú a comienzos del año 2019, por el Sr. Freddy Daniel Bazante Veloz, en el que haciendo uso de un ambiente controlado (Sandboxing), se plantea un modelo de machine learning

en el cual se recopilan atributos obtenidos del análisis dinámico del comportamiento del malware, que permite eventualmente, anticiparse a futuros ataques.

Por último, y como dato importante a tener cuenta, en el 2018 se hizo un estudio del impacto del Ransomware en los países latinoamericanos durante el año 2017, encontrándose lo siguiente:

> "…Perú encabeza la lista con el 25,1% del total de detecciones de los países latinoamericanos. Esto significa que 1 de cada 4 identificaciones de ransomware en Latinoamérica se realizó en territorio Inca.
>
> El segundo lugar lo ocupa México con el 19,6% de las detecciones, seguido de Argentina (14,5%), Brasil (14,0%) y Colombia (9,6%). La lista la complementan Chile (5,7%), Ecuador (4,6%), Venezuela (3,2%), Bolivia (2,1%) y Guatemala (1,4%), como los diez países con mayores porcentajes de detección en la región"[4].

Por lo anterior, se evidencia que Colombia está dentro de los países con mayor exposición a los ataques de este tipo. Los diferentes tipos de Malware se han transformado en un riesgo muy importante para las organizaciones, el cual ha ido evolucionando en cantidad, complejidad y variedad afectando tanto a usuarios como infraestructuras de organizaciones y continuidad en las empresas. Según ESET, en el año 2015 el 40% de los ataques informáticos corresponde a ataques con malware que explotan vulnerabilidades no detectadas por las organizaciones y un 16% a suplantación de correos de correos electrónicos (ESET 2016).

Según kaspersky se dimensionó al Ransomware desde dos olas: la primera desde la ola bloqueadora en donde el malware se parte en dos: el andes y después del cifrado donde bloqueaban el acceso al sistema operativo o al navegador de la

[4] MENDOZA, Miguel Ángel. "El impacto del Ransomware en Latinoamérica durante el 2017". {En línea}. {Marzo 1 de 2018} disponible en: (https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/)

víctima hasta que este pagaba su rescate su pago se hace en dinero o transferencias dinero electrónico, es un ataque muy rentable para los ciber delincuentes que se utiliza con frecuencia.

La segunda ola denominada los cifradores, donde se da inicio al bitcoin la moneda cifrada que es parecido a un activo digital imposible de rastrear su forma de operandi era cifrar los discos duros y la información con igual objetivo pago por su rescate donde la víctima se vería obligado en pagar su rescate. Según análisis de Kaspersky Security Network, en un año en un año el número de ataques se quintuplicó: De 131,111 intentos de infección entre 2014 y 2015 a 718,536 entre 2015 y 2016 (Kaspersky).

7.5 MARCO CONCEPTUAL

El Ransomware es un tipo de malware que al infectar nuestro ordenador le da paso al atacante o ciber delincuente la forma de bloquear por completo el PC desde una conexión externa de forma remota y encriptar la información y el control de todo nuestro ordenador. Con el fin de recibir un pago por el rescate de la información y restablecimiento normal de la información, este proceso está sumergido generalmente en la moneda virtual (bitcoin).

Aparece otro componente de este grupo de los virus denominado Malware a la familia que pertenecen los Ransonware. Según avast.com: la noción que se percibe es que es uno de los virus informáticos que más afectan a los usuarios, hace referencia a cualquier tipo de software malicioso cuyo objetivo es infectar el computador o dispositivo móvil su finalidad es extraer información personal de su víctima o contraseñas robar dinero y evitar que se tenga acceso a los sus dispositivos. El malware es la amenaza que puntea el ranking en equipos infectados.

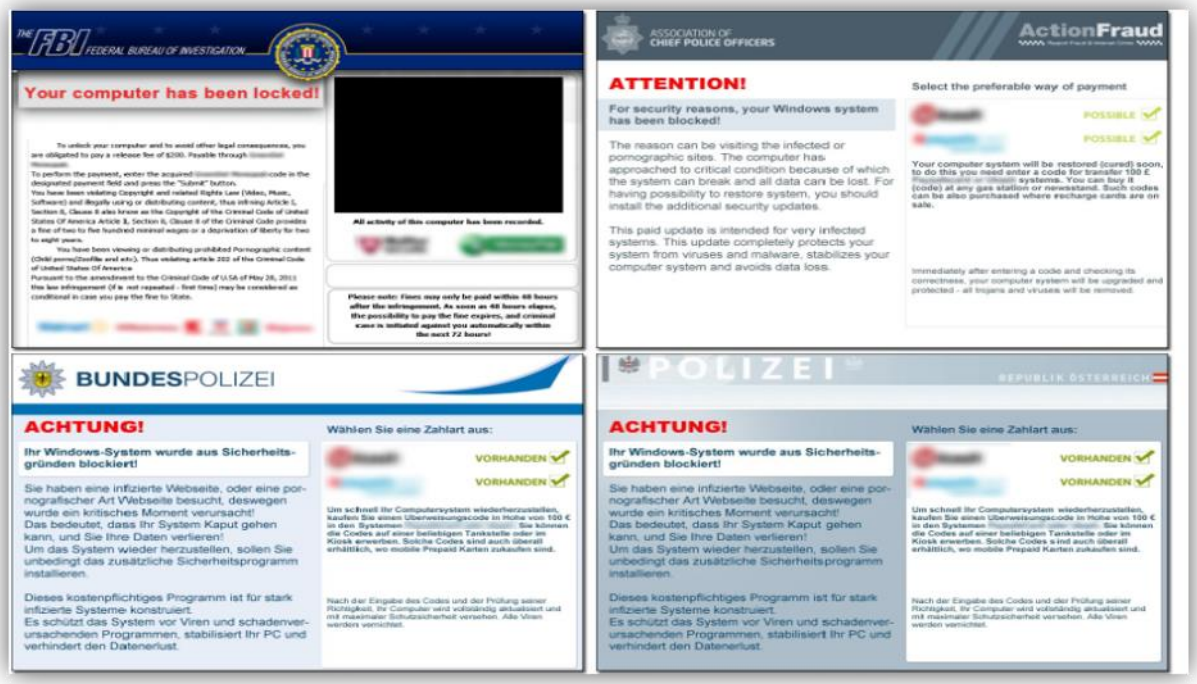
El término virus, esa amplia gama de códigos destructivos, fue utilizado por primera vez por Yisrael Radai en 1990 quien dijo “los troyanos constituyen solo un

pequeño porcentaje de malware (una palabra que acabo de acuñado por troyanos, virus, gusanos, etc.)”[5], entre los cuales podemos encontrar múltiples tipos de malware que se conocen a lo largo de su propagación.

A través de la historia se puede observar que constantemente se usan métodos distintos para acceder a la información digital de diversas maneras; uno de los más frecuentados es a través del Ransomware, un malware que desde el 2009 ha ido creciendo rápidamente y se ha expandido por todo el globo terráqueo. La distribución de este malware lo hace un delincuente cibernético con fines delictivos. Actualmente se pueden encontrar en el mundo diferentes tipos de Ransomware que se enfocan en el secuestro de información, entre ellos uno muy conocido a nivel mundial es el “Fake police Ransomware”. Este Ransomware se enfoca principalmente en el defacing de un portal de la policía o FBI, para recaudar dinero a cambio de la información “legalmente” confiscada. Además de las posibles variaciones de este malware, desarrollo un método de propagación vía spam por email, el cual valida en un servidor el idioma y región de la víctima para traducir el mensaje por completo.

[5] ELISAN, Christopher. Malware, rootkits & botnets a beginner's guide. New York: McGraw-Hill/Osborne, 2013. 384p.

Ilustración 7 Fake Police Rasomware



Fuente: Ransoware A Growing Menace, Gavin o Garman, Sysmantec security response Tomado de: ransomware-growing-menace-12-en.pdf

Según TrendLabs, entre los incidentes más notables en la mitad del 2019 con el auge de nuevas familias de Ransomware, sus principales ataques fueron a empresas multinacionales e incluso a entes gubernamentales. Su forma de ataque era el de enviar correos electrónicos de phishing a sus empleados, analizar las falencias de seguridad para obtener acceso a la red y luego moverse entre la red un caso de esto es el Ransomware LockerGonga que afecto a un empresa noruega generando pérdidas económicas, también se presentó el ataque a la ciudad de Baltimore Maryland en el ataque a sus sistemas de información, donde se pagó para su recuperación, toda esta cadena de ataques a grandes perfiles y escala y de pagos de gran valor aunque reportan gran disminución de las familias de los Ransomware el 77% de detecciones generadas en la mitad del 2018 y su comparación con c al segunda mitad del mismo año disminuyo en 55%. La única

familia de estos malware que se mantiene es el wannacry con mayor número de detecciones.

Dentro de las vulnerabilidades más relevantes encontradas en este nuevo periodo de propagación se encontraron defectos de hardware, como el meltfdown y spectre a principios del 2018 y mitad del 2019, en donde se demostró como los atacantes podían usar mal los enclaves diseñados para proteger y acceder a los datos de la protección de usa INTEL (SGX). Estos ataques son identificados como zombieload, fallout y rogué in flight data load (RIDL), donde los atacantes ejecutan códigos que filtran datos.

7.6 MARCO LEGAL

7.6.1 LEY 1273 DE 2009

“Por medio de la cual se crea un nuevo bien jurídico tutelado denominado ‘de la protección de la información y de los datos’ y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones." [6]

A partir de la Ley 1273 de 2009, en Colombia se tipificaron los delitos informáticos con las siguientes descripciones: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios web para capturar datos personales y transferencia no consentida de activos.

Específicamente, “el delito relacionado con los ‘daños informáticos’ está contemplado en el artículo 269d y se comete cuando una persona que, sin estar autorizada, modifica, altera, daña, borra, destruye o suprime datos del programa o de documentos electrónicos, en los recursos de las TIC.

El artículo 269e contempla el delito vinculado con el ‘uso de software malicioso’ técnicamente denominado malware, ya generalizado en internet. Se presenta cuando se producen, adquieren, venden, distribuyen, envían, introducen o extraen

[6] COLOMBIA, Congreso de la República. “Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se conservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial No. 47.223, 5 de enero de 2009.” {En línea}. Enero de 2009. {20 de marzo de 2020} disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html).

del país software o programas de computador que producen daños en los recursos de las TIC".[7]

7.6.2 LEY 599 DE 2000

Por la cual se expide el código penal colombiano. "En su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones:

Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles."[8]

[7] OJEDA, J. E., RINCÓN, F., ARIAS, M. E., DAZA, L.A. "Delitos informáticos y entorno jurídico vigente en Colombia." {En línea}. 2010. {13 de abril de 2020} disponible en: (http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003).

[8] OJEDA, J. E., RINCÓN, F., ARIAS, M. E., DAZA, L.A. "Delitos informáticos y entorno jurídico vigente en Colombia." {En línea}. 2010. {13 de abril de 2020} disponible en: (http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003).

8 RANSOMWARE: DESARROLLO A TRAVÉS DEL TIEMPO

La evolución del Ransomware ha sido influenciada en gran medida por una variedad de desarrollos en tecnología, economía, seguridad y cultura desde 1989. El Ransomware de hoy es una amenaza sofisticada que afecta a los usuarios en muchas regiones del mundo, particularmente aquellos que viven en economías desarrolladas y de alta tecnología. El mundo del Ransomware es como cualquier ecosistema de la vida real. Las amenazas que pueden adaptarse y evolucionar a su entorno pueden sobrevivir e incluso prosperar, mientras que aquellas que no pueden o no pueden adaptarse pueden eventualmente desaparecer.

"El Ransomware es único entre los delitos cibernéticos porque para que el ataque tenga éxito, requiere que la víctima se convierta en cómplice voluntaria después del hecho."[9]

El Ransomware se ha convertido en uno los tipos de malware más peligrosos para la seguridad de la información, teniendo en cuenta el año de su creación y su acelerada evolución, ha infectado a miles de organizaciones ocasionando incontables perdidas.

Su mecanismo de infección es muy agresivo, debido a que usa algoritmos de encriptación simétricos y asimétricos que hacen prácticamente imposible su desencriptación.

[9] JAMES, Scott. "¿Las mejores frases sobre seguridad informática?" {En línea}. Abril 4 de 2017. {Enero 10 de 2020} disponible en: (https://protegermipc.net/2017/04/04/las-mejores-frases-sobre-seguridad-informatica/).

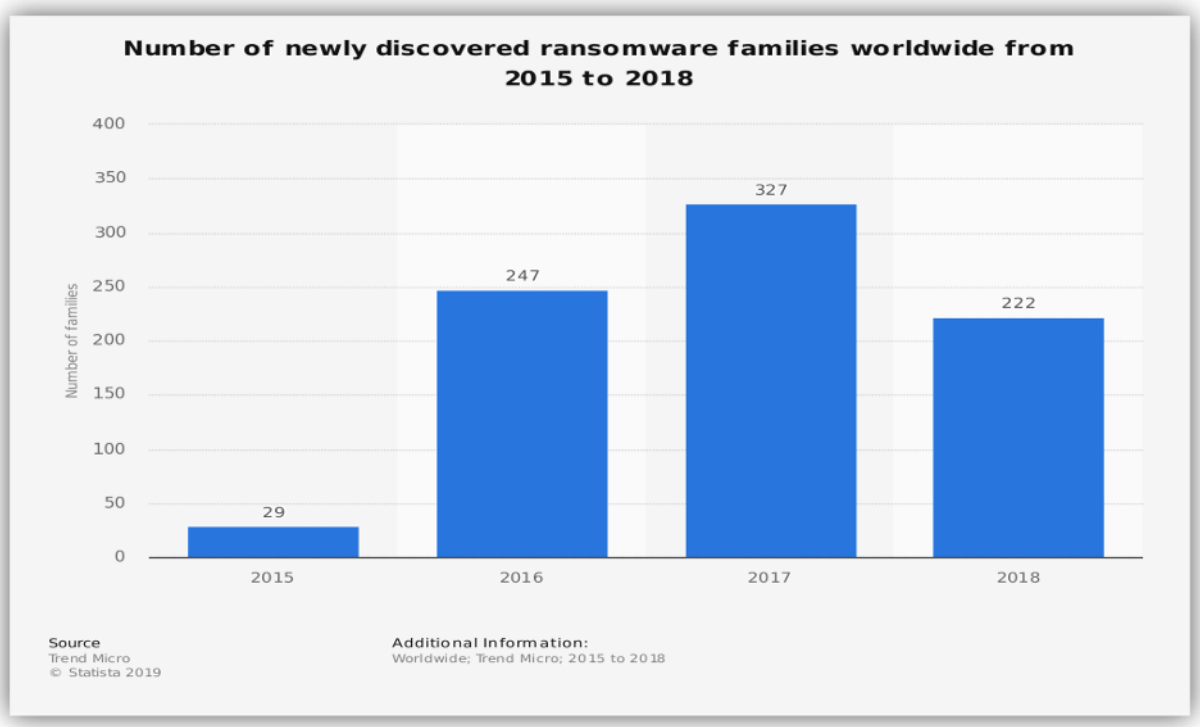
Antes del 2016 las víctimas eran usualmente usuarios que a través de spam quedaban infectados al descargar un adjunto infectado. Pero el panorama cambio totalmente en el año 2017 con dos grandes epidemias a nivel mundial, la primera fue “WannaCry”, la cual estableció la primera hipótesis sobre la verdadera intención del Ransomware, debido a que no solo era cuestión de dinero sino de sabotaje y eliminación de información.

Posteriormente la siguiente amenaza despejo cualquier duda sobre sus verdaderas intenciones, con el surgimiento de “Petya” las organizaciones pasaron a ser un objetivo principal, con esto no solo aumento la preocupación sobre la seguridad de la información, sino que a su vez comenzó una nueva perspectiva acerca del nivel de seguridad con el que cuentan diversas compañías a nivel global.

Por otra parte, el Ransomware no solo es prolífico en Windows, sino también en Android, Linux e incluso MacOS. El sistema operativo Android se consideró un candidato probable para la nueva generación de Ransomware móvil, no solo por su asombrosa participación de mercado del 86.7 por ciento en el segundo trimestre de 2019, según IDC[10], sino también porque tiene más de 1.4 mil millones de usuarios activos de 30 días en todo el mundo, según el CEO de Google, Sundar Pichai[11].

[10] IDC. “Smartphone Market Share”. {En línea}. {Enero 13 de 2020} disponible en: (https://www.idc.com/promo/smartphone-market-share/os).
[11] PICHAI, Sundar. “Google spent $1.2 million last year to protect CEO Sundar Pichai in an 'overall security program' that started months after the YouTube shooting”. {En línea}. Mayo 1 de 2019. {Enero 13 de 2020} disponible en: (https://www.businessinsider.in/google-spent-1-2-million-last-year-to-protect-ceo-sundar-pichai-in-an-overall-security-program-that-started-months-after-the-youtube-shooting/articleshow/69122609.cms)

Ilustración 8 Crecimiento de las familias de Ransomware a través del tiempo



***Fuente**: estadisticas 2018 crecimiento las familias Del Ransomware, Trend Micro 2018 Annual Security Roundup, page 11 **Tomado de**: https://www.trendmicro.com/es_es/business.html*

9 RANSOMWARE: TIPOS DE RANSOMWARE

9.1 LOCKER RANSOMWARE

Este tipo de ransomware fue diseñado para negar el acceso a los recursos informáticos. Esto generalmente bloquea la interfaz de usuario de la computadora o dispositivo y luego exige al usuario que pague una tarifa para restablecer el acceso a ella.

Las computadoras bloqueadas a menudo se quedarán con capacidades limitadas, como permitir que el usuario solo interactúe con el ransomware y pagar el rescate.

9.2 CRYPTO RANSOMWARE

Este tipo de ransomware es mucho más agresivo, debido a que encripta la información del sistema, pidiendo a una llave pare poder desencriptar la información, esta llave por lo general tiene un precio en una moneda poco rastreable como es Bitcoin.

9.3 BAD RABBIT

Bad Rabbit es un ataque de ransomware de 2017 que se propagó usando un método llamado ataque "drive-by", donde los sitios web inseguros son atacados y utilizados para llevar a cabo un ataque.

Durante un ataque de ransomware drive-by, un usuario visita un sitio web legítimo, sin saber que un hacker lo ha comprometido.

Los ataques automáticos a menudo no requieren ninguna acción de la víctima, más allá de navegar a la página comprometida. Sin embargo, en este caso, se infectan cuando hacen clic para instalar algo que en realidad es malware disfrazado. Este elemento se conoce como cuentagotas de malware.

Bad Rabbit utilizó una solicitud falsa para instalar Adobe Flash como un cuentagotas de malware para propagar su infección.

9.4 GOLDENEYE

El resurgimiento de Petya, conocido como GoldenEye, condujo a un ataque global de ransomware que ocurrió en 2017.

Apodado el "hermano mortal" de WannaCry, GoldenEye alcanzó más de 2.000 objetivos, incluidos destacados productores de petróleo en Rusia y varios bancos.

GoldenEye incluso obligó a los trabajadores de la planta nuclear de Chernobyl a verificar los niveles de radiación manualmente, ya que habían sido bloqueados de sus PC con Windows.

9.5 JIGSAW

Jigsaw es un ataque de ransomware que comenzó en 2016. Este ataque recibió su nombre ya que presentaba una imagen de la marioneta de la franquicia de películas Saw.

Jigsaw eliminó gradualmente más de los archivos de la víctima cada hora que la demanda de rescate no se pagó. El uso de imágenes de películas de terror en este ataque causó angustia adicional a las víctimas.

9.6 LOCKERGOGA

Esta variedad de ransomware golpeó a varias empresas manufactureras europeas, incluida Norsk Hydro. El ransomware se infiltró en la empresa a través de un correo electrónico de phishing, lo que provocó una interrupción global de TI y obligó a la empresa a ordenar cientos de computadoras nuevas.

9.7 LOCKY

Locky es un tipo de ransomware que fue lanzado por primera vez en un ataque de 2016 por un grupo organizado de hackers.

Con la capacidad de cifrar más de 160 tipos de archivos, Locky se propaga engañando a las víctimas para que lo instalen a través de correos electrónicos falsos con archivos adjuntos infectados. Este método de transmisión se llama phishing, una forma de ingeniería social.

Locky apunta a una variedad de tipos de archivos que a menudo usan diseñadores, desarrolladores, ingenieros y evaluadores.

9.8 PETYA

Petya (que no debe confundirse con ExPetr) es un ataque de ransomware que golpeó por primera vez en 2016 y resurgió en 2017 como GoldenEye.

En lugar de cifrar archivos específicos, este vicioso ransomware cifra todo el disco duro de la víctima. Lo hace cifrando la tabla maestra de archivos (MFT), lo que hace que sea imposible acceder a los archivos en el disco.

Petya se extendió por los departamentos de recursos humanos a través de un correo electrónico falso de solicitud de empleo con un enlace de Dropbox infectado.

Su origen se remonta en marzo de 2016 reportado por la empresa **Heise Security**, por pertenecer a la familia de virus troyanos uno de los métodos de propagación fue utilizar programas o páginas que funcionan como sistemas de archivos un ejemplo de esto fue utilizando dropbox.

Una empresa desarrolladora de software europea denominada Intellect Service crea una actualización para un programa de contabilidad llamado medoc el cual es muy utilizado por empresas en ucrania el mismo día del lanzamiento fue infectada esta actualización para descargar el malware en vez de la actualización de la actualización para el programa contable.

Durante su propagación existieron también variantes de este malware con ciertas peculiaridades con el mismo propósito un ejemplo de esta fue: RANSOM.PETYA.SMA esta variante se aprovechó de la vulnerabilidad emitida del protocolo SMB por Microsoft Security utilizando herramientas como eternalblue y eternalromance, para realizar su propagación

9.9 ¿CUÁL ES EL OBJETIVO PRINCIPAL DEL ATAQUE DE PETYA A LOS ORDENADORES?

Es infectar el MBR (MASTER BOOT RECORD) que se define como el registro de arranque principal o primer sector de arranque del disco duro que permite en el que esta la información necesaria para proceder con la carga del sistema

operativo para que la BIOS cargue el disco, en él se encuentran las tablas de particiones. El petya lo infecta para evitar cualquier acción del usuario e infectar y cifrar las particiones es decir crea una barrera entre el arranque del sistema operativo y el MBR.

10 RANSOMWARE: MECANISMOS DE INFECCIÓN

La gran mayoría de los ataques de Ransomware que se ven hoy en día se distribuyen mediante correos electrónicos no deseados y de phishing, o mediante sitios web que contienen el malware.

10.1 SPAM /PHISHING EMAILS

Durante años el spam ha sido utilizado potencialmente a través de emails o archivos adjuntos con el objeto de infecta a la víctima, con el Ransomware no es la excepción siendo la causa más frecuente de infección a nivel mundial, por lo general los correos sueles contener alguna información legal y suelen parecer de fuente confiables, aunque no lo sean.

El Phishing por su parte también ha afectado a gran cantidad de usuarios, por lo general en emails que han sido suplantados y direccionados a servidores que contienen malware con el fin de robar información confidencial o infectar liberar el Malware.

10.2 MALICIOUS WEB SITES/WEB ADS

Por otra parte, también existen sitios web potencialmente peligrosos que no cuentan con protocoles de seguridad y suelen estar con múltiples anuncios que se encuentras infectados para poder liberar el malware.

10.3 CLICKBAITS

Los Clickbaits tambien cuentan con un peligro moderado debido a que funcionan como anzuelo para captar clicks y visitantes a páginas o enlaces que pueden contener todo tipo de malware.

10.4 MALAS PRÁCTICAS DEL USUARIO

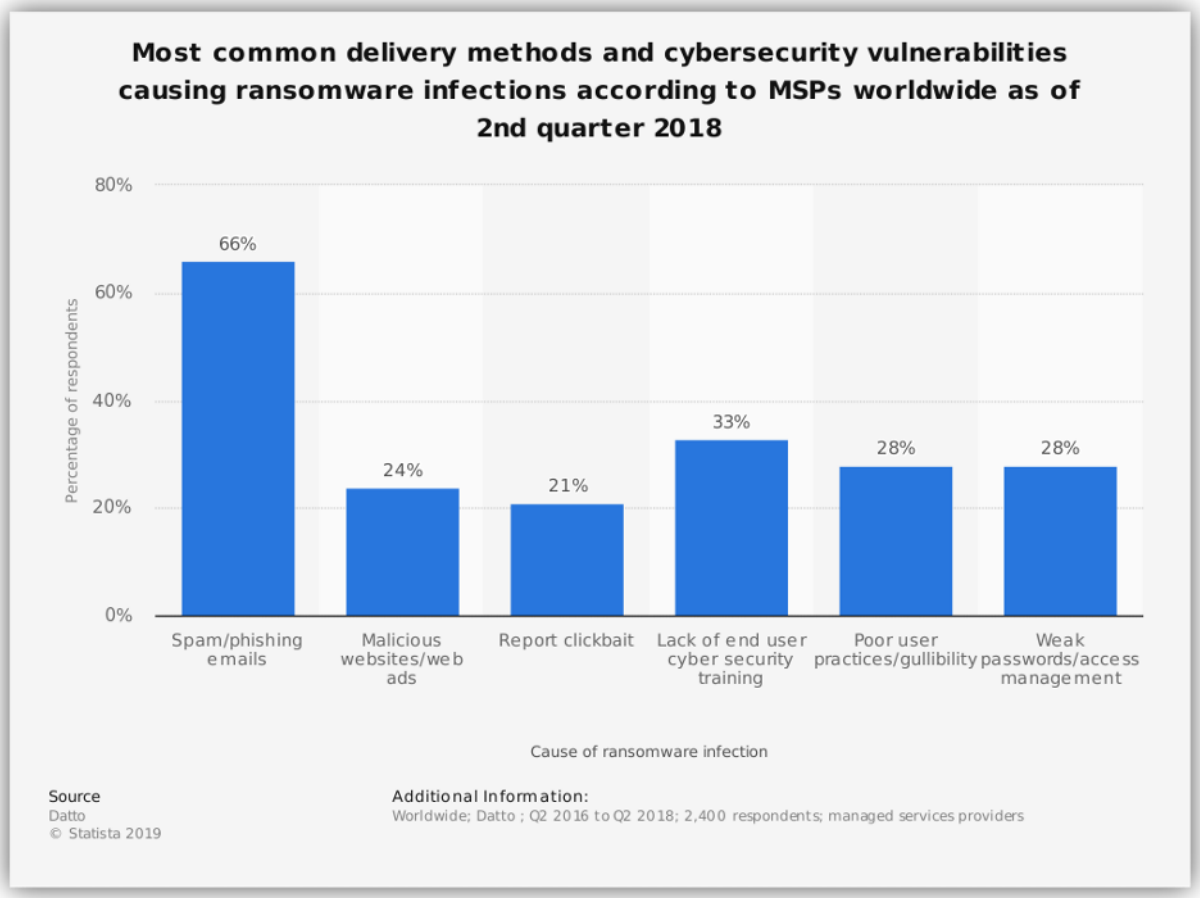
Las malas prácticas también pueden desencadenar problemas y son más comunes en ambientes donde no se tienen los controles o procedimientos necesarios para los procesos que requieren recursos informáticos.

10.5 CONTRASEÑAS DEBILES

Las contraseñas suelen ser una puerta de acceso a los ciberdelincuentes que cuentan con herramientas para capturar las que cuentan con parámetros débiles de seguridad al momento de su creación, luego de obtener acceso al sistema es muy fácil infectar el sistema con malware de todo tipo, exponiendo la información a ser hurtada, compartida o eliminada.

En el siguiente grafico se puede visualizar los métodos y vulnerabilidades más comunes causando infecciones de Ransomware en el 2 cuarto del 2018.

Ilustración 9 métodos y vulnerabilidades más comunes causando infecciones de Ransomware en el segundo cuarto del 2018.



***Fuente**: métodos y vulnerabilidades más comunes causando infecciones de Ransomware en el segundo cuarto del 2018., Trend Micro 2018 Annual Security Roundup, page 11 **Tomado de**: https://www.trendmicro.com/es_es/business.html*

11 RANSOMWARE: PREVENCION

Las siguientes medidas de prevención pueden evitar de manera óptima una infección de Ransomware si se encuentran estipuladas en un plan de seguridad

11.1 BACKUPS

El backup ciertamente es el mejor mecanismo para recuperar la información en caso de una infección, sea en línea o en cintas diarias es importante que no se encuentre mapeada dentro de la red, de esta manera no sería alcanzada por la infección.

También es importante que cuenten con una documentación adecuada para el proceso de backups, teniendo en cuenta que deben ser validados en un ambiente designado para ello.

11.2 CONCIENTIZACIÓN DE LOS USUARIOS

La seguridad es una responsabilidad compartida y por ello es importante siempre contar con mecanismos o procedimientos que ayuden al usuario a familiarizarse con las buenas prácticas de seguridad teniendo en cuenta los protocolos de la organización, al hacer parte al usuario de la importancia de la seguridad de la información, la probabilidad de ser infectado será menor.

11.3 PROTOCOLO DE MÍNIMO PRIVILEGIO

Para el control de privilegios se debe contar con un mínimo para la mayoría de los usuarios, debido a que de esta manera se limita el acceso y el control que el usuario puede ejercer sobre uno o varios directorios, con este control se reduce

significativamente una posible infección a directorios sensibles del S.O, de este mismo modo el número de usuarios root debe ser mínimo.

11.4 SOLUCIONES ANTIVIRUS

Dentro del abanico de herramientas de seguridad se encuentran los antivirus en este caso los especializados en Ransomware son la mejor opción, ya que realizan constante actualizaciones sobre las nuevas variaciones del malware y cuentan con análisis de archivos previo a ser ejecutados, esto también incluye carpetas comprimidas.

12 TAXONOMÍA DEL RANSOMWARE

Hay muchos factores que afectan la clasificación de los Ransomware. Y según su ataque se puede clasificar de la siguiente forma: plataforma de destino, criptosistema utilizado, gravedad de perdida de datos y la estructura de su ataque.

La clasificación basada en la plataforma se puede realizar desde un equipo destino dispositivo móvil y computación en la nube en su perseverancia del ataque debido a su facilidad de implementación en los dispositivos móviles está basado en LOT para sistemas operativos Windows, siendo estos los más susceptibles.

En la computación en la nube se convierte en el nicho de los ransomware el tipo de ataque es dirigido y no discriminado, los criptosistemas tienen una su clasificación en simétricos asimétricos o híbridos en el criptosistema simétrico utiliza se utiliza la misma clave para cifrar y descifrar los datos destinos el proceso asimétrico de los sistemas criptográficos se utilizan con la clase publica se utiliza para cifrar los datos destino mientras la clave privada se utiliza para el descifrado.

Y el cifrado híbrido es una alternativa ya que utiliza la velocidad de los criptosistemas y la resiliencia de los criptosistemas asimétricos considerando que el cifrado es el núcleo del modelo del ransomware.

En términos de estructura de ataque identificado por claves, la única clave pública híbrida sería la clave simétrica y pública y el proceso de eliminación de archivos que sobre escribe el archivo original después del cifrado o primitivamente lo elimina, siendo para la recuperación de datos un ataque.

Basado en la gravedad se encuentra el scareware, que no daña ni elimina los archivos, sólo engaña de una forma u otra. Locker ransomware bloquea el inicio

de sesión del sistema o el menú de arranque y el Detrimental ransomware encripta el objetivo de los archivos originales remanentes después del cifrado.

El resultado de esta categorización se encuentra en la siguiente figura:

Ilustración 10 Taxonomía del Ransomware

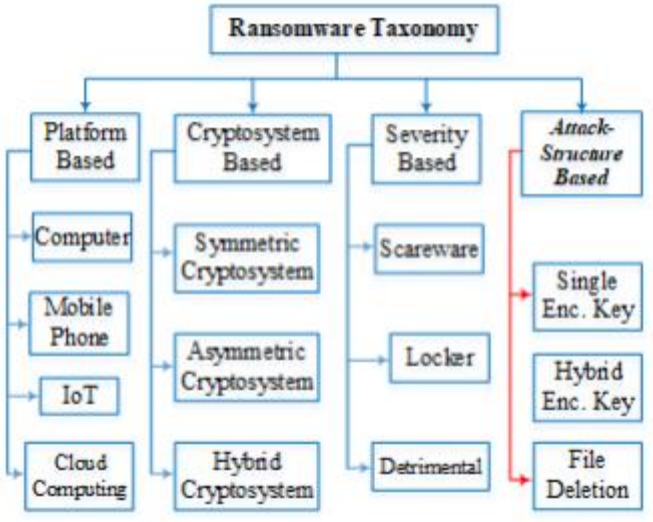


Ilustración *Taxonomía del Ransomware* ***Fuente:*** *ZIMBA, Aarón. CHISHIMBA, Mumbi. CHIHANA, Sipiwe. "A Ransomware Clasificación Framework Based on File Deletion and File Encryption Attack Structures". {En línea}. Junio de 2019. {Febrero 20 de 2020} disponible en: (https://www.researchgate.net/publication/333966134_A_Ransomware_Classification_Framework_Based_on_File-Deletion_and_File-Encryption_Attack_Structures)*

13 TÉCNICAS DE DETECCIÓN

13.1 MACHINE LEARNING

Según SAS Analytics Software & Solutions define “ método de análisis de datos que automatizan la construcción de modelos analíticos, es una rama de la inteligencia artificial basada en la idea de que los sistemas pueden aprender de los datos identificar patrones y tomar decisiones con una mínima intervención humana “

De esta forma los ordenadores algoritmos especiales Ml para usar los datos que reúnen y recopilan la información

Ilustración 11 Técnicas de detección y prevención Ransoware

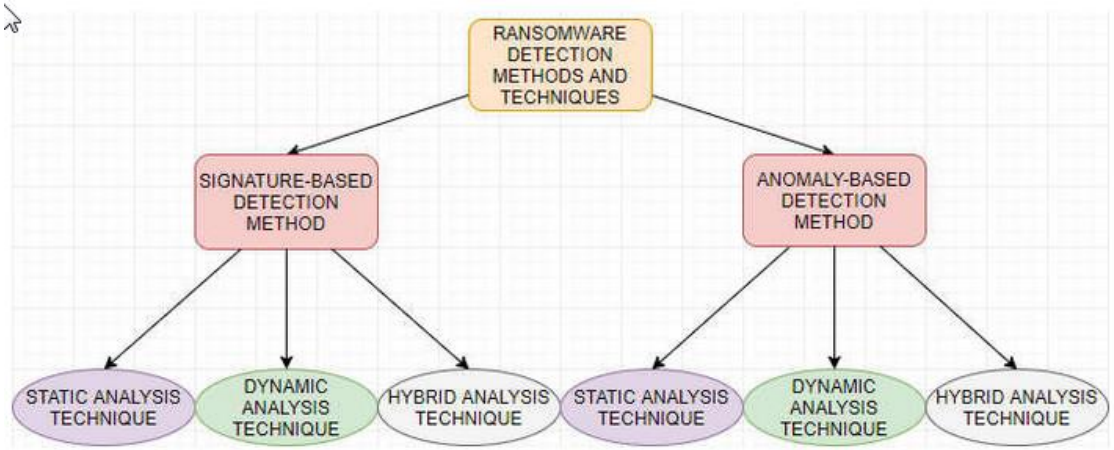


Ilustración *Técnicas de detección y prevención Ransoware* ***Fuente****: CELIKTAS, Baris. UNLU, Nafis. KARACUHA, Ertugrul. “Ransomware, Detection and Prevention Techniques, Cyber Security, Malware Analysis”. {En línea} Mayo de 2018. {Enero 18 de 2020} disponible en: (https://www.researchgate.net/figure/Ransomware-Detection-Methods-and-Techniques-45_fig11_326191046)*

13.2 DETECCIÓN DE FIRMAS:

Es una de las técnicas estándar para la identificación de malware, cada uno de este tipo tiene incluida la firma para saber cómo detectar la amenaza. Se hace la comparación de la firma digital como la huella digital permitiendo al software identificar al malware su funcionamiento es 100% en la base ransoware conocido ósea que si opera uno nuevo no va hacer identificado

13.3 DETECCIÓN DE TRÁFICO ANORMAL:

Esta técnica de análisis de tráfico tiene particularidad de métricas de funciones diferentes para la detección de intrusos y detección de tráfico que puedan relacionarse como maliciosas una de la gran desventaja de esta técnica que es captura tráfico legal o bueno y lo clasifique como malicioso

13.4 DETECCIÓN DE COMPORTAMIENTO DE ARCHIVO

Esta técnica podría clasificarse dentro del método de análisis de datos para el ransoware petya, la ejecución legitima del código normal de los archivos tienen un cierta definición cantidad de estructura en su tipo de comportamiento los algoritmos Ml Involucran esa depuración masiva o análisis de ejecución de código post modem, permitiendo la identificación origen del archivo que contiene la malware

Una característica fundamental de machine learning son las líneas de base normal que se recopila el funcionamiento normal y todo la actividad diaria de ejecución como se presentaría en una actividad normal inicio de sesión cierre de sesión tráfico de archivos modificación de nombres así sucesivamente una vez se reúna la base de la línea normal se puede identificar de manera efectiva las anomalías.

13.5 SISTEMA DE ANALISIS DE COMPORTAMIENTO

Otra de las técnicas para identificar el ransoware su objetivo es centrado en el comportamiento de archivo su protección se basa en que no progrese la infección sobre el sistema de archivos identificando cambios realizados

13.6 HONEYPOT

Esta técnica conocida como “sistema de trampa” su objetivo principal se basa en evitar los ataques al sistema informático con la función detectar y obtener información del ransoware identificando su procedencia para después tomar las medidas de seguridad. Dentro de sus herramientas están las alertas obtener información ralentizar el ataque y combinación un ejemplo de uso es implementar una red Honeypot

Ilustración 12 Red Honeypot

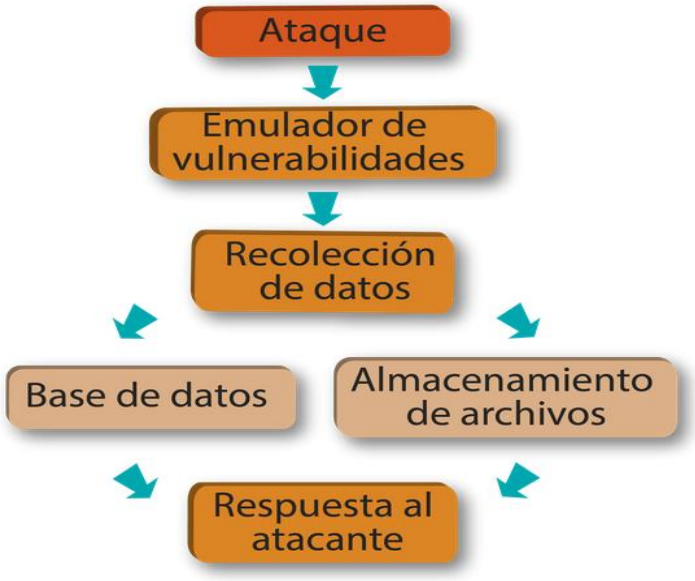


Ilustración *Honeypot,* ***Fuente:*** *ESPINOSA, Oscar. “Qué es y para qué sirve un Honeypot”. {En línea} {Marzo 8 de 2020} disponible en: (https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/).*

Se utiliza en la explotación de réplica conocida y los vectores de ataque de malware, con la verificación de existencias de modificaciones

13.7 STATISTIC

Esta técnica su enfoque se puede utilizar para analizar los rescates para entender sus características más importantes para su implementación tocaría

coger la interpretación de sus variantes e identificarlos en métodos estadísticos que permitan definir lo que conlleva más al ataque del malware.

13.8 USO DE HONEYPOT PARA DETECTAR EL RANSOWARE

La herramienta Cybersight Ransomstopper diseñada para prevenir y combatir anti-ramsoware en sistema operativos Windows permitiendo impedir la infección mediante ransoware, antes de que este tenga lugar.

El funcionamiento se basa en el principio de crear un **honeypot** (poner algo en el disco que traiga la atención del malware en primer lugar) para a partir de ahí estudiar lo que hace en el señuelo y tomar decisiones características que se encuentran:

Prevención: aplicación aprendizaje computacional durante la pre-ejecución de los archivos para impedir la ejecución en el equipo.

Engaño: los honeypots y trampas “en aperturas” se usan para cazar el ransoware antes de toque algo de valor

Detección: análisis de comportamiento del kernel y procesos/archivos en tiempo real.[12]

[12] PROTEGER MI PC. “Protección frente al ransomware en Windows con Cybersight Ransomstopper”. {En línea}. Diciembre 28 de 2018. {Marzo 3 de 2020} disponible en: (https://protegermipc.net/2017/12/28/cybersight-ransomstopper/).

14 RANSOMWARE: LABORATORIO PETYA

14.1 AMBIENTE CONTROLADO

El ambiente controlado de pruebas se realiza utilizando virtual box (máquina virtual) en un entorno con sistema operativo Windows 10, que nos permite virtualizar el sistema operativo es decir crear en el equipo anfitrión un equipo virtual para ello se debe configurar para que no exista alguna propagación del malware a utilizar o se propague por la red al equipo anfitrión.

La Configuración del entorno de red es por donde se intercambia la información para ello se bloqueará la salida de internet, deshabilitar el uso compartido entre la máquina virtual y el equipo anfitrión, deshabilitar la conexión de puertos USB en la máquina virtual y mantener actualizado el software de virtualización en este caso la máquina virtual. Las anteriores configuraciones de seguridad se realizarán cuando se ejecute el malware.

14.1.1 IMPLEMENTACION DEL ENTORNO VIRTUALIZADO

Ilustración 13 Configuración entorno de red en virtual box modo puente (Bridged)

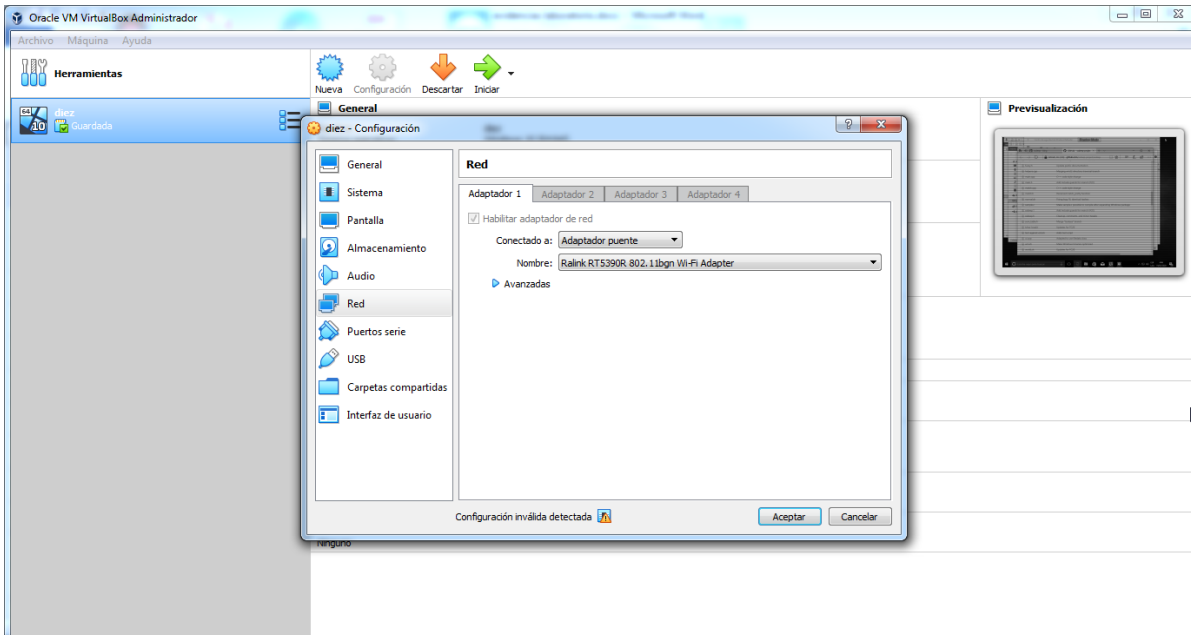


***Ilustración**: configuración entorno de red en virtual box modo puente, **Fuente:** Los Autores, este documento*

Ilustración 14 Sin habilitación de puertos Usb para mayor seguridad

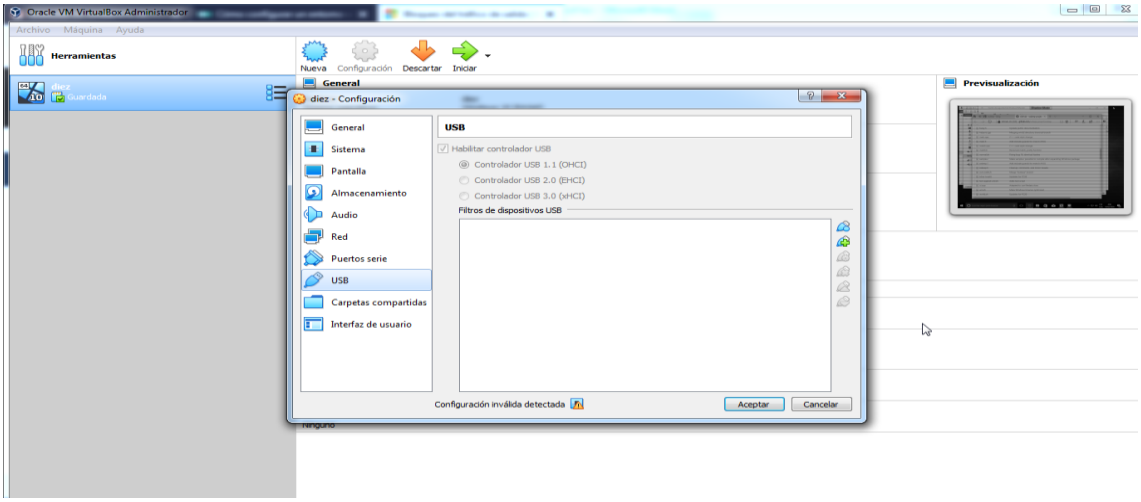
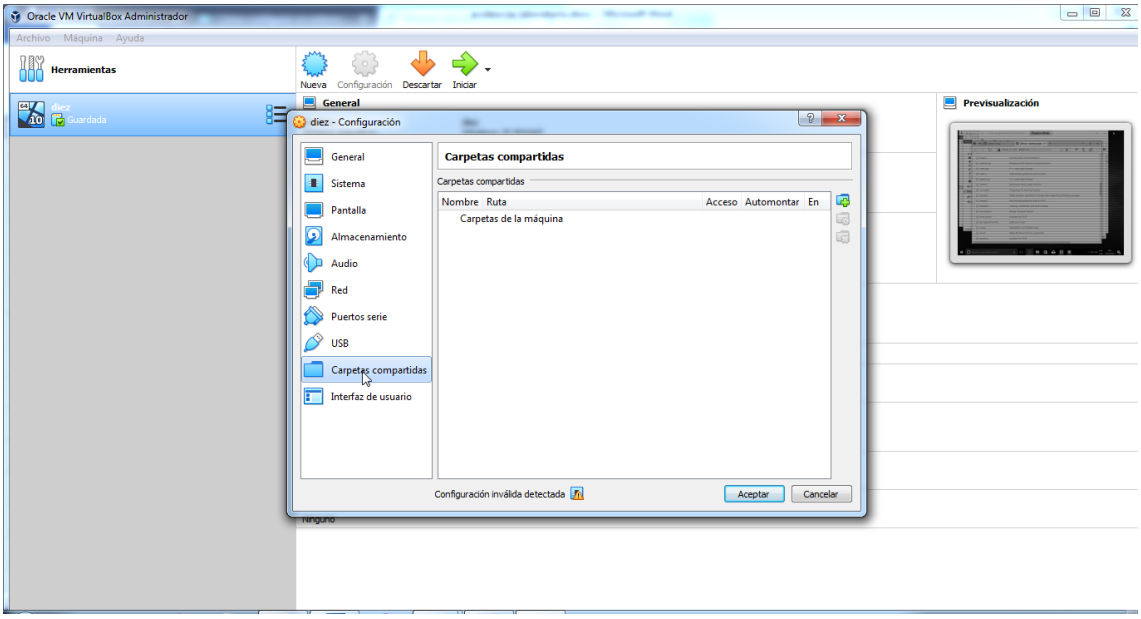


***Ilustración** sin habilitación de puertos Usb para mayor seguridad **Fuente:** Los Autores, este documento*

Ilustración 15 Sin uso de carpetas compartidas para evitar propagación del malware la equipo anfitrión

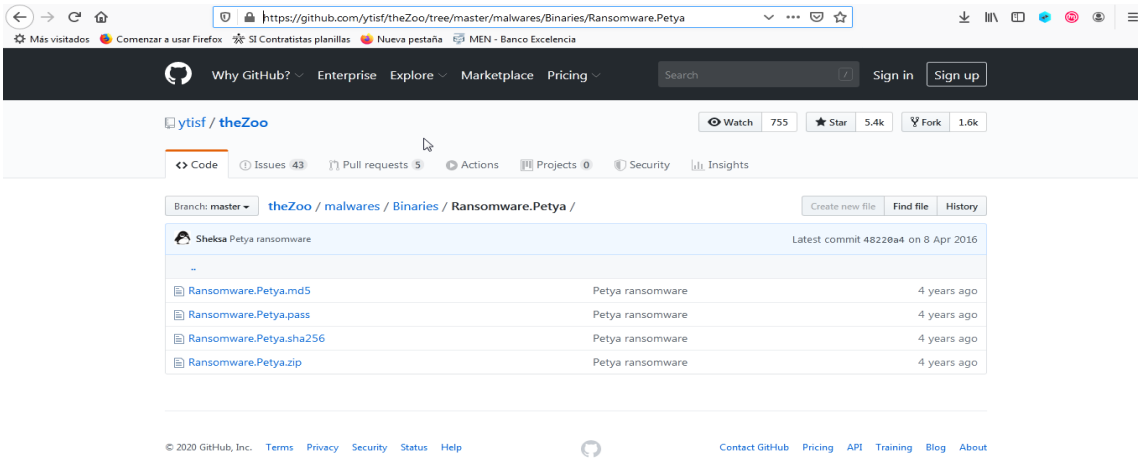


Fuente: Los Autores, este documento

14.2 FUENTE Y MUESTRA DEL RANSOMWARE PETYA

El Ransoware a ejecutar en el ambiente de prueba es Petya, la fuente de descarga es del repositorio de GITHUB: https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Ransomware.Petya. El contenido del repositorio se encuentra en .md5 .pass .sha256 .zip este último formato para ser descomprimido y obtener sus archivos su contraseña es: infected

Ilustración 16 Repositorio de Ransomware



Fuente: *Repositorio de malware Petya / GITHUB,2016* ***Tomando de: https://github.com/hasherezade/petya_recovery***

Para el siguiente laboratorio se utilizó una máquina virtual para simular el funcionamiento de la maquina víctima, en este caso un Windows 10 de igual manera se creó la siguiente cuenta en Gmail: unadtesting@gmail.com para la recepción del archivo infectado.

El archivo infectado usado en el siguiente laboratorio se descargó directamente de un repositorio de malwares de Github con fines educativos.

El servicio que se utiliza para el envío del archivo es WeTransfer. Este servicio permite el envío de archivos sin contar con una dirección de remitente existente.

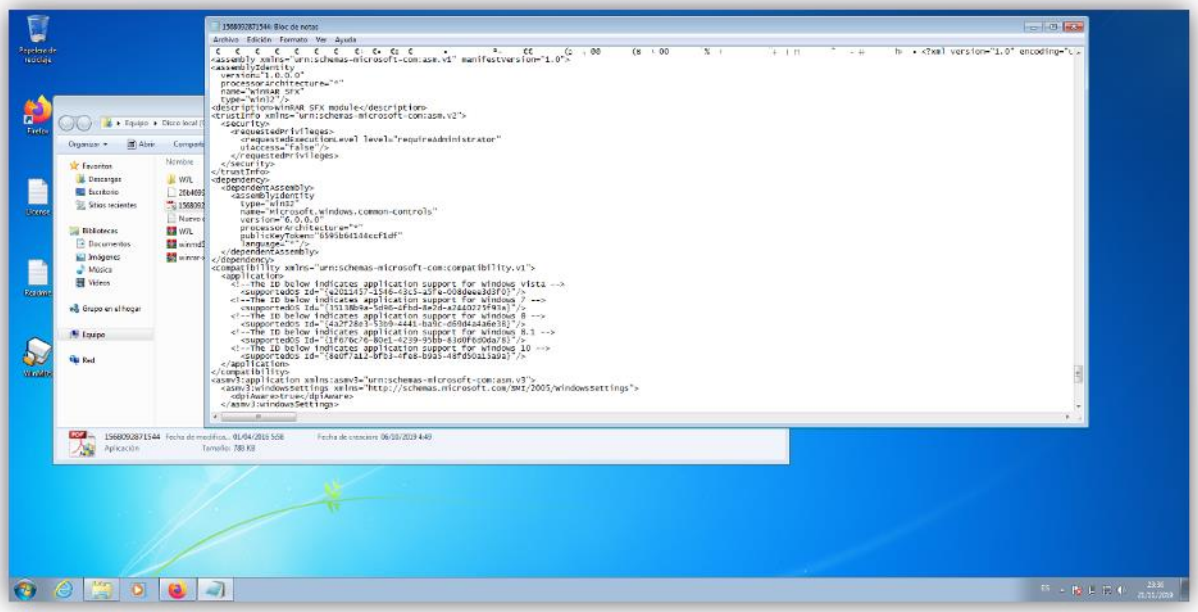
Se inicia enviando el archivo infectado camuflado como un archivo .PDF a la cuenta de Gmail previamente creada, se puede observar que la imagen cuenta

con un asunto falso y a su vez la cuenta de email del remitente parece ser de una empresa de cotizaciones.

En la siguiente imagen se visualiza que el código del archivo en efecto no se trata de un .PDF, sino que, por el contrario, trae un programa que se activará al ejecutar el archivo.

En esta máquina virtual se puede apreciar la carencia de aplicaciones de seguridad integrales que brinden un monitoreo constante sobre el flujo de la información que viaja a través de la red, tampoco cuenta con protocolos de acceso privilegiado y no hay ningún tipo de scanner ejecutándose en tiempo real lo que forma parte de una gran serie de vulnerabilidades.

Ilustración 17 Código Fuente del archivo infectado

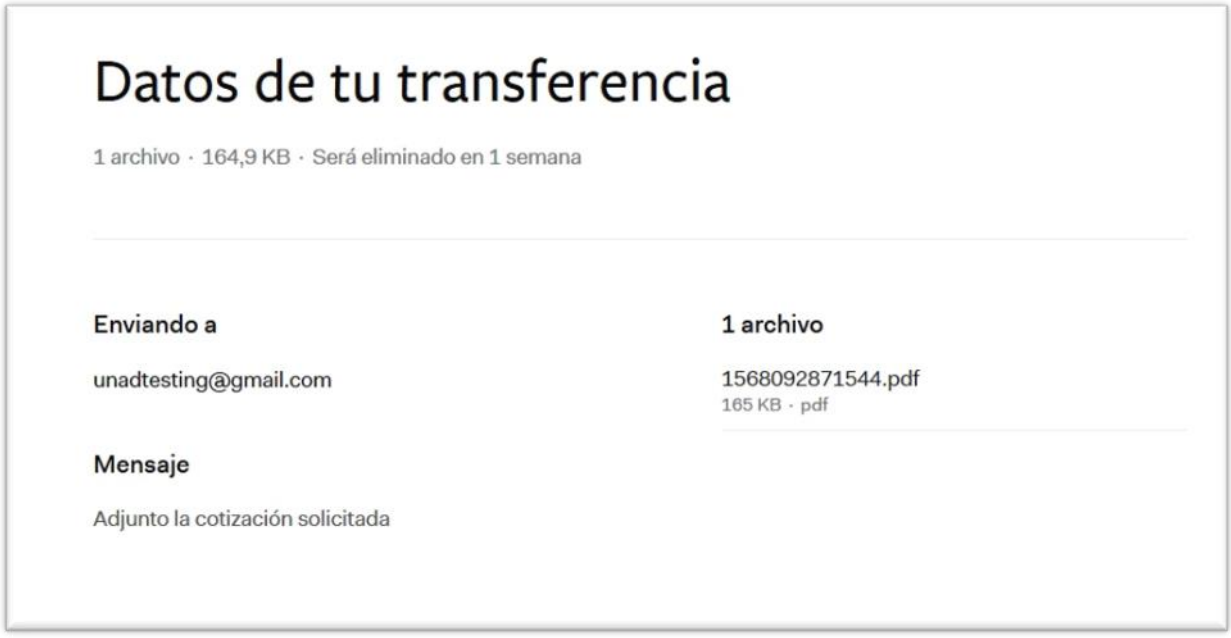


Fuente: Los Autores, este documento

Ilustración 18 Envió del email con el Ransomware como adjunto

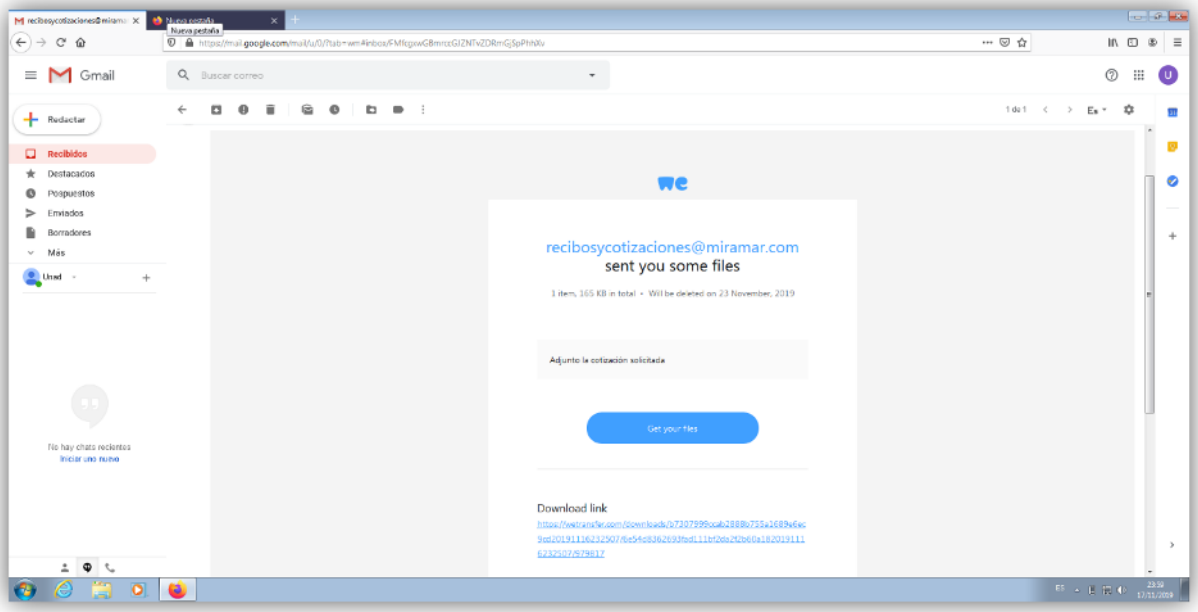
Fuente: Los Autores, este documento

Ilustración 19 Envió del archivo ha sido satisfactorio



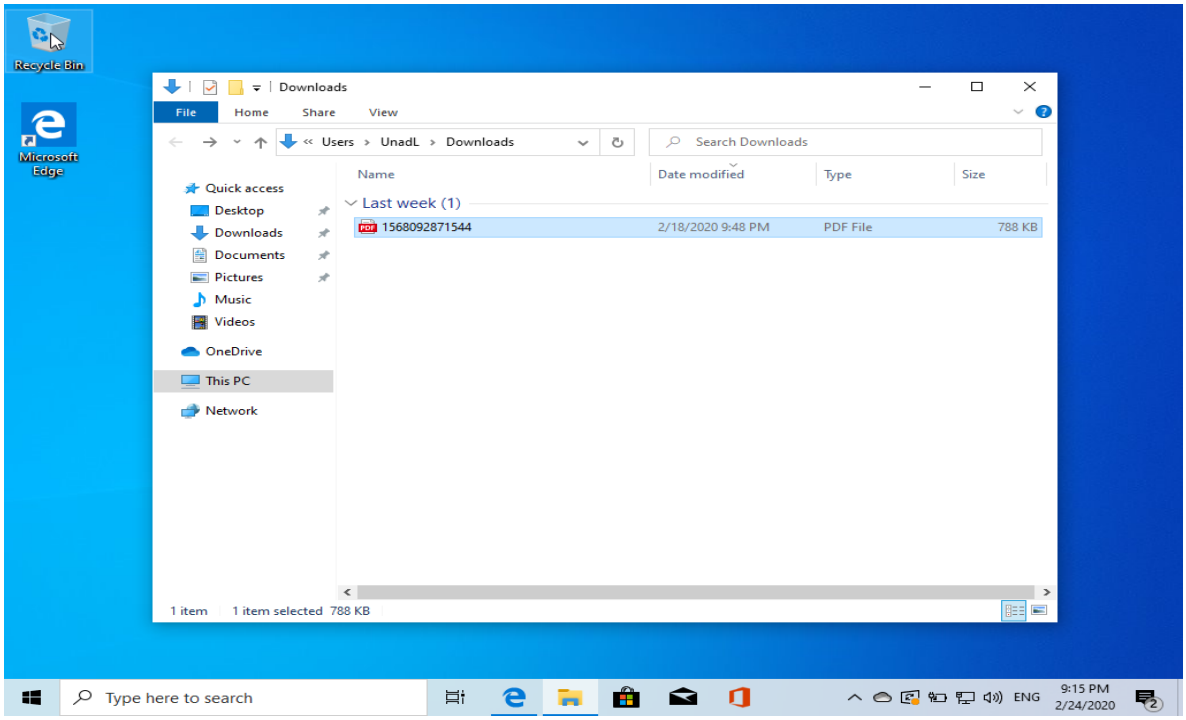
Fuente: Los Autores, este documento

Ilustración 20 La victima abre el correo



Fuente: Los Autores, este documento

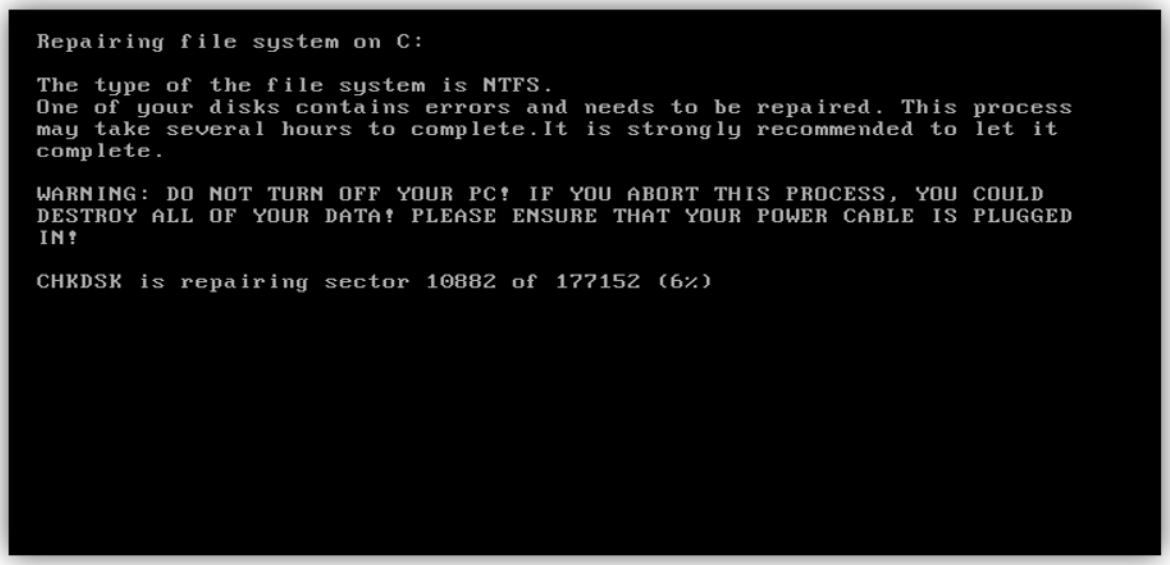
Ilustración 21 El usuario procede a descargar el archivo y a ejecutarlo



Fuente: Los Autores, este documento

Después de su actuación sobre este primer sector del disco duro el MBR al reiniciar o encender el ordenador su primer mensaje de ejecución es originado con el comando CHKDSK donde informa sobre una advertencia al usuario e errores en el disco y debe ser reparado mientras completa su secuencia en ese mismo preciso momento el ransomware está realizando su encriptación sobre la tabla de particiones en este caso el falso mensaje es para poder tener tiempo para realizar su encriptación .

Ilustración 22 El sistema se reinicia y empieza a encriptar el sistema con el Ransomware



Fuente: Los Autores, este documento

Al finalizar su proceso aparece el típico mensaje de color (rojo), donde informa al usuario que su información ha sido encriptado y la forma como puede recuperarla y no intentar recuperarla por sus medios ya que solo se puede recuperar a través de la llave especial para desencriptar a través de un pago. De esta forma el usuario se ve obligado a pagar por la llave para poder descifrar los datos si no accede la información se pierde.

Para lograr infectar el ordenador se necesita una ejecución de programas en el sistema operativo de la siguiente manera:

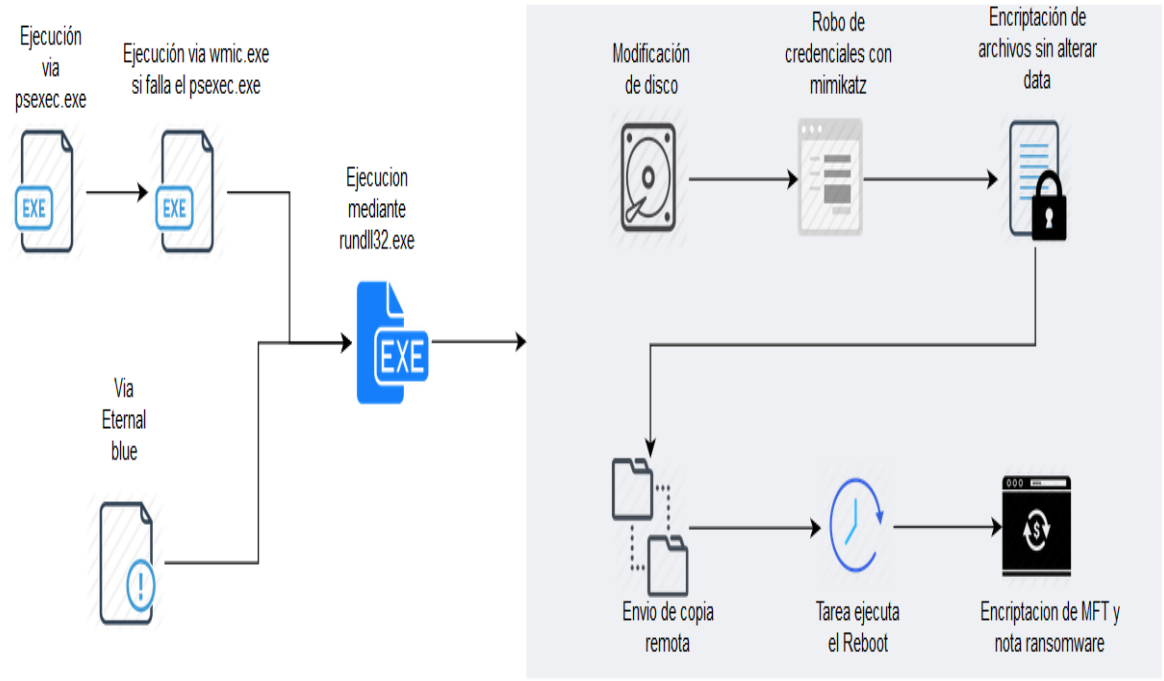
Después de ejecutarse el virus, ingresa al equipo por una herramienta denominada psexesvc.exe, este proceso en el equipo es el encargado de ejecutar otro proceso remotamente si este proceso falla también se aloja en el proceso wmiprvse.exe el cual sirve para administrar servicios clientes en el sistema operativo, ósea que se activamente automática mente cuando el cliente este utilizando para monitorear servicios o procesos, este virus no solo lo utiliza para ingresar si no para también controlar procesos y servicios y además para copiarse estos archivos si están en una red el equipo víctima, después el virus se aloja en el equipo como PERFC.DAT con ese archivo se apodera de los .DLL del sistema operativo como :rundll32 para cifrar los archivos.

Antes de cifrar los archivos extrae información del sistema infectado a través de la herramienta llamada Minikatz esta herramienta se encarga de extraer nombre de usuario y contraseñas en texto plano que se ubica en la sección de los directorios del Ransoware, si fuera el caso de que el usuario lo detecte y lo elimine. Después ya procede a Cifrar los datos verificando primero que antivirus tiene instalado y si está instalado, de ser así lo coloca en código el malware con el fin de que el antivirus vaya a actuar para eliminarlo.

El malware sobrescribe el MBR, pero no encripta la tabla maestro de archivos que almacena todos los metadatos, archivos, directorios, permisos, fecha de creación y se puede recuperar los datos siempre que haya una copia de seguridad del MBR.

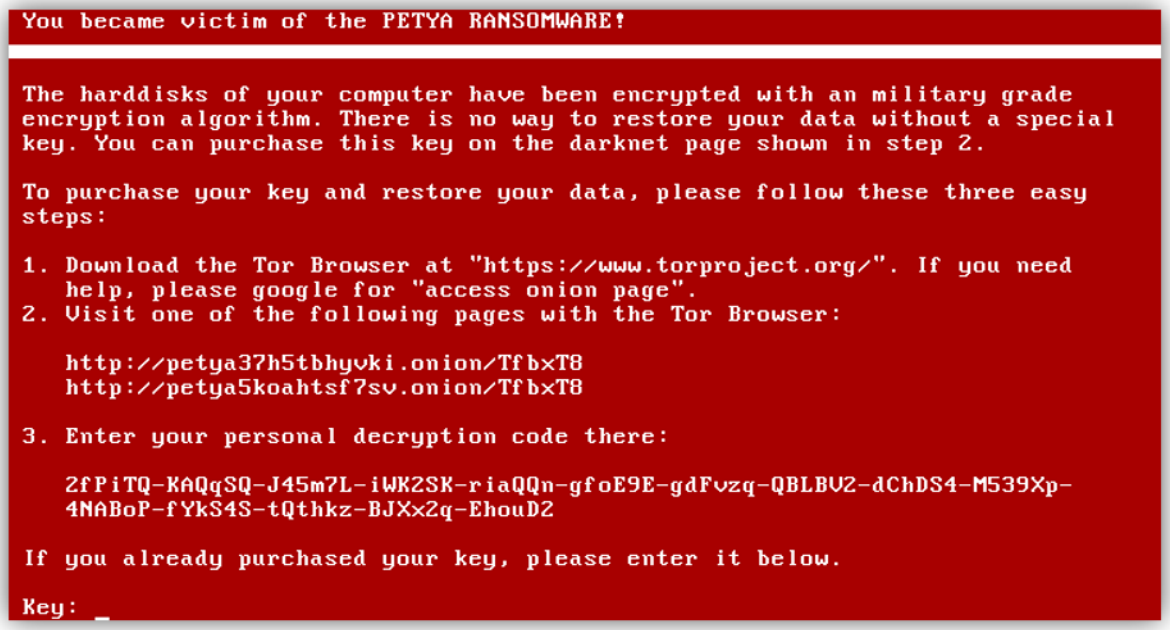
En el caso que no haya instalado un antivirus el malware sobre escribe todos los sectores de arranque

Ilustración 23 Proceso de Infección



Fuente: Los Autores, este documento

Ilustración 24 El acceso al sistema es bloqueado.



Fuente: Los Autores, este documento

Al momento de encriptar la información, se bloquea totalmente el acceso al sistema operativo. Posteriormente se realiza un análisis del archivo infectado para ver la naturaleza del Malware.

Tipos de archivos que el ransomware encripta en el sistema.

Ilustración 25 Lista de Extensiones

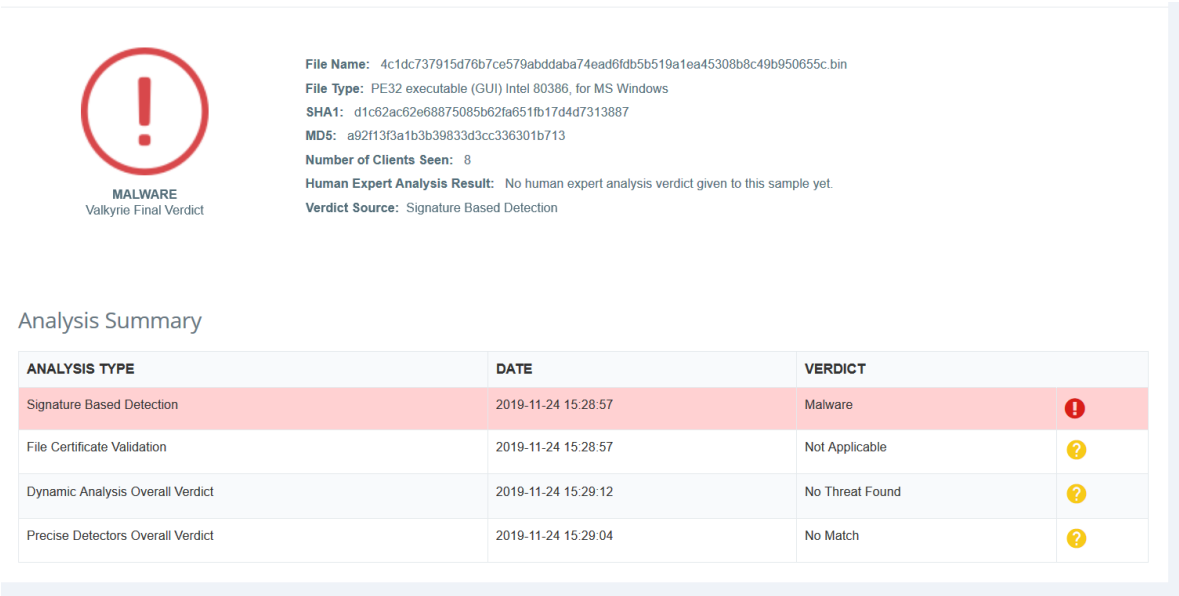
.3ds	.7z	.accdb	.ai	.asp	.a	spx	.avhd	.back	.bak
.c	.cfg	.conf	.cpp	.cs	.ctl	.dbf	.disk	.djvu	.doc
.docx	.dwg	.eml	.fdb	.gz	.h	.hdd.	dbx	.mail	.mdb
.msg	.nrg	.ora	.ost	.ova	.ovf	.pdf	.php	.pmf	.ppt
.pptx	.pst	.pvi	.py	.pyc	.rar	.rtf	.sln	.sql	.tar
.vbox	.vbs	.vcb	.vdi	.vfd	.vmc	.vmdk	.vmsd	.vmx	.vsdx
.vsv	.work	.xls	.xlsx	.xvd	.zip				

Fuente: Los Autores, este documento

Los archivos están encriptados con el algoritmo AES-128. Una clave AES se usa para cifrar archivos de una sola unidad. La clave AES-128 utilizada para el cifrado de archivos se cifra con el algoritmo de cifrado RSA-2048. La clave pública utilizada para RSA está presente en binario en forma codificada en base64.

Para ello se usó la herramienta forense llamada Valkyrie que permitió hacer una evaluación bastante completa de toda clase de archivos.

Ilustración 26 Análisis con herramienta forense Valkyrie



Fuente: Los Autores, este documento

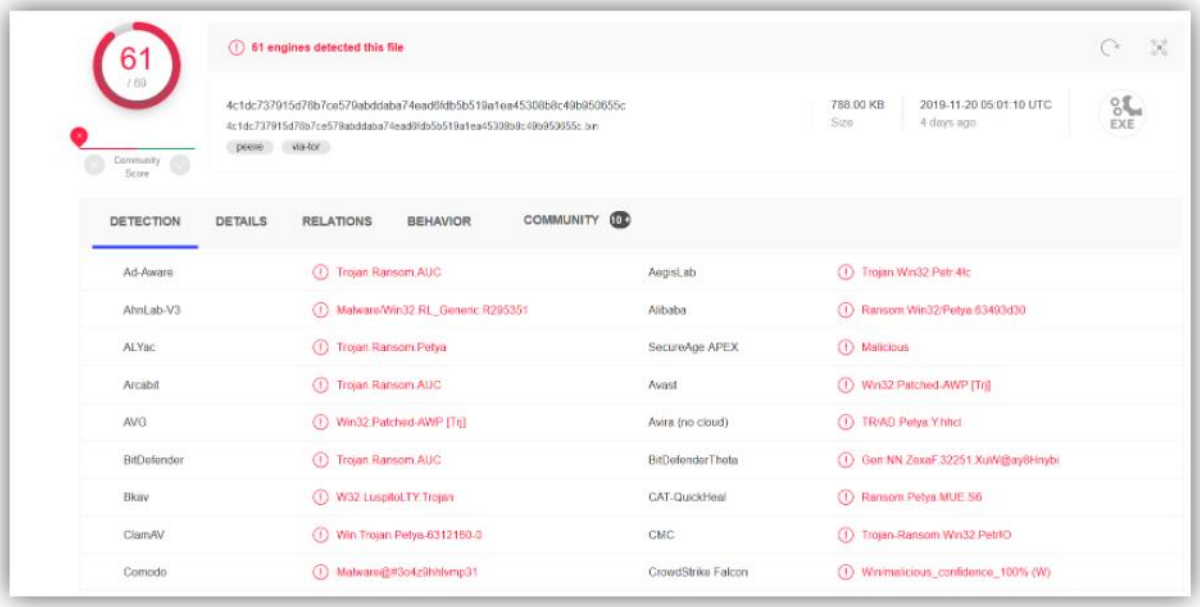
En este archivo se puede visualizar claramente que el análisis refleja, que en efecto el archivo .PDF contiene un malware y a su vez, revela el hash del mismo, que en este caso es: d1c62ac62e68875085b62fa651fb17d4d7313887.

Con este hash se puede llevar a cabo otro análisis en un portal web dedicado al análisis de virus y malware.

Ilustración 27 Portal VirusTotal

Fuente: Los Autores, este documento

Ilustración 28 Reporte VirusTotal

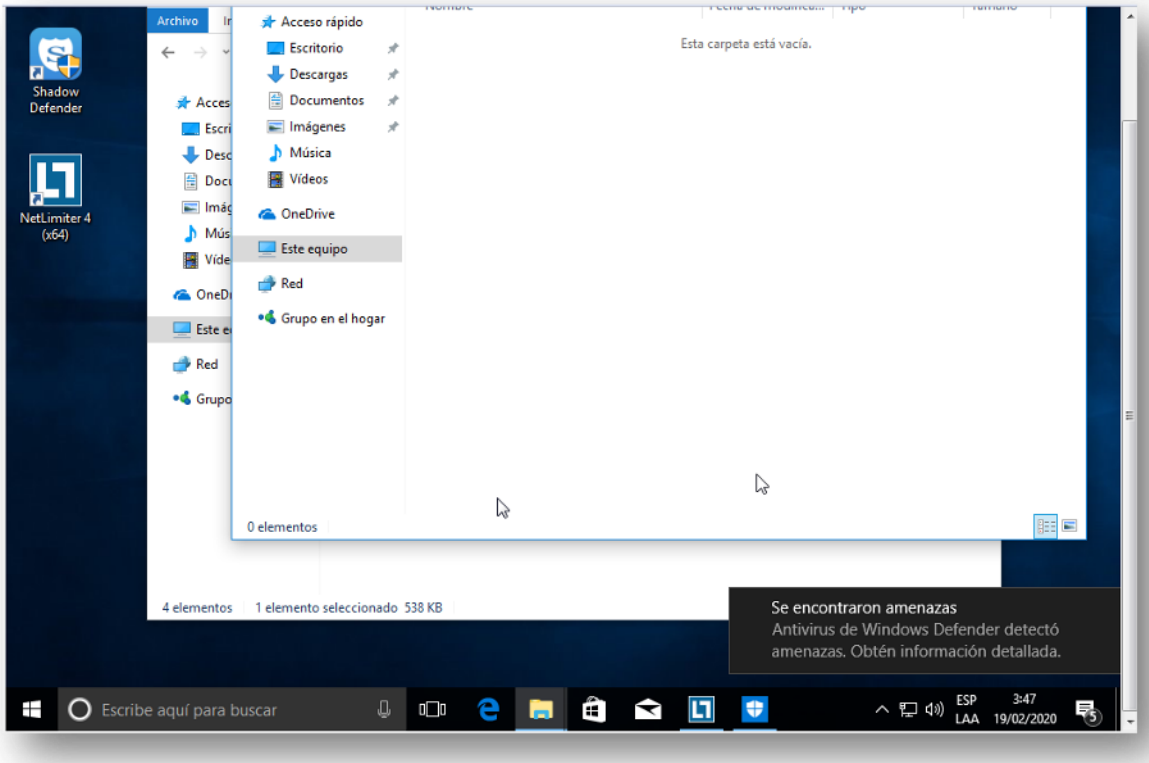


Fuente: Los Autores, este documento

En el reporte generado por VirusTotal se evidencia claramente el tipo de malware que es, haciendo referencia al PETYA. Además, se evidencia el nombre con que es detectado en diferentes antivirus.

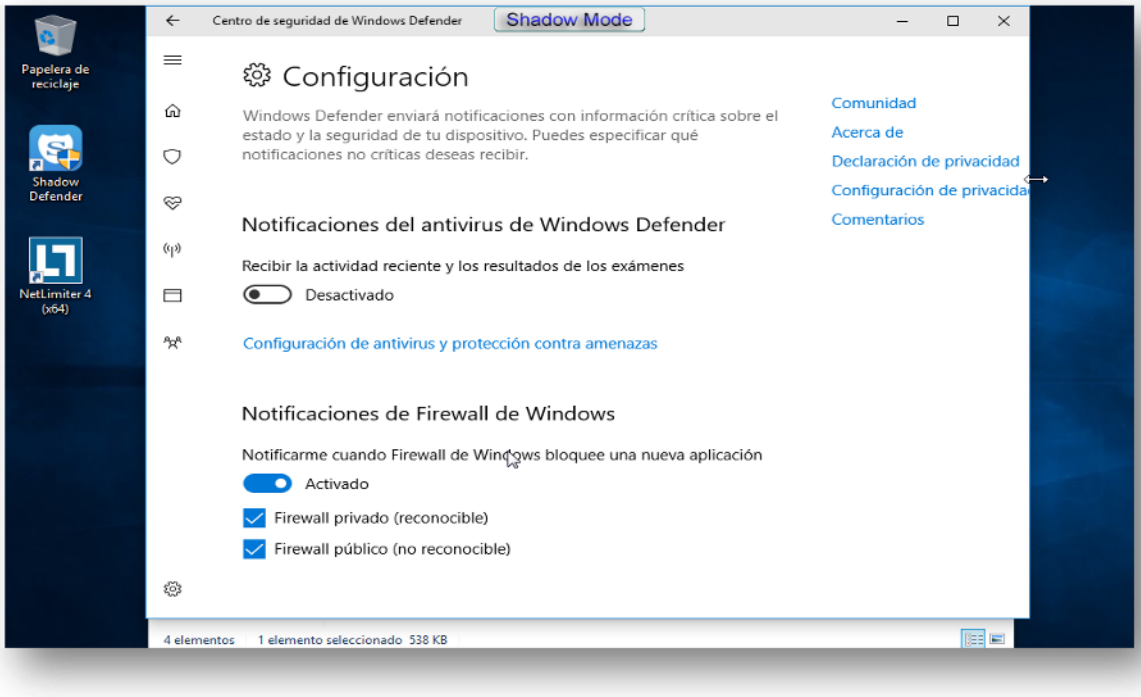
Se procede a realizar el analisis con Windows defender desde el momento que se descomprime archivos

Ilustración 29 Windows defender detecta amenazas al momento de descomprimir



Fuente: Los Autores, este documento

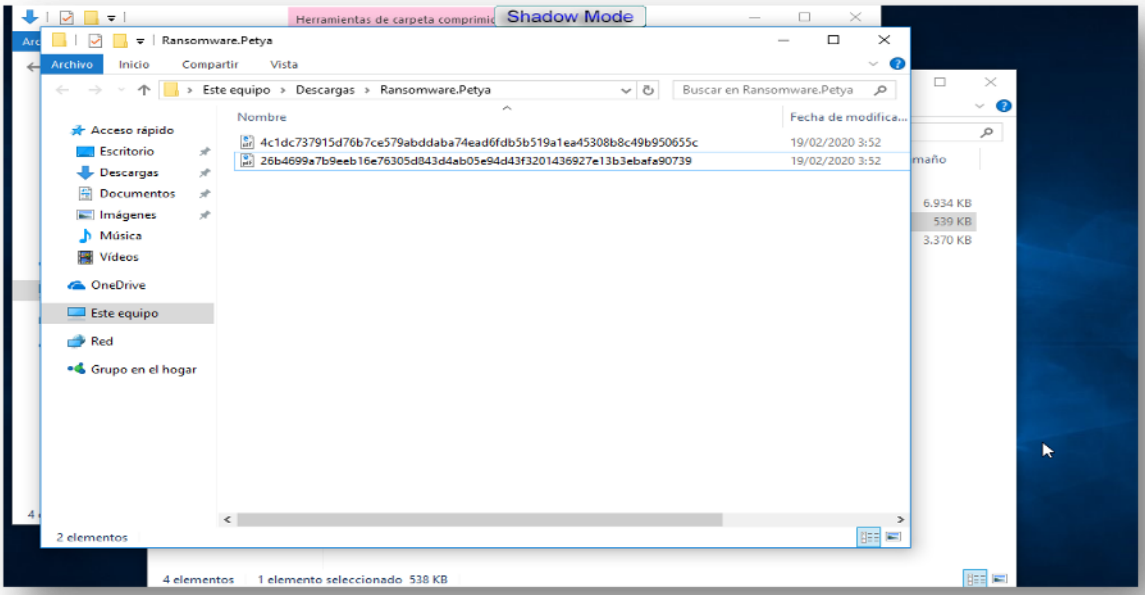
Ilustración 30 Configuración predeterminada de Windows defender



Fuente: Los Autores, este documento

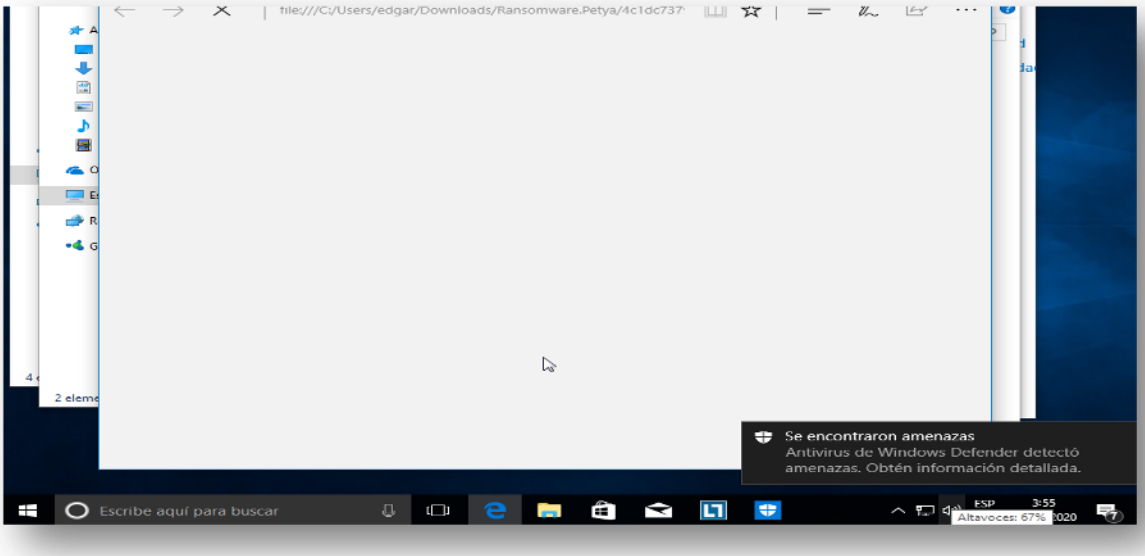
Archivos de contenido del código malicioso de petya listo para su ejecución , estos archivos tiene la extensión .bin y pueden ser modificado a .exe o formato de texto como .pdf para su actuar en el equipo

Ilustración 31 Archivos infectados



Fuente: Los Autores, este documento

Ilustración 32 Restricción y alerta de archivos sospechosos descargados

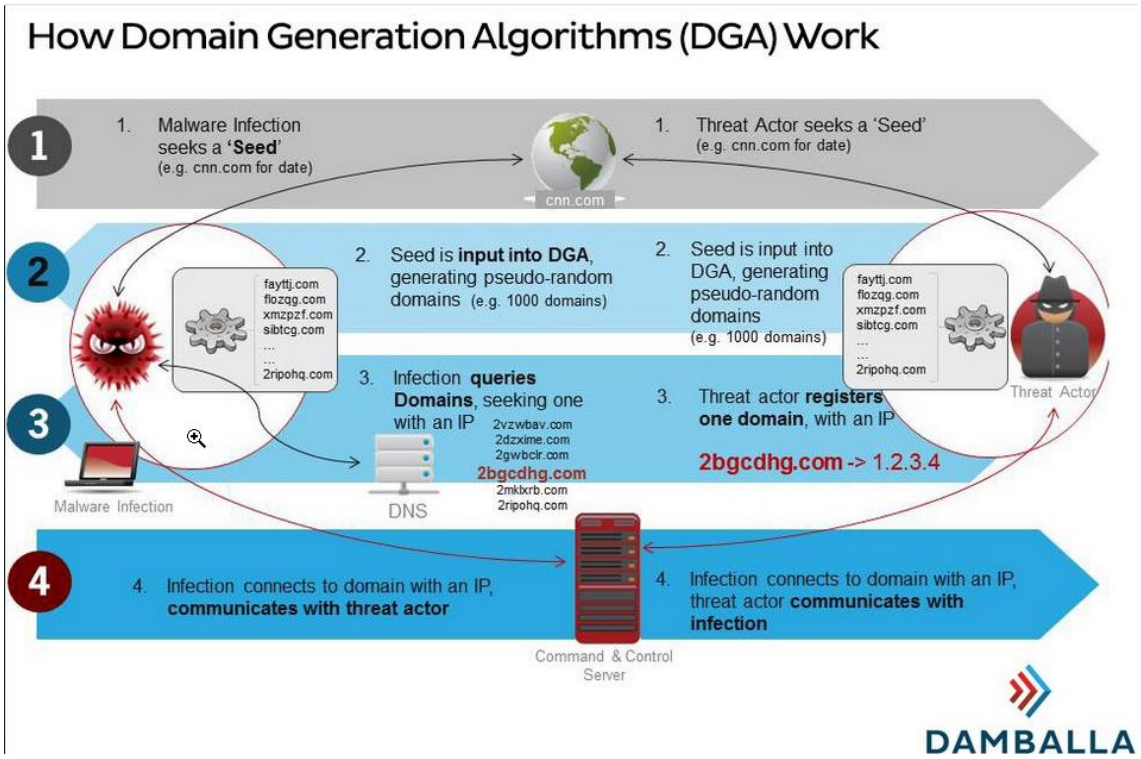


Fuente: Los Autores, este documento

14.3 USO DE SERVIDORES DE COMANDO Y CONTROL (C & C)

Es un servidor centralizado que los atacantes en línea utilizan para emitir comandos para tener control sobre los malwares, bots, rootkits y recibir toda recepción de capturas de ellos. Su utilidad se centra en crear redes de computadores infectados y ejecutar acciones dañinas como: robar, eliminar, encriptar datos y pagos por su rescate, este tipo de servidores utilizan algoritmos de generación de dominios para que se haga difícil su detección.

Ilustración 33 DGA



Fuente: *RAMÍREZ, Adrián. "How Domain Generation Algorithms (DGA) Work". {En línea} {Enero 8 de 2020} disponible en: (https://www.adrianramirez.es/wp-content/uploads/2016/05/How-DGA-work.png).*

14.3.1 FASES ALGORITMO GENERACIÓN DE DOMINIO (DGA)

1. se genera una semilla utilizada por el malware para crear dominios aleatorios.
2. Se Inserta el algoritmo (DGA) en el malware para que con la primera fase se generen los dominios
3. El equipo víctima se conectará a cada dominio pero solo uno será válido y se habrá registrado de forma manual por el atacante con datos falsos
4. El atacante tiene control sobre el Bonet sin ser detectado ya que puede ser dinámico.

Ilustración 34 Código para generar dominios

```
def generate_domain(year: int, month: int, day: int) -> str:
    """Generate a domain name for the given date."""
    domain = ""

    for i in range(16):
        year = ((year ^ 8 * year) >> 11) ^ ((year & 0xFFFFFFF0) << 17)
        month = ((month ^ 4 * month) >> 25) ^ 16 * (month & 0xFFFFFFF8)
        day = ((day ^ (day << 13)) >> 19) ^ ((day & 0xFFFFFFFE) << 12)
        domain += chr(((year ^ month ^ day) % 25) + 97)

    return domain + ".com"
```

***Fuente**: WIKIPEDIA. "Domain generation algorithm". {En línea}. {Enero 13 de 2020} disponible en: (https://en.wikipedia.org/wiki/Domain_generation_algorithm).*

La detección de este tipo de cifrado es muy compleja debido a que su uso puede ser para proteger información como redes bancarias o si se usa con fines de enmascarar la comunicación con servidor C&C cuando se utiliza esta comunicación es necesario que la red la victima tenga funcionalidades adicionales para analizar el tráfico de la red, el malware se ejecutara sin ser detectado hasta que se descubran los servidores y se adiciones a las listas negras de direcciones ip y dominios maliciosos.

14.4 ENCRIPCION DE ARCHIVOS Y CRIPTOGRAFIA

El ransomware utiliza una combinación de criptografía simétrica y asimétrica para lograr su objetivo. Se utiliza una clave simétrica estándar de cifrado avanzado (AES) para cifrar los archivos de la víctima. Esta clave se encripta con la clave pública del atacante y se almacena en el sistema o se entrega al servidor de C&C del atacante. La clave simétrica no cifrada se elimina del host para garantizar que la víctima no pueda descifrar los archivos sin pagar el rescate. En algunos casos, como Petya y PetrWrap, la criptografía de clave elíptica se implementa en lugar de Rivest-Shamir-Adleman (RSA) como el esquema de clave pública.

El pseudocódigo presentado a continuación muestra el proceso de cifrado de archivos realizado por ransomware común que implementa una metodología de cifrado híbrido en un host de Windows. La clave simétrica AES se genera en el sistema host utilizando CryptoAPI en el host, y luego los archivos se cifran con esta clave. La clave se almacena de forma segura en el host cifrándola con una clave pública RSA asimétrica que se envió con el ransomware. La clave no cifrada se destruye. Luego se muestra una nota de rescate para el usuario con instrucciones de pago.

```
//Pseudo Código para encripción de archivos
{
HCRYITKEY generateKey(hProv) //Manejador de llave
HCRYETKEY symmetricKey;
CryptGenKey(hProv, CALG_AES_2S6, Iu, &symmKey); // genera AES-256 llave
return symmetric Key;                          // retorna llave generada


}

void encryptUserData(hProv, symKey) {
for every file type FTYPE:     // busca por tipos de archivos especificos
    encryptuserFIIe(hProv. symKey);            // encripta archivos
}

Void houseKeeping(hProv, symKey) {
HCRYPIKEY asymmetricpubKcy = getasymmetricPubKey(hProv): // obtiene llave
publica RSA
void* encryptedsymKcy = exponKey(symKcy, asymmetricpubKey);//  encripta y
codifica llave AES

LocalFree(encryptedsymKey);       // elimina traces de llave simetrica
}

void encryption_thread() {   // main function

HCRYPTKEY symKey;
symKey = generateKey(hProv);   // llamado a la function de generado de llave
encryptUserData(hProv, symKey); // llamado a la function de encriptado
houseKecping(symKcy);       // limpieza houseKecping
CryptDcstroyKey(symKey);       // Eliminar de la llave en memoria
CryptReIeaseContext(hProv, O); // liberar manejador a CSP

}
```

14.5 MÉTODOS DE ENCRIPTACIÓN DE DATOS

Los módulos de cifrado estándar que utilizan las familias de ransomware podrían dividirse en las siguientes tres categorías:

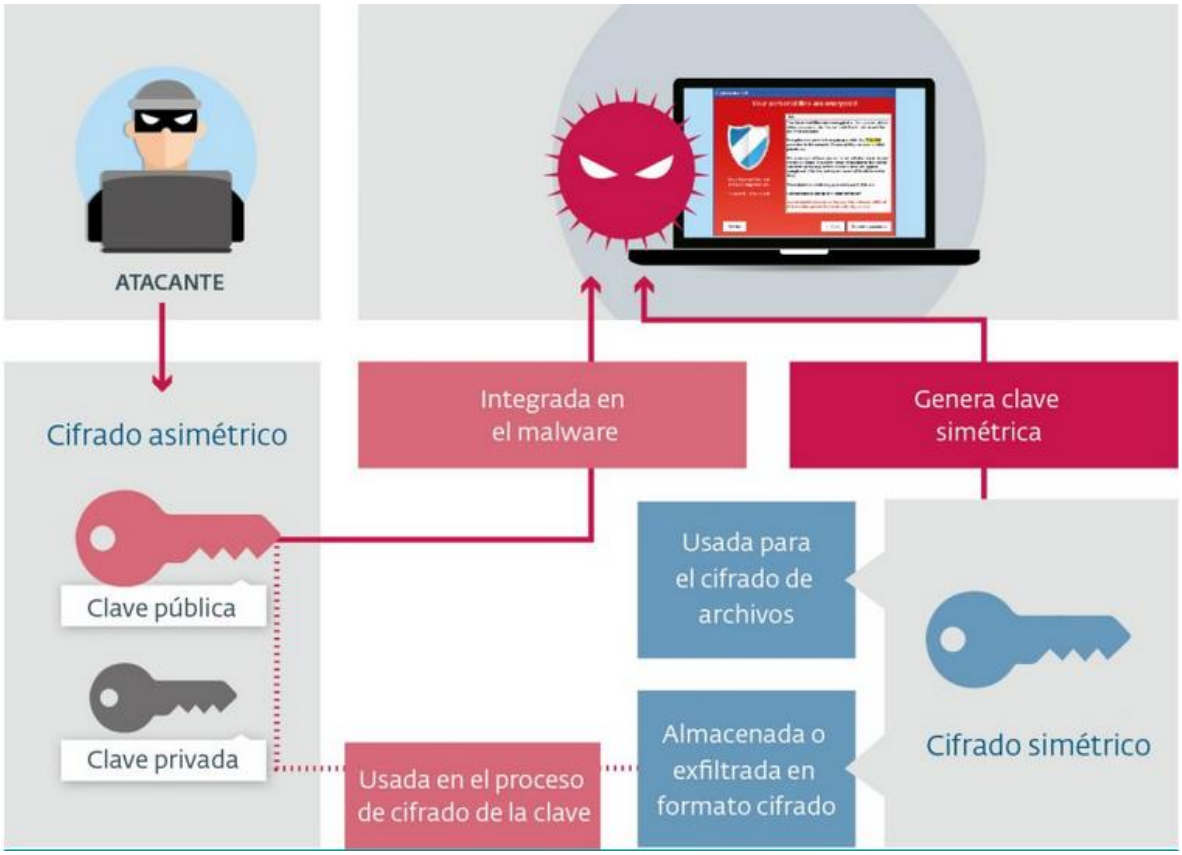
Cifrado asimétrico: algunas familias de ransomware usan criptografía de clave pública / privada para cifrar los datos de la víctima, como CryptoWall que usa RSA. En estas familias, las claves de encriptación se generan directamente en la máquina de la víctima, tal como la usa el ransomware WannaCry, o se entregan a través del canal C&C, tal como lo usa el ransomware Locky, o incrustadas en el binario, tal como lo usa el ransomware TeslaCrypt ;

Cifrado simétrico: este método se usa principalmente con la clave de cifrado incrustada en el malware. Diferentes familias de ransomware adoptan diferentes métodos de cifrado simétrico, así como patrones, por ejemplo, UIWIX primero cifra los datos con AES-256 en Cipher Block Chaining (CBC) seguido de un cifrado RC4 , y el ransomware Bucbi utiliza un método de cifrado menos conocido. llamado GOST ;

Técnicas híbridas: tales métodos utilizan primero algoritmos de clave simétrica, por ejemplo, AES-256 y CBC, para encriptar los archivos / sistema de la víctima. Luego, utilizan métodos de cifrado asimétricos, por ejemplo, RSA-1024, RSA-2048 o ECC, para cifrar la clave simétrica. Estas técnicas son utilizadas por varias familias de ransomware como CryptoLocker y Spora [34]. En las técnicas híbridas, generalmente los delincuentes incrustan la clave pública RSA dentro de la carga maliciosa binaria y, por lo tanto, no necesitan comunicarse con C2 para recuperar la clave de cifrado. Por lo tanto, cuando la víctima paga el rescate, los delincuentes usan la clave privada RSA correspondiente para descifrar los archivos / sistemas del usuario.

El uso de algoritmos criptográficos estándar y API es una forma conveniente para que los atacantes cifren los datos de la víctima; sin embargo, la ejecución de demasiadas API para una gran cantidad de datos requiere privilegios de administrador, lo que no siempre es el caso de un ataque de ransomware. Esto limita la cantidad de máquinas / archivos a los que podría apuntar un ransomware. Además, es trivial para los sistemas antimalware monitorear o limitar el acceso de los usuarios privilegiados a las API de Crypto, lo que conduce a la falla de la ejecución del ransomware. Por lo tanto, algunas familias de ransomware utilizan un mecanismo de cifrado personalizado. Por ejemplo, Mischa utiliza una clave generada aleatoriamente como semilla para una operación XOR para cifrar los datos de la víctima. Diversificar las técnicas de cifrado y limitar el uso de API criptográficas estándar podría considerarse una técnica de evasión para aquellos productos antimalware que dependen de la detección de actividades de API criptográfica estándar.

Ilustración 35 Esquema de cifrado doble en el ransomware criptográfico



Fuente: PUODZIUS, Cassius. "Cómo y por qué el cifrado moldeo al ransoware criptográfico". {En línea} Septiembre 13 de 2016. {Mayo 12 de 2020} disponible en: (https://www.welivesecurity.com/la-es/2016/09/13/cifrado-ransomware-criptografico/).

15 CONCLUSIONES

Se detectaron y diagnosticaron vulnerabilidades en un sistema operativo Windows infectado con Ransonware, por medio de la implementación de un ambiente virtual controlado. Entre las diversas vulnerabilidades que se encontraron en el sistema operativo Windows 10, se identificó que la descarga y uso no controlado de software expone en gran manera al sistema a infección por malware, y por ello se recalca la necesidad primordial de utilizar herramientas de seguridad integrales al interior de las empresas, que no solo se comporten como un antivirus tradicional, sino que puedan brindar diversos mecanismos de control y monitoreo en tiempo real sobre toda la información que se envía y se recibe en la red organizacional.

Se implementó un ambiente virtual controlado, lo cual permitió conocer de primera mano el funcionamiento del Ransomware y determinar de forma efectiva qué acciones realizar para contrarrestar el malware del sistema infectado. Ciertamente, esta es una práctica común usada para el desarrollo de laboratorios, que utilizan datos similares a los de producción para reproducir y ejecutar diferentes tipos de Malware con el fin de conocer los puntos ciegos de los sistemas de información. De esta forma, es posible afirmar que, en situaciones reales el uso de ambientes virtuales controlados se constituye en una metodología de gran importancia para lograr diseñar e implementar planes de acción que sean efectivos frente a diversos ataques, y que sirvan de manera significativa a la gestión de los riesgos informáticos.

Se identificaron y propusieron herramientas de seguridad informática, como la implementación de algunos controles básicos que ayuden a prevenir el desarrollo y actuación de los ransomware, entre los cuales se encuentran: realización de backups, ejecución de programas de concientización para los usuarios, protocolos de privilegios mínimos y uso de antivirus, los cuales servirán como herramientas para analizar los diferentes tipos de malware que se puedan presentar en el

desarrollo de las operaciones cotidianas. De acuerdo con este laboratorio se concluye que, el Ransomware no solo afecta la disponibilidad de la información sino también la integridad de esta, por lo tanto, su porcentaje de efectividad será en primer lugar establecido por la capacidad de bloquear o eliminar los archivos del sistema de la víctima. Por esto, al igual que con cualquier malware que ponga en riesgo el acceso a la información, la principal herramienta para recuperarla será contar con una copia de respaldo.

Se identificó y se presentó información que puede llegar a ser muy útil para los programas de capacitación y formación de los colaboradores al interior de las organizaciones, para que sepan cómo dar manejo a situaciones relacionadas con Ransomware, y de esta forma se logre reducir el impacto de este tipo de riesgo si se llegara a presentar, o minimizar la probabilidad de ocurrencia del mismo en el mejor de los casos, implementando medidas de prevención.

16 RECOMENDACIONES

• Implementar un programa de formación y concientización al interior de las empresas frente a los controles de seguridad de la información. Como los usuarios finales son objetivos, los empleados y las personas deben ser conscientes de la amenaza del ransomware.

• Escanear los correos electrónicos entrantes y salientes en las diferentes bandejas para detectar anomalías y filtrar archivos sospechosos para evitar que lleguen a los usuarios.

• Configurar los firewalls para bloquear el acceso a las direcciones IP maliciosas conocidas.

• Parchear sistemas operativos, software y firmware en dispositivos. Considere usar un usar un sistema centralizado de gestión de parches.

• Configurar los programas antivirus y antimalware para realizar exploraciones periódicas automáticamente.

• Administrar el uso de cuentas privilegiadas según el principio del privilegio mínimo.

• Configurar los controles de acceso, incluidos los permisos de archivos, directorios y recursos compartidos de red.

• Deshabilitar las macros de los archivos recibidos por correo electrónico.

• Implementar políticas de restricción de software (SRP) u otros controles para evitar programas desde la ejecución desde ubicaciones comunes de Ransomware, como carpetas temporales compatible con navegadores de Internet populares o programas de compresión / descompresión,

• Considerar la posibilidad de deshabilitar el protocolo de escritorio remoto (RDP) si no se está utilizando.

• Utilizar la lista blanca de aplicaciones, que solo permita que los sistemas ejecuten programas conocidos y permitido por la política de seguridad.

• Ejecutar entornos del sistema operativo o programas específicos en un entorno virtualizado.

• Clasificar los datos basados en el valor organizacional.

17 BIBLIOGRAFÍA

ESET. “Tendencias en seguridad informática para el 2019”. {En línea}. {10 diciembre 2018} disponible en: (https://www.eset.com).

SÁNCHEZ, Eduardo Patricio. Hardening. {En línea}. {14 de enero de 2015} disponible en: (http://www.magazcitum.com.mx/ ?p=2109#.ViUM_n4veM8)

TIDY, Joe. “Coronavirus: cómo los piratas informáticos están usando el miedo a la enfermedad covid-19 para difundir virus informáticos”. {En línea}. {13 de marzo de 2020}. En BBC News Mundo disponible en: (https://www.bbc.com/mundo/noticias-51853454).

MENDOZA, Miguel Ángel. “El impacto del Ransomware en Latinoamérica durante el 2017”. {En línea}. {Marzo 1 de 2018} disponible en: (https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/).

ELISAN, Christopher. Malware, rootkits & botnets a beginner's guide. New York: McGraw-Hill/Osborne, 2013. 384p.

COLOMBIA, Congreso de la República. “Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se conservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial No. 47.223, 5 de enero de 2009.” {En línea}. Enero de 2009. {20 de marzo de 2020} disponible en:

(http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html).

OJEDA, J. E., RINCÓN, F., ARIAS, M. E., DAZA, L.A. “Delitos informáticos y entorno jurídico vigente en Colombia.” {En línea}. 2010. {13 de abril de 2020} disponible en: (http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003).

OJEDA, J. E., RINCÓN, F., ARIAS, M. E., DAZA, L.A. “Delitos informáticos y entorno jurídico vigente en Colombia.” {En línea}. 2010. {13 de abril de 2020} disponible en: (http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003).

JAMES, Scott. “¿Las mejores frases sobre seguridad informática?” {En línea}. Abril 4 de 2017. {Enero 10 de 2020} disponible en: (https://protegermipc.net/2017/04/04/las-mejores-frases-sobre-seguridad-informatica/).

PICHAI, Sundar. “Google spent $1.2 million last year to protect CEO Sundar Pichai in an 'overall security program' that started months after the YouTube shooting”. {En línea}. Mayo 1 de 2019. {Enero 13 de 2020} disponible en: (https://www.businessinsider.in/google-spent-1-2-million-last-year-to-protect-ceo-sundar-pichai-in-an-overall-security-program-that-started-months-after-the-youtube-shooting/articleshow/69122609.cms)

ZIMBA, Aarón. CHISHIMBA, Mumbi. CHIHANA, Sipiwe. “A Ransomware Clasificación Framework Based on File Deletion and File Encryption Attack Structures”. {En línea}. Junio de 2019. {Febrero 20 de 2020} disponible en:

https://www.researchgate.net/publication/333966134_A_Ransomware_Classification_Framework_Based_on_File-Deletion_and_File-Encryption_Attack_Structures).

CELIKTAS, Baris. UNLU, Nafis. KARACUHA, Ertugrul. “Ransomware, Detection and Prevention Techniques, Cyber Security, Malware Analysis”. {En línea} Mayo de 2018. {Enero 18 de 2020} disponible en: (https://www.researchgate.net/figure/Ransomware-Detection-Methods-and-Techniques-45_fig11_326191046).

ESPINOSA, Oscar. “Qué es y para qué sirve un Honeypot”. {En línea} {Marzo 8 de 2020} disponible en: (https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/).

PROTEGER MI PC. “Protección frente al ransomware en Windows con Cybersight Ransomstopper”. {En línea}. Diciembre 28 de 2018. {Marzo 3 de 2020} disponible en: (https://protegermipc.net/2017/12/28/cybersight-ransomstopper/).

RAMÍREZ, Adrián. “How Domain Generation Algorithms (DGA) Work”. {En línea} {Enero 8 de 2020} disponible en: (https://www.adrianramirez.es/wp-content/uploads/2016/05/How-DGA-work.png).

WIKIPEDIA. “Domain generation algorithm”. {En línea}. {Enero 13 de 2020} disponible en: (https://en.wikipedia.org/wiki/Domain_generation_algorithm).

PUODZIUS, Cassius. “Cómo y por qué el cifrado moldeo al ransoware criptográfico”. {En línea} Septiembre 13 de 2016. {Mayo 12 de 2020} disponible en: (https://www.welivesecurity.com/la-es/2016/09/13/cifrado-ransomware-criptografico/).

CNN. “¿Qué es un virus ‘ransomware’ y cómo actúa?”. {En línea}. 2017 {Febrero 20 de 2020} disponible en: (http://cnnespanol.cnn.com/2017/05/15/que-es-un-virus-ransomware-y-como-actua/).

SEGU INFO. “Consejos para prevenir ransomware”. {En línea}. Marzo 11 de 2016. {Enero 12 de 2020} disponible en: (http://blog.segu-info.com.ar/2016/03/22-consejos-para-prevenir-el-ransomware.html).

XATAKA. “Qué es el ransomware, cómo actúa y cómo prevenirlo”. {En línea}. Marzo 7 de 2016 {Mayo 5 de 2020} disponible en: (https://www.xataka.com/seguridad/que-es-el-ransomware-que-ahora-tambien-afecta-a-los-macs).

MICROSOFT. “Microsoft Security Intelligence Report Volumen 13”. {En línea}. Enero – Junio de 2012. {Abril 14 de 2020} disponible en: (https://www.microsoft.com/es-ES/download/details.aspx?id=34955).

MIFSUD, Elvira. “MONOGRÁFICO: Introducción a la seguridad informática”. {En línea} Marzo 26 de 2012. {Febrero 10 de 2020} disponible en: (http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-).

PANDASECUITY. “¿Qué es un Ransomware?”. {En línea}. Noviembre 15 de 2013. {Enero 19 de 2020} disponible en: (http://www.pandasecurity.com/spain/mediacenter/consejos/que-es-un-ransomware/).

BROADCOM. “Ransomware a growing manace”. {En línea}. {Marzo 1 de 2020} Disponible en: (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf).

MENDOZA, Miguel Ángel. “El impacto del Ransomware en Latinoamérica durante el 2017”. {En línea} Marzo 1 de 2018. {Abril 5 de 2020} disponible en: (https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/).

GITHUB. “Yara-Rule / rules”. {En línea}. {Julio 25 de 2019} disponible en: (https://github.com/Yara-Rules/rules).

OPEN DATA SECURITY. “Petya, el último ransomware que atacó Europa, Asia y Estados Unidos”. {En línea}. Junio 28 de 2017. {Abril 20 de 2020} disponible en: (https://opendatasecurity.io/es/petya-ultimo-ransomware-que-ataco-europa-asia-estados-unidos/).

INCIBE-CERT. “Petya Nuevo ataque mundial del ransomware”. {En línea}. Junio 27 de 2017. {Junio 30 de 2019} disponible en: (https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/petya-nuevo-ataque-mundial-ransomware).

PANDA ANTIVIRUS. “Cuál era el objetivo real de los creadores de Petya”. {En línea}. Julio 19 de 2017. {Mayo 2 de 2020}. Disponible en: (https://pandaantivirus.com.ar/objetivo-real-los-creadores-petya/).

MUNDO INSIDER. “Las Claves de Petya y el Origen de la Infección en Ucrania”. {En línea}. Junio 28 de 2017. {Abril 4 de 2020} disponible en: (https://www.mundoinsider.com/125449/las-claves-petya-origen-la-infeccion-ucrania/).