Universitat Oberta de Catalunya

uoc.edu

Guía de prevención y respuesta frente a ataques de ransomware

Carlos Alberto Crego Sánchez
Master en Ciberseguridad y Privacidad
Privacidad

Albert Jové Canela
Cristina Pérez Sola

28 de diciembre del 2021

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Guía de prevención y respuesta frente a ataques de ransomware*
Nombre del autor:	*Carlos Alberto Crego Sánchez*
Nombre del consultor/a:	*Albert Jové Canela*
Nombre del PRA:	*Cristina Pérez Solá*
Fecha de entrega (mm/aaaa):	12/2021
Titulación:	*Master Universitario en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*Privacidad*
Idioma del trabajo:	*Castellano*
Palabras clave	*Ransomware, Prevención, Defensa*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El ransomware lleva bastantes años figurando entre las amenazas más importantes para la economía y la seguridad de las empresas.

Este tipo de malware tiene como objetivo el cifrado de los datos de una compañía para, a posteriori, pedir un rescate a la víctima a cambio de descifrarlos, normalmente mediante Bitcoins, ya que resultan más difíciles de rastrear.

Un ataque de ransomware, puede paralizar por completo la actividad de la compañía infectada, por lo que el impacto económico es grande y causa graves daños a la reputación.

En los últimos años, se están detectando ataques mucho más dirigidos y cada vez más inteligentes que roban la información antes de cifrarla para pedir rescates más cuantiosos amenazando con hacer públicos los datos, lo que puede conllevar graves sanciones de acuerdo con la legislación vigente.

La complejidad para resolver los ataques de ransomware a posteriori es tan elevada que en muchas ocasiones no se pueden recuperar los datos cifrados, es por ello, que la mejor forma de defenderse es la prevención mediante una combinación de herramientas, buenas prácticas y formación en ciberseguridad.

El presente trabajo fin de master tiene como objetivo hacer un estudio del ransomware, detallando los vectores de ataque más empleados para su distribución y suministrando directrices y herramientas para que tanto PYMES como particulares puedan reducir el riesgo de infección.

Abstract (in English, 250 words or less):

Ransomware has been among the most important threats to the economy and security of companies for many years.

This type of malware aims to encrypt the data of a company to ask the victim for a ransom in exchange for decrypting it, usually through Bitcoins, since they are more difficult to track.

A ransomware attack can completely paralyze the activity of the infected company, so the economic impact is great and causes serious damage to the reputation.

In recent years, much more targeted and increasingly intelligent attacks are being detected that steal information before encrypting it to demand larger ransoms, threatening to make the data public, which can lead to serious administrative fines according to current legislation.

The complexity to resolve ransomware attacks afterwards is so high that in many cases the encrypted data cannot be recovered, which is why the best way to defend oneself is prevention through a combination of tools, good practices, and cybersecurity training.

The objective of this final master's dissertation is to study ransomware, detailing the attack vectors most used for its distribution and providing guidelines and tools so that both SMEs and individuals can reduce the risk of infection.

Índice

Lista de figuras

Presentación del trabajo

Contexto y Justificación

El ransomware es un tipo de malware en continua evolución que impide el acceso a los activos digitales almacenados en un equipo o dispositivo informático, amenazando con destruirlos o hacerlos públicos si no se accede a pagar un rescate en un determinado plazo.

El ransomware se propaga, como otros tipos de malware, por múltiples vías: campañas de spam, vulnerabilidades, malas configuraciones de software o herramientas de activación de programas no oficiales.

Los ciberdelincuentes tratan de que la víctima abra un archivo adjunto infectado o haga clic en un enlace que le lleve a un sitio web donde será infectada.

En la actualidad, muchos estudios revelan que el ransomware es la forma más prevalente de amenaza de ciberseguridad para los negocios.

A pesar de las medidas de seguridad empleadas por las organizaciones para proteger sus activos digitales, el ransomware sigue dominando las estadísticas en los ataques de ciberseguridad, las víctimas pueden ser de todo tipo, particulares, empresas muy pequeñas o grandes corporaciones.

Como profesionales de la ciberseguridad queremos emprender una campaña de concienciación tanto para PYMES como para particulares detallando los peligros a los que se enfrentan y suministrándoles directrices y herramientas para minimizar el riesgo de infección.

Objetivos del Trabajo

A continuación, se proporciona la lista de objetivos del presente TFM:

- Hacer un estudio del ransomware para entender su historia, su evolución, anatomía y particularidades.

- Estudiar las diferentes tipologías de ransomware.

- Analizar los vectores de ataque empleados para distribuir ransomware.

- Elaborar una lista de medidas de prevención para que tanto usuarios como empresas puedan reducir el riesgo de infección.

- Elaborar un plan de respuesta a incidentes de ransomware.

- Evaluar las consecuencias legales de una infección por ransomware, sobre todo en caso de que se sospeche que hay una fuga de datos.

Enfoque y método seguido

En el ámbito de la gestión de proyectos existen varias metodologías, algunas de ellas, muy conocidas en el ámbito empresarial como la descrita en la guía del PMBOK o en ITIL.

La guía del PMBOK podría aplicarse como metodología al presente trabajo fin de master dado que se trata de una metodología aplicable a cualquier tipo de proyecto, sin embargo, su implementación es bastante compleja cuando se trata de proyectos a pequeña escala como es el caso.

En el ámbito del desarrollo de software, existen metodologías que se pueden aplicar al ciclo de vida de gestión de proyectos, algunas de las más conocidas son Scrum, Lean y Kanban y son aplicables cuando el desarrollo se debe llevar a cabo de forma iterativa e incremental debido a que no se conocen de antemano todos los detalles de lo que se pretende desarrollar o construir.

Para el presente trabajo fin de master, se ha decidido emplear la metodología Kanban, ya que se adapta bien a cualquier tipo de proyecto, sobre todo a aquellos donde los requisitos están poco definidos de antemano como es el caso.

La metodología Kanban está ganando gran popularidad en los últimos años entre las empresas como una manera de gestionar el trabajo de forma fluida.

En Kanban, las tareas se representan mediante tarjetas que se mueven a través de diversas etapas hasta su finalización.

La metodología Kanban se basa en el empleo de un tablero que se encuentra dividido en columnas (imagen 1), el número de columnas puede variar dependiendo del nivel de complejidad y del tipo de proyecto, por ejemplo, en proyectos de desarrollo lo habitual es usar las siguientes columnas:

- **Pendiente**: En esta columna se incluye la lista de tareas pendientes de desarrollo, las tareas se deben ordenar de acuerdo con su prioridad, colocando arriba las que tengan mayor prioridad.

- **En desarrollo**: En esta columna se incluyen todas las tareas que se encuentran actualmente en desarrollo.

- **Pruebas**: En esta columna se incluyen todas las tareas que se encuentran en proceso de revisión para comprobar si realmente se ha completado el desarrollo de acuerdo con los requerimientos.

- **Despliegue**: En esta columna se incluyen las tareas que se encuentran pendientes de ser desplegadas o entregadas.

- **Finalizado**: En esta última columna se incluyen las tareas finalizadas.

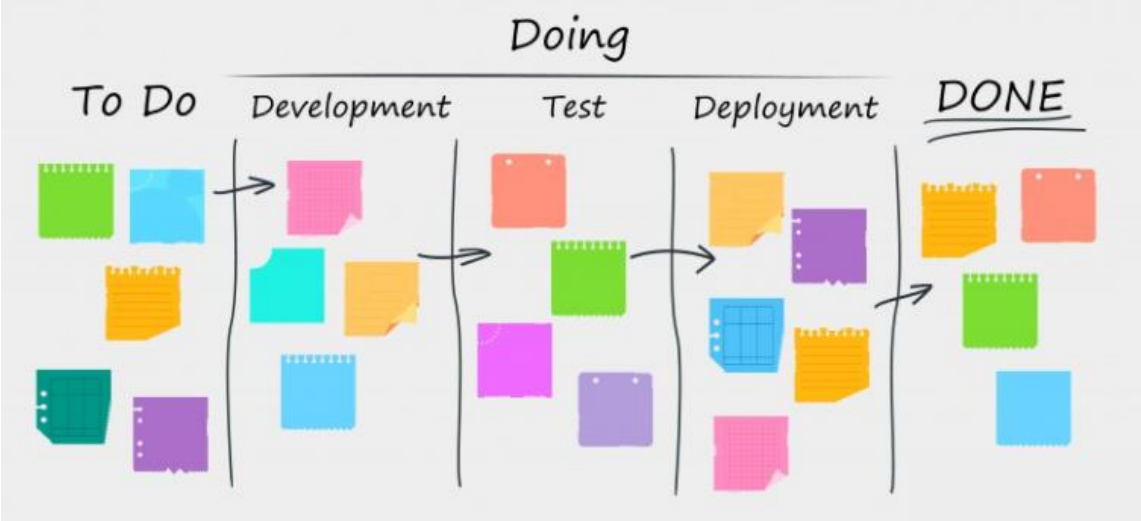

Imagen 1. Columnas de un tablero Kanban.

Aunque el presente trabajo fin de master se trata de un trabajo de investigación y no de desarrollo, el tablero Kanban que manejaremos incluirá todas las columnas descritas anteriormente empleándolas de la siguiente manera:

- **Pendiente**: En esta columna se incluirán todos los apartados del trabajo fin de master cuya investigación está pendiente de desarrollar.

- **En desarrollo**: En esta columna se incluirán todos los apartados del trabajo fin de master cuya investigación se encuentra en desarrollo.

- **Pruebas**: En esta columna se incluirán todos los apartados del trabajo cuya ortografía, bibliografía y contenido se encuentra pendiente de revisión.

- **Despliegue**: En esta columna se incluirán todos los apartados del trabajo fin de master que ya hayan sido revisados y que se encuentren pendientes de ser incluidos en una entrega parcial.

- **Finalizado**: En esta columna se incluirán todos los apartados del trabajo fin de master que ya hayan sido incluidos en alguna entrega parcial.

El uso de Kanban como metodología nos permitirá obtener el máximo rendimiento ya que permite visualizar las tareas que se están acometiendo en un momento dado, las que se encuentran por hacer y las finalizadas.

También nos permitirá limitar la cantidad de trabajo en proceso estableciendo metas asequibles, realizar un seguimiento del tiempo de forma continua a fin de evaluar el trabajo con precisión, identificar los cuellos de botella y permitir la lectura fácil de lo que está ocurriendo con un solo vistazo.

Planificación

El plan de trabajo y el listado de tareas se encuentran recogidos en el Anexo I.

Capítulo 1

Introducción al Ransomware

El rápido desarrollo tecnológico ha traído consigo un incremento de los ciberataques, en un mundo donde el cibercrimen evoluciona a la par que lo hace la tecnología se utilizan ciberataques tan complejos que pueden llegar a comprometer millones de dispositivos simultáneamente, uno de los más temidos hoy en día es el ransomware.

El objetivo del ransomware no es dañar el sistema de archivos del dispositivo, de hecho, un dispositivo infectado con ransomware es completamente funcional, en su lugar, restringe el acceso a una parte de los archivos almacenados, normalmente, aquellos que tienen una importancia relevante para la víctima, como documentos, agendas de contactos, fotos, vídeos, código fuente, etc.

La infección viene acompañada de una nota ubicada en un archivo del escritorio de la víctima o de un mensaje por pantalla donde se amenaza con destruir los archivos si no se accede a pagar un rescate dentro de un periodo de tiempo. Los cibercriminales que hay detrás del ransomware recolectan el pago del rescate usando métodos de pago anónimos como por ejemplo tarjetas prepago y criptomonedas como Bitcoin para evitar ser rastreados por las autoridades.

En las primeras versiones, los ataques de ransomware utilizaban métodos muy sencillos para restringir el acceso de la víctima a los archivos del dispositivo, uno de los más comunes era bloquear el acceso a las herramientas del sistema o al escritorio, sin embargo, en las versiones más modernas los ataques de ransomware utilizan algoritmos de cifrado para restringir el acceso a los archivos de la víctima lo que los hace inaccesibles sin la clave de descifrado.

Hay que considerar que a medida que aumenta la dependencia de la tecnología, las personas dependen más de los dispositivos donde se pueden llegar a almacenar información muy sensible como por ejemplo contratos, operaciones bancarias, presupuestos, agendas, secretos comerciales, por lo que un ataque de ransomware exitoso puede llegar a tener consecuencias devastadoras.

Actualmente, los ataques de ransomware son un problema que afecta a las personas, el sector público y empresas de todo tipo, de hecho, un informe elaborado por el programa Cybersecurity Ventures [1] estima que los ataques de ransomware afectarían a una empresa cada 14 segundos para finales de 2019, en este informe se estimaba que el coste de los daños alcanzaría los 11.500 millones de dólares.

Sin embargo, en otro informe elaborado por Cisco Systems [2], se indica que los ataques de ransomware estaban creciendo en 2019 a una tasa anual del 350%.

En este primer capítulo, abordaremos la aparición del ransomware y hablaremos brevemente sobre su historia, tipos, componentes, lo que lo diferencia de otros tipos de malware y como logra su persistencia en los dispositivos de las víctimas.

1.1. Evolución del ransomware

Muchos estudios revelan que el primer ransomware documentado, fue AIDS Trojan [3], también conocido como PC Cyborg, y apareció en 1989.

El autor de este virus fue un biólogo llamado Joseph Popp que envió por correo postal 20.000 disquetes infectados a los asistentes a la conferencia sobre el SIDA de la organización mundial de la salud, cada disquete contenía un cuestionario interactivo que se utilizaba para activar el malware después de que el dispositivo fuese reiniciado 90 veces.

El ransomware AIDS Trojan ocultaba todos los directorios y cifraba los nombres de los archivos ubicados en la unidad C:\ del dispositivo infectado lo que inutilizaba por completo el sistema operativo Windows, para deshacer los cambios realizados por el virus en el sistema de archivos, la víctima tenía que pagar 189$ en un apartado postal panameño.

El siguiente paso en la evolución se produjo en 1996 cuando dos investigadores escribieron un artículo presentado en la conferencia de seguridad y privacidad de IEEE, en este artículo se planteaba una prueba de concepto que usaba criptografía de clave pública para crear código malicioso y poder así extorsionar a los propietarios de los dispositivos infectados, fue en este artículo donde por primera vez se plantearon los términos de extorsión criptoviral y criptovirologia [4] para dar nombre a este tipo de ciberataque.

Hasta 2005, el ransomware no era muy conocido en el mundo del cibercrimen por lo que no se produjeron incidentes relevantes con este tipo de malware, sin embargo, todo cambió en 2005, cuando los creadores de ransomware comenzaron a utilizar el cifrado en su código malicioso.

En 2005 [5], surgieron nuevas variantes de ransomware como Archiveus y GPCoder, ambos, utilizaban cifrado RSA de 1024 bits, considerado cifrado fuerte en ese momento lo que dificultaba la recuperación de los archivos mediante el empleo de técnicas de fuerza bruta.

El caso de Archiveus era muy particular porque cifraba todos los archivos que se encontrasen en la carpeta de documentos y habilitaba un sitio web donde las víctimas podía adquirir una contraseña de 30 dígitos para recuperar sus archivos.

Por aquel entonces, las compañías de antivirus respondieron a la amenaza añadiendo la firma de cada variante de ransomware descubierta en su lista de firmas de antivirus, esto contribuyó a detener la mayoría de los ataques en ese momento.

En 2008, apareció la criptomoneda Bitcoin, por lo que a partir de 2009 la mayoría de las variantes de ransomware la incorporaron como medio para pagar el rescate dado que proporcionaba anonimato, lo que dificultaba mucho a las autoridades la tarea de rastrear los pagos.

En 2009, surgió un ataque de ransomware diferente conocido como Vundo [6], esta nueva variante cambió la estrategia al utilizar técnicas de scareware para convencer a las víctimas de que compren software de seguridad como XPAntivirus2009 indicándoles que su dispositivo había sido infectado con un virus.

Vundo fue un malware polimórfico, lo que significa que su ejecutable cambiaba frecuentemente, sin embargo, los proveedores de antivirus añadieron todas las variantes de Vundo descubiertas en las bases de datos de firmas para detenerlo.

En 2011, apareció WinLock, considerado el primer ejemplo de ransomware de bloqueo (locker) distribuido globalmente. WinLock evitaba que la víctima iniciase sesión en su dispositivo en lugar de cifrar los archivos y afectó solo a dispositivos con sistema operativo Windows.

En 2012, el ransomware expandió sus operaciones para apuntar a los proveedores de servicios y comenzó a usar tácticas amenazantes como las empleadas por Vundo para extorsionar a sus víctimas, una de las que más éxito cosecho fue la de emplear mensajes en los que se hacía pensar a las víctimas que habían cometido un delito.

Los creadores de ransomware atacaron algunos sitios web de pornografía y software pirateado y utilizaron mensajes para hacerse pasar por la administración de justicia e informar a las víctimas de que habían violado la ley al ver contenido de pornografía infantil o que habían infringido los derechos de autor al descargar contenido pirateado, en el mensaje, se informaba a las víctimas que sus archivos personales habían sido bloqueados por la administración de justicia y que debían pagar una multa a la policía para recuperar el acceso al dispositivo bloqueado.

El ransomware más conocido que usaba este tipo de táctica fue Reveton, el caso de Reveton fue muy significativo ya que utilizaba tarjetas prepago y criptomonedas Bitcoin para recolectar el pago de los rescates, algunas fuentes estiman que Reveton obtuvo ingresos de 44.000$ por día en cada país [7].

Animados por los ingresos conseguidos por Reveton, el cibercrimen empezó a apostar fuerte por el ransomware y entre 2013 y 2015 aparecieron nuevas variantes como Cryptolocker, Torrentlocker, Cryptowall y Teslacrypt, estas nuevas variantes utilizaban algoritmos de cifrado fuerte como AES y RSA de 2048 bits lo que contribuyó a un crecimiento explosivo en los ingresos obtenidos a cambio de rescates llegando a alcanzar la cifra de 325 millones de dólares a finales de 2015.

El caso de Cryptolocker fue especialmente interesante ya que introdujo el despliegue de servidores de C&C (ver apartado 1.3) en la red TOR y empleaba una botnet de dispositivos infectados como mecanismo de distribución.

En 2016, el ransomware continuó su evolución añadiendo características más avanzadas a sus operativas como por ejemplo el empleo de una cuenta atrás que hacía que se incrementase el precio del rescate cada día que la víctima no ejecutaba el pago, además, aparecieron variantes que podían propagarse a través de la red automáticamente, se añadieron nuevas formas de pago del rescate y se simplificó el proceso haciéndolo más fácil incluso para usuarios con nociones muy básicas de informática, las variantes más destacables que aparecieron fueron Locky, Petya y SamSam.

El caso de Locky fue interesante ya que se considera que fue el primer ransomware en ser distribuido a escala global mediante técnicas de phising y el uso de archivos de Microsoft Word con macros maliciosas, en pleno apogeo llegó a infectar hasta 100.000 dispositivos diariamente.

2016 fue un año a señalar por el número de variantes que aparecieron, el número de familias de ransomware descubiertas fue de 247, lo que supuso un incremento del 752% sobre el año anterior [8], esto contribuyó a que el 2017 fuese catalogado por los expertos en seguridad como el año dorado del ransomware.

Una de las variantes que apareció en 2017 fue Doxware cuyo caso es muy significativo ya que amenazaba a sus víctimas con hacer públicos sus datos si rechazan el pago del rescate, Doxware tenía en el punto de mira a grandes corporaciones, políticos, celebridades y otras figuras públicas [9].

Sin embargo, el ciberataque más famoso que tuvo lugar en 2017 fue el del ransomware WannaCry, este malware se extendió a nivel mundial, las instrucciones de rescate estaban traducidas a 27 idiomas y tenía capacidad para propagarse automáticamente a través de la red, el programa Cybersecurity Ventures, estimó el coste de los ataques por ransomware en 2017 en 5.000 millones de dólares [10] de los cuales 4.000 millones se debieron a WannaCry [11].

El enorme aumento en los daños provocados por el ransomware en 2017 se debió principalmente a que el grupo de hackers Shadow Brokers [12] filtro un repositorio que contenía entre otras cosas, exploits secretos y herramientas de hacking de la NSA, que permitieron a los creadores de ransomware explotar vulnerabilidades en dispositivos de escritorio, servidores, VPN y firewalls, básicamente estas herramientas fueron empleadas por el cibercrimen para difundir el ransomware a nivel mundial utilizando vulnerabilidades no parcheadas en sistemas operativos Windows.

En 2018, los ataques de ransomware decrecieron, de acuerdo con informes publicados por Kaspersky's [13] y Malwarebytes [14], las infecciones por ransomware cayeron un 30% a nivel mundial.

Sin embargo, continuaron apareciendo nuevas variantes cada vez más sofisticadas y con capacidad para propagarse automáticamente, la más significativa fue Grandcrab ya que se apoyaba en el concepto de "ransomware como servicio" (RaaS), Grandcrab permitía ejecutar y planificar los ataques mediante el uso de campañas de spam que enviaban emails con un archivo ZIP adjunto que contenía el ransomware.

Aunque es difícil predecir el futuro de la ciberseguridad, un reciente estudio elaborado por el programa Cybersecurity Ventures [15] estima que los daños provocados por el cibercrimen alcanzarán la cifra de 6 trillones de dólares para 2021, de los cuales 20.000 millones de dólares se corresponderán con ataques de ransomware.

Ahora que tenemos unas nociones básicas de historia del ransomware y de cómo ha evolucionado hasta el día de hoy, discutiremos brevemente el concepto de malware para comprender mejor el papel del ransomware.

1.2. Malware

Malware, es un término general empleado para describir todos los tipos de software que pretenden alterar el estado funcional de un dispositivo.

La mayoría de los tipos de malware necesitan ser ejecutados por el usuario para que el código malicioso se propague a otros dispositivos o través de la red, el malware puede propagarse físicamente usando disquetes, CD/DVDs, memorias USB o puede ser distribuido a través de internet, por ejemplo, mediante archivos adjuntos en mensajes de email, software pirata, software gratuito y redes sociales.

Hay diferentes tipos de malware, dentro de cada clase podemos encontrar subtipos, a continuación, se proporcionará una descripción general de los tipos de malware más conocidos:

Virus

Se trata del término más antiguo empleado para hacer referencia a software malicioso, el principal objetivo de un virus informático es dañar el sistema operativo del dispositivo de la víctima volviéndolo inestable para obligar al usuario a formatear el disco duro para devolverlo a su estado original.

Gusanos

Inicialmente, el propósito de los gusanos no es destruir o comprometer el sistema operativo como los virus, sino replicarse de un dispositivo a otro a través de la red sin la intervención del usuario.

Los gusanos más modernos, pueden transportar malware como, por ejemplo, ransomware.

Cryptojacking

Normalmente se trata de fragmentos de código Javascript que infectan los dispositivos silenciosamente cuando la víctima hace clic en el link de un email o de un sitio web comprometido.

Scareware

Se trata de una forma de malware que emplea técnicas de ingeniería social para causar un estado de conmoción, estrés, ansiedad o la percepción de una amenaza para persuadir a las víctimas a que compren e instalen software no deseado. El scareware pertenece a la categoría de malware dirigido a la extorsión digital que es la misma categoría a la que pertenece el ransomware.

Adware y Spyware

El malware de tipo Adware tiene como propósito mostrar publicidad en el dispositivo de la víctima sin su consentimiento.

Sin embargo, el problema surge cuando el Adware viene con otro programa malicioso denominado Spyware cuyo propósito es registrar y rastrear la actividad online del usuario y robar información confidencial como nombres de usuario y contraseñas mediante el empleo de keyloggers.

Backdoors

Los backdoors o puertas traseras existen dentro de muchos tipos de malware, en términos generales, no es más que un código malicioso que abre un puerto en el dispositivo de la víctima para permitir ejecutar acciones no autorizadas.

Troyanos

Se trata de otro tipo de malware que se instala de forma silenciosa en el dispositivo de la víctima y que se presenta bajo la apariencia de un archivo normal para engañar a los usuarios para que lo descarguen y lo instalen.

La mayoría de los troyanos actúan como backdoors, dando acceso no autorizado al atacante sobre el dispositivo infectado, lo que le proporciona control total.

Rootkits

Un rootkit es un tipo de malware que tiene capacidad para obtener acceso administrativo al dispositivo infectado. La detección de rootkits es difícil porque tienen capacidad para evitar que los antivirus lo detecten.

La eliminación de rootkits puede ser complicada o prácticamente imposible, especialmente cuando los rootkits residen en el kernel o en el firmware en cuyo caso pueden requerir el reemplazo de parte del hardware.

Keylogger

Se trata de un tipo de malware que se utiliza para registrar cada tecla que se pulsa en el teclado, los keyloggers también funcionan en dispositivos móviles.

Los keyloggers almacenan la información recopilada y la envían al atacante, quien luego puede extraer información, como por ejemplo credenciales.

Downloaders

Un downloader no es más que un malware cuyo propósito consiste en descargar otro malware, contienen dentro del código malicioso la URL de descarga.

Browser Hijacker

Se trata de un código malicioso desarrollado para controlar la configuración del navegador, como la página de inicio o el proveedor de búsqueda estándar, a menudo se incluyen con software gratuito y barras de herramientas del navegador y también pueden contener adware y spyware.

También pueden cambiar la configuración de proxy del navegador, lo que compromete la privacidad y la seguridad.

Botnets y ataques DDoS

Un ataque de denegación de servicio distribuido (DDoS) es un tipo de ciberataque que causa que un servicio o recurso en la red sea inaccesible para los usuarios legítimos, se generan mediante la saturación de los puertos de un servidor empleando múltiples flujos de información desde varios puntos de conexión hacia el mismo servidor haciendo que se sobrecargue

Los creadores de este tipo de malware construyen botnets, que no son más que redes de dispositivos infectados mediante la difusión de software malicioso a través de correos electrónicos, sitios web y redes sociales.

Una vez que un dispositivo ha sido infectado, el atacante lo controla de forma remota sin conocimiento de la víctima y lo utiliza como parte de un ejército de dispositivos para lanzar flujos de información de forma simultánea contra cualquier objetivo, normalmente servidores o sitios web.

1.3. Anatomía del Malware

En términos generales, todo malware está formado por los siguientes componentes:

Payload

Es el componente encargado de causar daño al dispositivo de la víctima, algunos ejemplos del daño causado por el payload serían los siguientes:

- Robo de información confidencial como contraseñas y datos personales.
- Espionaje y monitorización.
- Añadir el dispositivo a una botnet.
- Descargar malware.
- Bloquear el acceso a los archivos y pedir un rescate por restaurar el acceso.
- Abrir una puerta trasera (backdoor) en el dispositivo de la víctima.

Persistencia

El componente de persistencia es el encargado de mantener vivo el malware una vez que el dispositivo infectado ha sido reiniciado, su objetivo es persistir los archivos necesarios para su funcionamiento en el sistema de archivos o bien dotar de un mecanismo que permita la reinfección.
La siguiente lista muestra algunos ejemplos de donde se suele esconder el malware dentro del sistema de archivos del sistema operativo Windows:

- Carpetas de inicio de sesión
- Registro de Windows
- Servicios de Windows
- Tareas planificadas
- Carpetas temporales y Accesos directos

Silenciador

Es el componente encargado de hacer pasar desapercibida la actividad llevada a cabo por el malware y de este modo alargar su vida, para ello se emplean diversas técnicas como, por ejemplo:

- Ocultación de procesos, sockets, módulos y DLLs.
- Modificación de la extensión de los archivos que forman parte del malware.
- Alteración del comportamiento en función del contexto de ejecución, por ejemplo, si se detecta la existencia de herramientas de análisis de malware, el código malicioso podría optar por proteger las comunicaciones con los servidores encargados de recibir la información robada del dispositivo de la víctima o evitar enviarla.

Ofuscador

Es el componente encargado de evadir los escáneres de antivirus y los sistemas de detección de intrusos (IDS).

Los ofuscadores más sofisticados modifican el código del malware mediante técnicas de compresión y cifrado haciendo que la firma digital cambie de modo que el malware no sea detectado por el antivirus.

Controlador (C&C)

Es el componente responsable de enviar instrucciones y datos al malware y de recibir los datos extraídos de los dispositivos infectados como por ejemplo contraseñas. Mediante el controlador el atacante puede programar la descarga de una nueva versión del malware instalado o distribuir una clave criptográfica en el caso de malware de tipo ransomware.

Algunos tipos de malware emplean servicios en la nube como clientes de correo web y servicios de hosting como controladores a fin de evadir los sistemas de detección.

1.4. Tipos de Ransomware

Existen 2 tipos de ransomware: los de cifrado (crypto) y los de bloqueo (locker).

Ransomware de bloqueo (locker)

El ransomware de bloqueo es aquel que impide que la víctima acceda a sus archivos personales para luego exigirle un rescate que le permita recuperar el acceso.

Muchos ransomware de este tipo emplean técnicas de lo más variopintas para impedir el acceso del usuario a sus archivos personales, por ejemplo, mediante el bloqueo del escritorio o impidiendo que el usuario inicie sesión.

En comparación con el ransomware de cifrado, el ransomware de bloqueo emplea técnicas relativamente sencillas que cualquier usuario con conocimientos avanzados de informática puede sortear, como resultado, la mayoría de ransomware de bloqueo se puede eliminar de los dispositivos infectados sin alterar el sistema operativo ni los archivos comprometidos.

Ransomware de cifrado (crypto)

Se trata del tipo más peligroso y el que más extendido se encuentra en la actualidad.

Este tipo de ransomware cifra todos o parte de los datos personales del dispositivo de la víctima tomándolos como rehén hasta que la víctima paga el rescate y obtiene la clave de descifrado del atacante.

En grandes corporaciones y organismos públicos puede tener un efecto devastador si no existe una copia de seguridad para restaurar el funcionamiento de los dispositivos infectados, en estos casos, la víctima sólo tiene una opción, pagar el rescate.

Una vez que el ransomware de cifrado se ha instalado en un dispositivo, busca sigilosamente archivos relevantes para la víctima de acuerdo con su extensión y comienza a cifrarlos, en el caso de los ransomware de cifrado más modernos y sofisticados, la búsqueda tiene lugar no solo en el disco duro local sino también en todas las unidades externas y archivos compartidos en la red.

Tras cifrar todos los archivos del dispositivo, el ransomware de cifrado presenta una nota de rescate al usuario mostrando una cuenta atrás y solicitando el pago del rescate para recuperar el acceso a los archivos comprometidos.

Los ransomware de cifrado más modernos solicitan el pago del rescate principalmente a través de la criptomoneda Bitcoin.

WannaCry, el ransomware más famoso hasta la fecha y que causó estragos a nivel mundial en 2017, pertenece a la tipología de ransomware de cifrado.

Chantaje y extorsión

El ransomware también puede categorizarse de acuerdo con el objetivo que el atacante persigue, en este caso, podemos diferenciar entre ransomware de extorsión y ransomware de chantaje.

El chantaje y la extorsión son 2 delitos completamente distintos, el chantaje consiste en obtener información de la víctima que en caso de ser revelada pueda perjudicar su posición social, económica, familiar o de cualquier otra índole, la extorsión, por el contrario, persigue obtener el dinero de la víctima.

1.5. Particularidades del Ransomware

Algunos tipos de malware tienen como objetivo robar información confidencial como por ejemplo nombres de usuario, contraseñas, pulsaciones de teclas, archivos personales, etc.

Otros, sin embargo, lo que persiguen es proporcionar acceso externo al dispositivo de la víctima a través de puertas traseras, en otros casos, lo que se persigue es causar daños mediante la eliminación de archivos, cambios en la configuración del sistema o corrompiendo archivos del sistema operativo para volverlo inestable.

En el caso del ransomware, su propósito final es extorsionar o chantajear a las víctimas sin dañar el sistema operativo o los archivos comprometidos, pero, hay otras características que lo diferencian de otros tipos de malware.

La diferencia más significativa es que a diferencia de otros tipos de malware que requieren permisos de administrador para ejecutar el código malicioso, el ransomware sólo depende de los permisos que actualmente tenga asignados el dispositivo de la víctima dentro de la organización para cifrar los archivos.

El cifrado empleado por el ransomware tiene la capacidad para cifrar todo tipo de archivos, así como para codificar los nombres de estos.

Los ransomware más sofisticados, pueden usar técnicas para evadir su detección por parte de antivirus, así como para sortear las reglas del firewall y en algunos casos conectar el dispositivo de la víctima a una botnet para usarlo como arma en otros ciberataques.

Actualmente, la mayoría de los ransomware se pueden propagar a través de las redes y permiten el robo de información confidencial del dispositivo para enviarla al atacante.

En los últimos tiempos, también tienen en cuenta la ubicación geográfica a fin de presentar la nota de rescate usando el idioma de la víctima y emplean métodos de pago anónimos, normalmente a través de la criptomoneda Bitcoin.

1.6. Síntomas de infección

Para averiguar si un dispositivo ha sido infectado por ransomware, tenemos que prestar atención a los siguientes síntomas:

- No podemos abrir archivos y cada vez que lo intentamos recibimos un mensaje de error indicando que el archivo que estamos intentando abrir tiene la extensión equivocada o está corrupto (imagen 2).

- El fondo de pantalla del escritorio es reemplazado por una imagen que muestra instrucciones de rescate.

- Cuando iniciamos sesión en lugar de acceder al escritorio se muestra una pantalla con instrucciones de rescate.

- Aparece una ventana que cubre la pantalla completa, que no es posible cerrar y que muestra un temporizador de cuenta atrás que alerta al usuario del tiempo restante que queda antes de que se incremente el precio del rescate y de las consecuencias de negarse a pagarlo.

- Aparecen archivos en todos los directorios donde se encuentran los archivos cifrados por el ransomware. Esto archivos suelen tener extensiones como txt, png y html y suelen tener el nombre escrito en letras mayúsculas como, por ejemplo, YOUR_FILES_ARE_ENCRYPTED.html.

- Los nombres de los archivos aparecen codificados y tienen una extensión diferente o no la tienen.

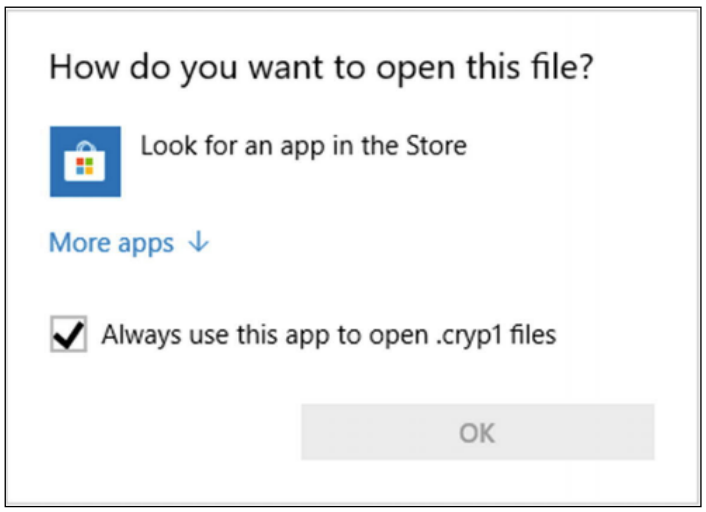

Imagen 2. Aviso de Windows10 para archivos con extensión desconocida.

Capítulo 2

Métodos de distribución del ransomware

En este capítulo, profundizaremos en los diferentes vectores de ataque empleados por los ciberdelincuentes para infectar el dispositivo de la víctima con ransomware dejando de lado las medidas preventivas ya que serán expuestas en los capítulos 3 y 4.

A grandes rasgos, el ransomware emplea las mismas técnicas de distribución que las empleadas por otros tipos de malware, por tanto, profundizaremos en aquellas cuyo uso se encuentra más extendido.

2.1. El correo electrónico

El correo electrónico es el método de distribución más empleado por los ciberdelincuentes para difundir ransomware. En una investigación llevada a cabo por IBM en 2017 se concluyó que el 59% de los ataques de ransomware y el 91% de todo el malware se distribuía a través de correo electrónico [18].

Los servicios de correo electrónico se pueden emplear de diferentes formas para difundir ransomware, principalmente a través de campañas de spam y correos electrónicos de phishing.

La técnica más extendida consiste en enviar mensajes de correo con archivos adjuntos que cuando son descargados y ejecutados infectan el dispositivo al instante.

Otra técnica menos extendida pero igualmente eficaz para difundir ransomware a través del correo electrónico es incrustar enlaces que llevan a sitios web maliciosos que contienen ransomware, cuando la víctima hace clic en ellos, se le redirige al sitio web malicioso que, a su vez, infectará el dispositivo de la víctima.

En la distribución de ransomware mediante spam, se emplean tácticas de ingeniería social para persuadir a los destinatarios a que descarguen y abran archivos adjuntos maliciosos o visiten sitios web infectados haciendo clic en el link suministrado.

Un hecho interesante es que, en marzo de 2021, los mensajes de spam representaron el 45% del tráfico de correo electrónico en todo el mundo, a pesar de todo, el porcentaje ha declinado con respecto a 2018 donde el spam supuso un 55% de todos los correos electrónicos enviados a nivel mundial [19].

En la imagen 3, podemos observar un ejemplo de correo spam empleado para distribuir el ransomware GlobeImposter [20].

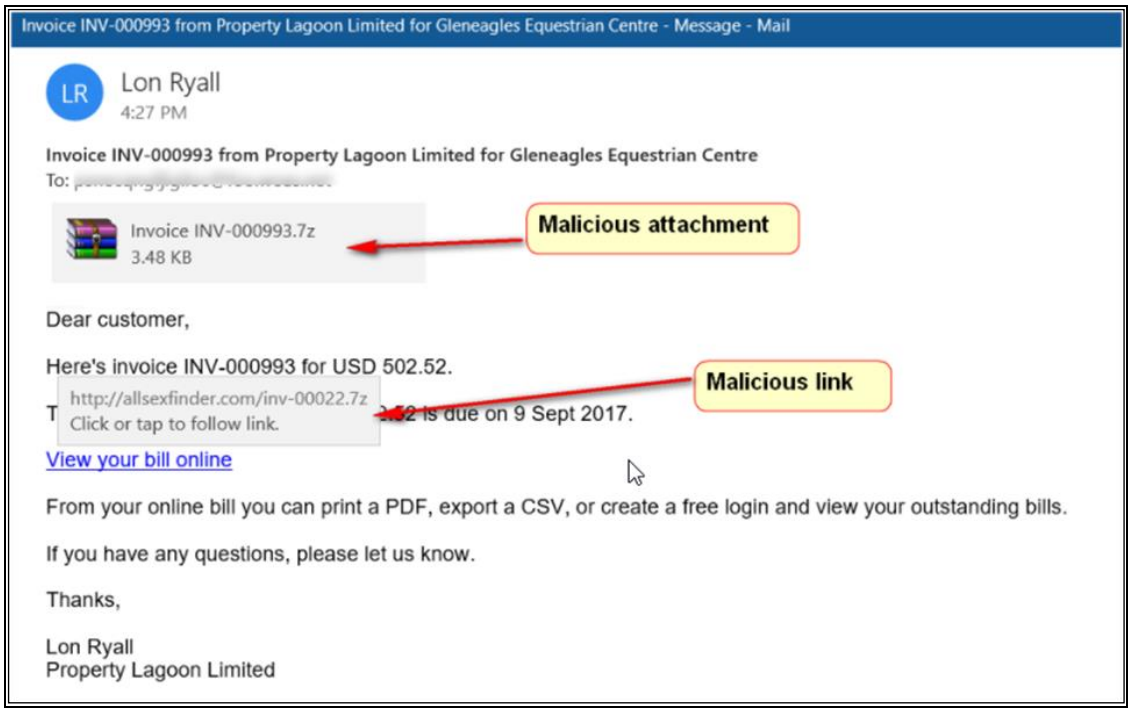

Imagen 3. Ejemplo de campaña de spam para distribuir ransomware.

Los correos electrónicos de spam pueden categorizarse por su contenido:

• **Anuncios no solicitados:** Se envían de forma masiva y sin el permiso del destinatario para promocionar productos o servicios de una entidad comercial.

Aunque la legislación de la mayoría de los países prohíbe este tipo de publicidad, actualmente, su uso continúa estando ampliamente extendido.

• **Correos de phishing:** Se envían de forma masiva a un gran número de personas. Un correo electrónico de phishing pretenderá ser genuino (de una fuente confiable) utilizando el mismo formato que usa la empresa legítima en sus comunicaciones formales, además de usar una redacción inteligente para llamar la atención de la víctima.

El phishing tiene como objetivo recopilar información confidencial del usuario como, por ejemplo, información de inicio de sesión o datos personales engañando a la víctima para que entregue la información al atacante o abra un archivo adjunto que contenga malware (ver imagen 4).

De acuerdo con el objetivo cuya identidad se pretende robar o suplantar, o de acuerdo con la técnica empleada, podemos encontrar varias variantes, algunas de las más extendidas son las siguientes:

• **Spear phishing:** A diferencia de los correos electrónicos de phishing que se envían de forma masiva, el spear phishing es un ataque personalizado que tiene como objetivo a una persona u organización específica.

• **Whale phishing:** Se trata de un ataque similar al spear phishing y utiliza las mismas tácticas, pero se diferencia por estar dirigido a empleados de alto perfil dentro de las organizaciones como directores ejecutivos o directores financieros, su objetivo es robar información confidencial a la que empleados de perfil más bajo no suelen tener acceso.

• **Spoofing:** Se trata de otra variante de phising donde se cambia el encabezado del correo electrónico para que parezca que se originó desde una fuente legítima. En términos generales, los destinatarios están más dispuestos a descargar y abrir archivos adjuntos de correos electrónicos que provienen de fuentes legítimas.

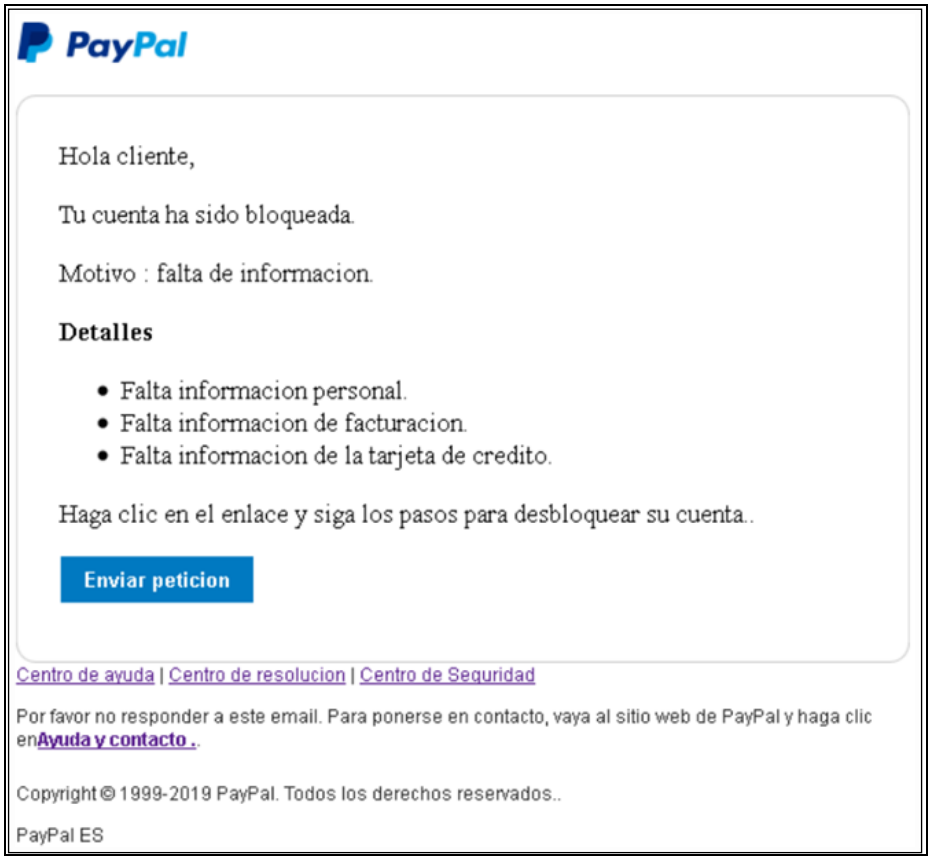

Imagen 4. Ejemplo de correo de phising pretendiendo ser de Paypal

2.2. Suplantación de sitios web

Este tipo de ataques están dirigidos a empresas con altos niveles de seguridad en las que los usuarios visitan frecuentemente sitios web de confianza cuyo contenido está relacionado con la organización a la que pertenecen.

Estos sitios web, han sido previamente estudiados e infectados por los ciberdelincuentes**,** quienes suelen realizar primero un perfil de las víctimas potenciales llevando a cabo un estudio de sus costumbres.

Una vez que un empleado de la compañía objetivo visite el sitio web infectado, infectará su equipo con malware, lo que permitirá a los atacantes tomar el control del equipo y poder así espiar y robar información de la compañía.

Estos ataques basan una gran parte de su éxito en la confianza, ya que los usuarios suelen bajar el nivel de atención cuando se trata de sitios web que visitan diariamente. Estas webs generalmente se encuentran incluidas, incluso dentro de las listas blancas de navegación por los equipos de IT corporativos.

Para evitar la detección por parte de los sistemas de seguridad corporativos, los ciberdelincuentes suelen emplear vulnerabilidades de día 0, es decir, que aún no se han comunicado a empresas de seguridad informática ni a fabricantes para poder crear herramientas de detección y mitigación.

2.3. Malvertising

El malvertising se trata de una técnica que consiste en manipular la publicidad online con el objetivo de infectar dispositivos y buscar agujeros de seguridad en el navegador empleado por la víctima. Cuando el usuario accede a alguno de esos anuncios, se instala malware sin que la víctima sea consciente de ello.

Las estrategias más habituales de malvertising son la esteganografía, el scareware o las actualizaciones de software falsas.

El procedimiento empleado para infectar a las víctimas es el siguiente:

1. El atacante adquiere un espacio publicitario online en una página web relevante para la víctima, por ejemplo, en un medio de comunicación online.

2. El atacante oculta el código malicioso dentro de los anuncios.

3. La víctima carga la página que contiene el anuncio malicioso.

4. La víctima hace clic en el anuncio malicioso lo que hace que el navegador haga una redirección a un sitio web comprometido donde se aloja un exploit kit que al ejecutarse comienza a evaluar el navegador de la víctima en busca de vulnerabilidades, cuando se encuentra una vulnerabilidad, se instala el malware.

2.4. Exploit kits

Un Exploit no es más que un trozo de código, una secuencia de comandos o un pequeño programa que se aprovecha de un bug o vulnerabilidad no detectada, para provocar daños en los dispositivos.

Los exploits suelen distribuirse en packs o kits que llevan a cabo una comprobación de las vulnerabilidades del sistema atacado, en cuanto se detecta una vulnerabilidad o varias, se dispara el exploit correspondiente.

Muchos exploit kits utilizan técnicas de ofuscación de código para evitar ser detectados y cifran las URL para evitar que se deshabiliten.

Sin embargo, hay Exploit kits que actúan sin haber sido detectados todavía, se les conoce como día cero y no tienen solución ya que estos exploits se aprovechan de vulnerabilidades que no han sido detectadas.

Los Exploit kits están formados por 4 componentes:

- **Landing page:** Se trata de una página web que contiene el código responsable de buscar vulnerabilidades en el dispositivo de la víctima, por ejemplo, analizando el navegador y los complementos instalados para averiguar si son vulnerables.

- **Gate:** Se trata del componente que evalúa si continuar con el ataque o cesarlo, la decisión se toma en función de los criterios establecidos por el atacante, por ejemplo:

    - Si el exploit está diseñado para atacar SO Windows y el dispositivo de la víctima está usando Android, entonces, se cesa el ataque.

    - Algunos atacantes, podrían estar diseñando una campaña de distribución de ransomware en una región geográfica en concreto, como, por ejemplo, países de la Unión Europea, por tanto, si la víctima se encuentra en Asia, no hay necesidad de continuar con el ataque.

    - Los Exploit kits más avanzados son capaces de detectar el entorno de ejecución del dispositivo para averiguar si es virtualizado o no, en cuyo caso, se podría decidir no continuar con el ataque.

- **Exploit:** Se trata del componente encargado de explotar la vulnerabilidad detectada por el componente *Landing Page* una vez que se ha comprobado que se cumplen los criterios establecidos para llevar a cabo el ataque,

- **Payload:** Como se ha explicado en el capítulo 1, el payload, es la parte del malware encargada de causar el daño, en el caso del Exploit kit, el payload es el malware que se instalará en el dispositivo de la víctima. El payload puede ser cualquier tipo de malware, incluyendo un downloader que descarga cualquier otro malware.

Entre los exploits más conocidos, se encuentran los siguientes:

- **Angler:** Fue el primero en ser capaz de detectar antivirus y entornos virtualizados, el malware lo ejecuta en memoria sin tener que escribir en el disco duro.

- **Nuclear Pack:** Surgió en 2009, ataca a sus víctimas con un amplio abanico de exploits: Java, Flash, Silverlight, PDF e Internet Explorer.

- **Neutrino:** Surgió en 2016, contiene algunos exploits que se aprovechan de vulnerabilidades en Java, el dueño lo puso a la venta por 34.000 dólares.

- **Blackhole:** Fue la amenaza más extendida en la web en 2012, tenía como objetivo vulnerabilidades de versiones antiguas de navegadores.

- **EternalBlue:** Fue desarrollado por la NSA y filtrado por el grupo de hackers Shadow Brokers en abril del 2017, su fama se debe a que fue usado para distribuir el ransomware WannaCry.

2.5. Memorias USB y medios extraíbles

A pesar de que los ataques basados en dispositivos USB requieren que el atacante tenga acceso físico al dispositivo de la víctima, la distribución de malware mediante dispositivos USB ha aumentado drásticamente a lo largo de los años debido a la falta de conciencia en ciberseguridad de los usuarios.

Hay muchos tipos de malware, especialmente los gusanos, que se propagan a través de memorias USB y medios extraíbles, una vez que la víctima inserta la memoria USB que ha sido comprometida, el malware se instalará automáticamente.

Los ciberdelincuentes utilizan diferentes métodos para infectar y propagar malware a través de dispositivos USB, la más extendida, consiste en colocar de forma intencionada dispositivos USB cargados con malware en las zonas comunes de una organización, como, por ejemplo, el aparcamiento, los baños, cafeterías, etc.

En un experimento llevado a cabo por la universidad de Illinois para medir la efectividad de ataques de este tipo, se colocaron 297 dispositivos USB en todo el campus de la universidad. La gran mayoría de los dispositivos fueron recogidos por personal y estudiantes, y la mitad de ellos fueron insertados en equipos de la universidad [21].

Try2Cry [22], es un ejemplo de ransomware que se propaga a través de memorias USB, cuando se ejecuta, busca unidades USB conectadas al dispositivo infectado y envía una copia de sí mismo llamada Update.exe a la carpeta raíz de cada una de las unidades USB que encuentre, después oculta el archivo en la unidad USB y lo reemplaza por accesos directos a archivos de Windows, cuando se abren, ejecutan el ransomware en segundo plano.

Otro ejemplo es el del gusano Stuxnet que en 2010 resultó en la instalación de malware en una red de centrales nucleares iraníes [23].

2.6. Sitios web de contenido pirata

El malware puede venir incluido como parte de un software, especialmente si ha sido descargado de Internet. La infección ocurre cuando se instala un programa infectado en el dispositivo y el malware que contiene se instala, silenciosamente, al mismo tiempo.

Los programas descargados de sitios web que alojan contenido pirateado suelen venir asociados con un programa ejecutable llamado Crack.exe, Patch.exe o Keygen.exe que desbloquea la versión de prueba del programa pirateado y lo hacen funcionar como el pago.

La ejecución de programas ejecutables para desbloquear software original es peligrosa, especialmente cuando el programa pirateado indica al usuario que desactive el antivirus para evitar conflictos durante la instalación.

La mayoría de los archivos Crack.exe, Patch.exe y Keygen.exe suelen ocultar malware que se instala silenciosamente en el dispositivo de la víctima cuando se ejecutan.

Ryuk, es un ejemplo de ransomware que se distribuyó mediante esta técnica, un caso muy sonado fue el ocurrido en un instituto de investigación biomolecular europeo donde el ataque resulto en la pérdida del trabajo de investigación de toda una semana debido a la ausencia de un backup.

La infección se produjo cuando uno de los estudiantes descargó una copia pirata de una herramienta de visualización de datos y procedió a ejecutarla, en su lugar, lo que instaló fue un conjunto de herramientas de espionaje que permitió a los atacantes obtener las credenciales de acceso del estudiante, lo que les permitió acceder por RDP a la red del instituto e instalar el ransomware.

2.7. Macros de Microsoft Office

Las macros de Microsoft Office son un conjunto de instrucciones y comandos escritos con Visual Basic para Aplicación (VBA) que permiten automatizar tareas en programas de la suite de Microsoft Office como Excel y Word.

Prácticamente desde el nacimiento de las macros de Microsoft Office, los ciberdelincuentes las han usado para llevar a cabo acciones maliciosas como, por ejemplo, usar el comando VBA KILL para eliminar archivos o instalar malware en los dispositivos de las víctimas.

La distribución de malware mediante macros de Microsoft Office es relativamente sencilla, los ciberdelincuentes, suben a un sitio web en Internet el archivo de Microsoft Office que contiene la macro, cuando la víctima abre el archivo infectado, la macro realiza las acciones maliciosas en el dispositivo de la víctima.

En las primeras versiones de Microsoft Office la función de macros se encontraba habilitada de forma predeterminada, sin embargo, esto planteaba un riesgo de seguridad por lo que a partir de Office 2003, Microsoft agregó un nivel de seguridad que evitaba que se cargaran automáticamente (ver imagen 5).

Un ejemplo de ransomware que infecta dispositivos usando macros de Microsoft Word es el ransomware Locky [24].

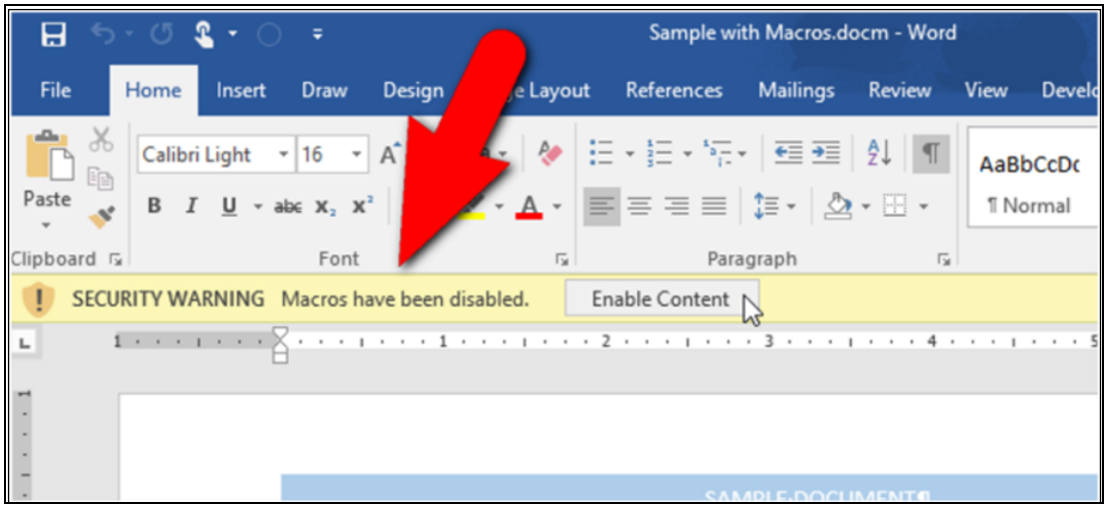

Imagen 5. Aviso emitido por Word cuando se abren archivos con macros

2.8. Ransomware como servicio (RaaS)

Los servicios en la nube han hecho que muchos negocios que tradicionalmente operaban con su propia infraestructura de IT y aplicaciones hayan optado por contratar servicios de IT en la nube para reducir sus costes operativos.

En la actualidad, existen diferentes modelos de servicios en la nube, los 3 más comunes son los siguientes:

- Software como servicio (SaaS): Consiste en el acceso y uso de aplicaciones alojadas en la nube a través de internet, un ejemplo sería Office 365.

- Infraestructura como servicio (IaaS): Consiste en el uso de infraestructura de IT como, por ejemplo, servidores web, servidores de correo, bases de datos, etc. Un ejemplo de IaaS es Microsoft Azure o Amazon Web Services.

- Plataforma como servicio (PaaS): Se trata de servicios empleados por desarrolladores para construir aplicaciones en la nube. Un ejemplo de PaaS es Visual Studio Team Services.

El modelo de ransomware como servicio (RaaS) adopta un enfoque similar al de software como servicio (SaaS), el RaaS consiste en publicar un servicio en la nube y luego comercializarlo en el mercado negro y en foros de la dark web para distribuir ransomware utilizando un modelo de suscripción, lo que simplifica enormemente los ataques para ciberdelincuentes novatos.

A cambio del servicio proporcionado, los fabricantes del RaaS obtienen un porcentaje de los rescates pagados por las víctimas.

RaaS es un modelo de negocio emergente que normalmente implica a 3 actores: el autor del malware, el proveedor del servicio y los agentes de ataque.

Los autores de malware se responsabilizan de desarrollar el código del ransomware y de las instrucciones para su uso, después lo integran en un dashboard online del proveedor del servicio para disponerlo para venta o alquiler. Los agentes, son ciberdelincuentes que acceden al dashboard donde después de pagar por el servicio, parametrizan el ransomware y monitorizan el estado de los pagos llevados a cabo por las víctimas que han sido infectadas.

En la imagen 6, podemos observar un ejemplo de RaaS llamado DataKeeper, que permite a los ciberdelincuentes personalizar el ransomware, este servicio se encuentra alojado en la red TOR [25].

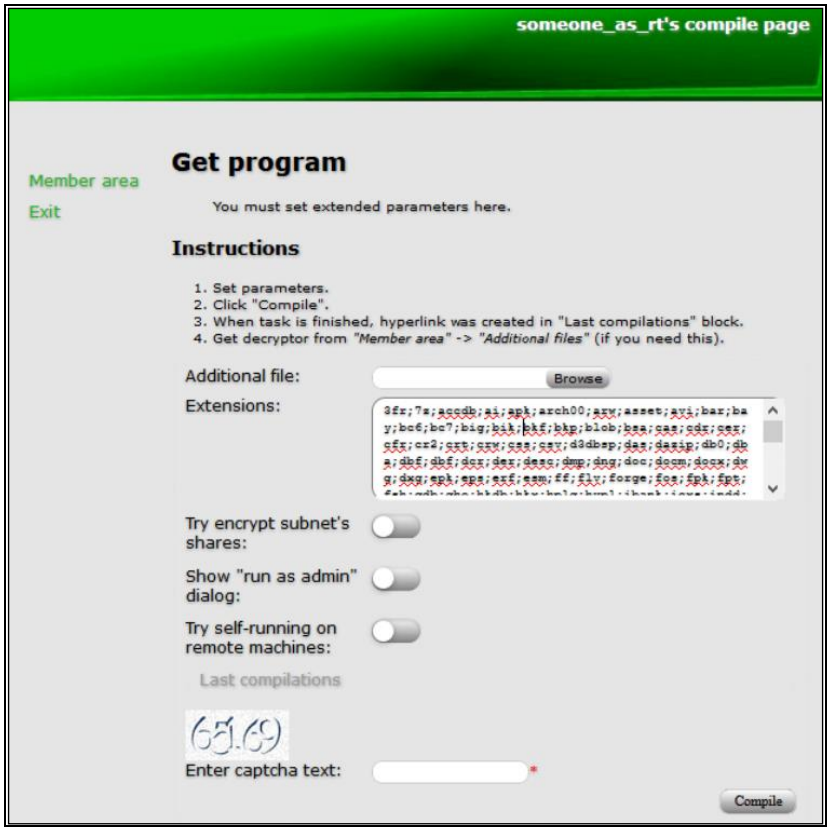

Imagen 6. Pantalla de configuración del RaaS DataKeeper

2.9. Conexión a escritorio remoto

En la actualidad, muchas empresas subcontratan parte de sus operaciones e infraestructura de IT a proveedores de servicios de IT. Aunque en la mayoría de los casos estos proveedores suelen estar ubicados en el mismo país que sus clientes, en ocasiones, se ubican en el extranjero.

Para permitir que los empleados puedan teletrabajar y que los proveedores de servicios realicen su trabajo, Windows ofrece el protocolo de escritorio remoto o RDP (remote desktop protocol).

Mediante el protocolo RDP, se permite al proveedor de servicios de IT acceder a la pantalla, teclado y ratón del equipo remoto del cliente usando una combinación de usuario y contraseña.

Los ciberdelincuentes, suelen emplear ataques de fuerza bruta explotando contraseñas débiles y técnicas de ingeniería social para obtener las credenciales de inicio de sesión en el equipo remoto, después de adquirir esta información, el atacante tiene vía libre para acceder al equipo remoto de la víctima e instalar malware, así como para infiltrarse en la red.

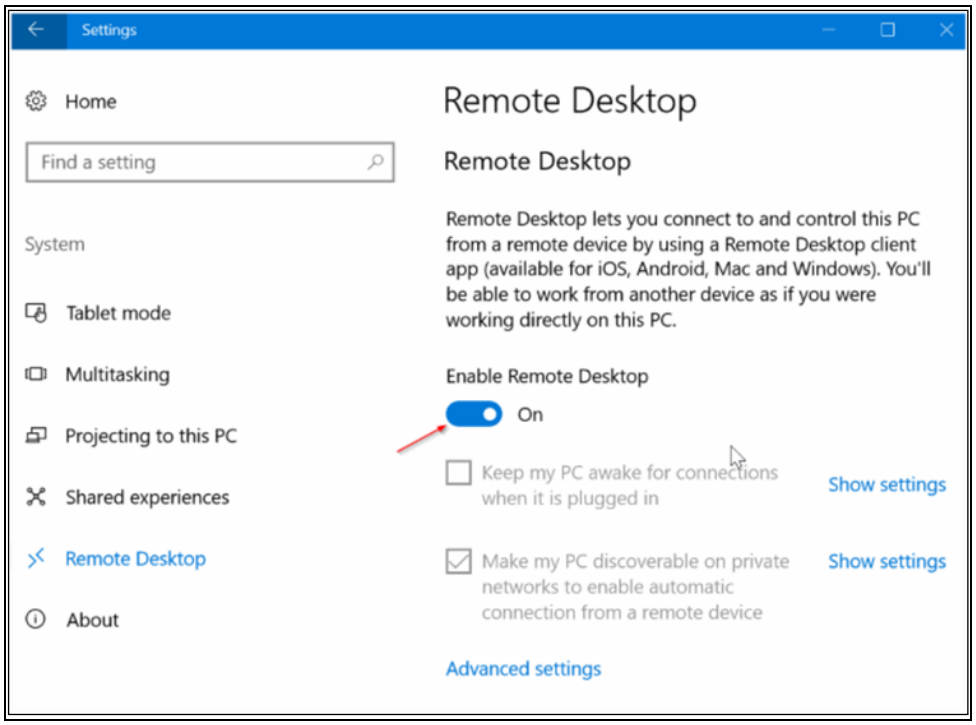

Imagen 7. Activación del acceso remoto al escritorio con Windows 10.

Actualmente, en Internet, podemos encontrar sitios web como Shodan (https://www.shodan.io), que nos facilita la localización de dispositivos de IoT que tienen comprometido el acceso por RDP [26].

La pandemia del COVID-19 ha cambiado radicalmente la naturaleza del trabajo, obligando a los empleados a realizar gran parte de su trabajo a través de RDP. Conscientes del cambio de escenario, los ciberdelincuentes han intentado explotar la oportunidad para aumentar sus ganancias.

Pese a la creciente importancia del RDP y de otros servicios de acceso remoto, las organizaciones a menudo descuidan su correcta configuración y no hacen uso de capas adicionales de autenticación o protección, lo que ha contribuido a que los ciberdelincuentes hayan convertido este vector de ataque en uno de los más usados en 2019 y 2020 para distribuir ransomware.

2.10. Proveedores de servicios de IT

Los proveedores de servicios de IT son empresas que ofrecen servicios como, por ejemplo, soporte remoto para infraestructura de IT, monitorización de red, administración remota de firewalls, sistemas de detección de intrusiones (IDS), administración de dispositivos móviles, gestión de incidentes de seguridad y otros servicios de consultoría.

Los clientes de un proveedor de servicios de IT suelen ser pequeñas y medianas empresas que tienen un personal de IT reducido y que necesitan subcontratar algunas de sus tareas para reducir sus costes operativos.

Para realizar el trabajo de forma remota, algunos proveedores de servicio de IT utilizan software especializado para acceder de forma remota a la infraestructura de IT de sus clientes.

Sin embargo, en los últimos tiempos, los ciberdelincuentes han comenzado a piratear el software empleado para el acceso remoto a fin de distribuir ransomware y otro tipo de malware entre las empresas que subcontratan parte de sus funciones de IT a proveedores de servicios. REvil es un ejemplo de ransomware que se propaga utilizando este método [27].

2.11. Botnets

Las botnets ya fueron mencionadas en el Capítulo 1, un bot es un dispositivo cuya seguridad ha sido comprometida y que es controlado por un servidor o botmaster y usado para lanzar junto con otros miles o incluso millones de dispositivos comprometidos (bots) ataques de denegación de servicio distribuidos (DDoS), campañas de phising o enviar malware a otros dispositivos.

Sin embargo, las botnets puede explotarse para jugar otro papel como, por ejemplo, descargar ransomware o cualquier otro tipo de malware del servidor para infectar el propio dispositivo (bot) que forma parte de la botnet.

Tal y como se mencionó en el capítulo 1, Cryptolocker fue el primer ransomware en utilizar una botnet como método de distribución.

Sin embargo, Cryptolocker no fue el único caso, en 2020, Microsoft bloqueó Trickbot, una peligrosa botnet conocida por infectar a más de 1 millón de dispositivos en todo el mundo con el ransomware Ryuk.

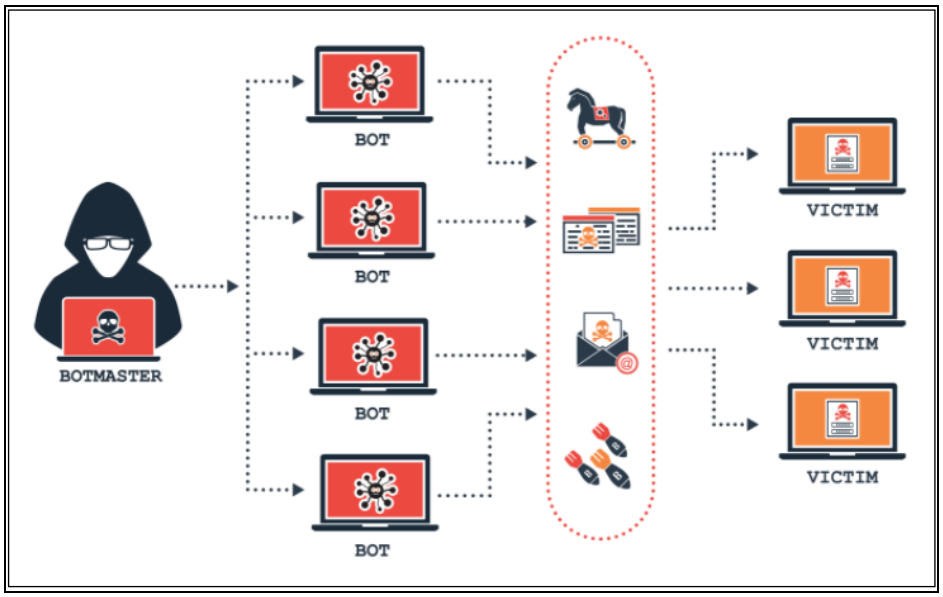

Imagen 8. Esquema de una botnet.

2.12. Vulnerabilidades de día cero

Las vulnerabilidades de día cero, son aquellas que no han sido todavía descubiertas ni por el fabricante del software ni por los fabricantes de antivirus.

Dentro de la ciberseguridad, están consideradas las vulnerabilidades más peligrosas puesto que si un ciberdelincuente consigue encontrar una vulnerabilidad de día cero antes que el fabricante o que un proveedor de antivirus, podrá explotarla mientras no sea remediada.

Es muy frecuente la venta en el mercado negro y en la dark web de exploits que aprovechan este tipo de vulnerabilidades, su precio se establece en base a su impacto y al número de dispositivos vulnerables.

2.13. Falta de formación

Todos los años, grandes empresas sufren ataques de ciberseguridad que resultan en la exposición de millones de datos confidenciales.

Varias investigaciones apuntan a que la falta de conciencia en ciberseguridad y la falta de personal capacitado para contener los ataques y monitorizar la red juega un papel clave a la hora de exponer a las organizaciones a diferentes amenazas, especialmente, el ransomware.

La conciencia y la capacitación de los empleados de una empresa sobre ciberseguridad se considera el primer dique de contención para proteger los sistemas informáticos de una empresa ya que garantiza que los empleados están al tanto de las diferentes técnicas de ataque que pueden emplear los ciberdelincuentes para atacar los sistemas de la organización y que tienen el conocimiento de cómo mitigar y reportar los incidentes de seguridad usando el canal apropiado.

Todas las soluciones de ciberseguridad empleadas por una empresa para protegerse de los ataques como por ejemplo, el empleo de firewalls para proteger el acceso a la intranet, sistemas de detección de intrusos (IDS), antivirus corporativos, etc., son inútiles si un solo empleado hace clic de forma inconsciente en un enlace malicioso dentro de un correo electrónico de phising ya que pondrá en peligro a toda la red corporativa haciendo que todas las medidas de protección implementadas resulten inútiles.

En el Anexo III del presente trabajo fin de master se aborda en detalle la formación en ciberseguridad como mecanismo de prevención.

Capítulo 3

Métodos de defensa en equipos de usuario

Los ataques de ransomware pueden afectar a cualquier tipo de dispositivo, pero estadísticamente son los dispositivos conectados a la red los que reportan la mayor cantidad de incidentes.

Desde el nacimiento de Internet, la seguridad de los dispositivos se ha considerado el primer dique de contención contra los ataques de malware.

La seguridad de dispositivos es un término empleado para describir todas las tecnologías y técnicas empleadas para dotar de protección contra ataques de malware a un dispositivo informático y es una de las claves para proteger las redes ya que la mera existencia de un solo dispositivo cuya seguridad se encuentre comprometida, hace vulnerable a toda la red.

En este capítulo se profundizará en los diferentes elementos de defensa que podemos emplear para conseguir que un dispositivo de usuario conectado a la red sea menos vulnerable a ataques de ransomware.

3.1. Instalación de soluciones Antivirus

La instalación de buen software de antivirus sigue siendo la primera línea de defensa de un dispositivo conectado a la red contra ataques de malware.

Actualmente, existen muchas soluciones de antivirus gratuitas, sin embargo, la mayoría de ellas carecen de las características necesarias para prevenir ataques de ransomware.

Los antivirus más completos, incluyen un firewall integrado y otros complementos de protección como soluciones antispam y antiphising que dotan de una capa extra de defensa para prevenir infecciones de malware a través del correo electrónico.

No es aconsejable instalar más de un antivirus en el mismo dispositivo ya que puede dar lugar a problemas de incompatibilidad, sin embargo, es habitual que en entornos corporativos se usen diferentes soluciones de antivirus en función del tipo de dispositivo que se desea proteger ya que hoy en día, existen soluciones especializadas para servidores web, servidores de correo, puertas de enlace, equipos de usuario, etc.

No debemos olvidar que la protección proporcionada por el antivirus por si misma es insuficiente contra ataques de ransomware cuyo vector de ataque empleado son los correos de phising o los ataques de ingeniería social donde las personas sin concienciación en ciberseguridad son el eslabón más débil.

3.2. Mantener el dispositivo actualizado

Mantener actualizados tanto el sistema operativo como las aplicaciones instaladas, es otro de los elementos clave en la defensa no solo contra ransomware, sino contra todo tipo de malware.

Tal y como se pudo ver en el Capítulo 2, los exploit kits son uno de los vectores de ataque empleados para distribuir ransomware donde el método de infección consiste en dirigir a la víctima a un sitio web que explorará el dispositivo en busca de aplicaciones vulnerables que permitan la ejecución del ransomware.

Para reducir el riesgo de que un exploit kit sea ejecutado en aplicaciones vulnerables, debemos asegurarnos de que todas las aplicaciones instaladas se encuentren actualizadas, sobre todo, el navegador, los complementos del navegador y las soluciones de antivirus.

La forma más sencilla de mantener el sistema actualizado es usar un programa de gestión de parches y actualizaciones. Los programas de gestión de parches y actualizaciones controlan las versiones de todas las aplicaciones instaladas en el dispositivo y las actualiza automáticamente cuando el fabricante libera una nueva versión o un parche de seguridad. Algunos programas de gestión de parches y actualizaciones son:

- Patch Management Software de ManageEngine
- Software Updater de Avira
- Patch My PC Updater
- IObit Software Updater

En entornos corporativos, es aconsejable usar directivas para controlar las actualizaciones automáticas en los equipos (ver imagen 9).

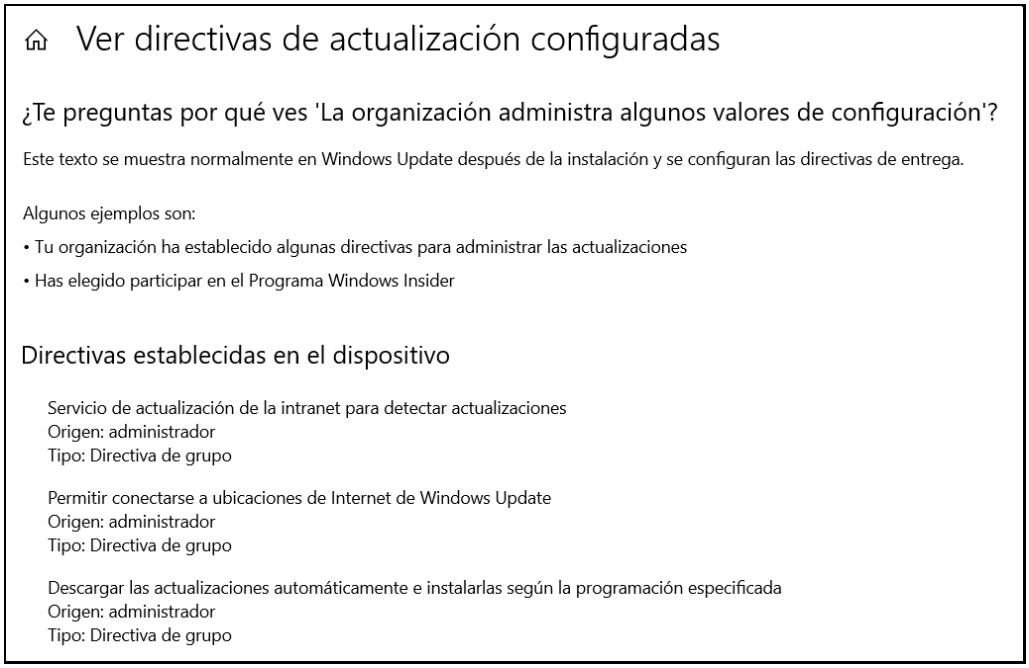

Imagen 9. Pantalla de directivas de actualización de Windows10.

El uso de software con mantenimiento descontinuado está completamente desaconsejado, por ejemplo, Microsoft ya no proporciona actualizaciones de seguridad ni soporte técnico para Windows XP, Windows Vista y Windows7.

Los sistemas operativos con mantenimiento descontinuado pueden contener agujeros de seguridad que no serán reparados por el fabricante y, por tanto, pueden ser explotados para eludir el antivirus e incluso el firewall y de este modo infectar el dispositivo de la víctima y la red a la que está conectado.

Para terminar, es muy importante no olvidarse de actualizar el firmware en los dispositivos de red como routers, switches y balanceadores.

3.3. Usar entornos virtualizados

El uso de tecnología de virtualización nos permite proteger los dispositivos informáticos de ransomware y otras amenazas de malware.

Mediante el uso de un sistema operativo virtualizado, podemos ejecutar programas, abrir archivos adjuntos de correo electrónico, descargar e instalar programas de Internet y visitar sitios web comprometidos de forma segura sin preocuparnos de infectar el sistema operativo con malware, ya que los sistemas operativos virtualizados se ejecutan en un entorno que se encuentra aislado del sistema operativo anfitrión.

Las soluciones de virtualización más empleadas hoy en día por los equipos de IT de grandes empresas son Oracle VirtualBox y VMware Workstation.

La tecnología de virtualización también puede usarse para crear entornos de sandbox donde ejecutar aplicaciones en un entorno aislado sin tener que virtualizar el sistema operativo completo, algunas de las soluciones de sandboxing más populares son:

- Shade Sandbox
- Sandboxie
- BitBox

También existen algunas soluciones online de sandbox como WebGap, que nos permite navegar por la web aislando el navegador y su actividad del dispositivo y de la red a la que se encuentra conectado.

Sin embargo, existen familias de ransomware que tienen capacidad para detectar si el código malicioso se está ejecutando en un entorno virtualizado o de sandbox para de este modo, alterar su comportamiento y evitar la detección o decidir no ejecutar las acciones maliciosas.

3.4. Deshabilitar redirecciones en el navegador

Controlar las redirecciones en el navegador nos permitirá evitar ser redireccionados a sitios web fraudulentos o maliciosos.

Los principales navegadores web pueden configurarse para evitar que se produzcan redireccionamientos, por ejemplo, para configurar esta función en Google Chrome debemos hacer lo siguiente:

1. Abrir los ajustes de ventanas y redirecciones de Chrome, la forma más rápida de hacerlo es a través de la siguiente URL:

   chrome://settings/content/popups

2. Configuramos la opción “No permitir que los sitios envíen ventanas emergentes ni utilicen redirecciones” (ver imagen 10).

Los navegadores más modernos también disponen de protección integrada contra phising y malware, esta funcionalidad se basa en listas negras de enlaces maliciosos que son conocidos por tratarse de sitios web de phising o por albergar exploit kits y otros tipos de malware, de este modo, en caso de que el usuario intente descargar algo de un sitio web catalogado como malicioso, el navegador bloqueará la descarga.

Para habilitar esta función en Chrome, debemos hacer lo siguiente:

1. Abrir los ajustes de seguridad de Chrome, la forma más rápida de hacerlo es a través de la siguiente URL:

   chrome://settings/security

2. En el apartado “Navegación segura”, seleccionamos la opción “Protección estándar” (ver imagen 11).

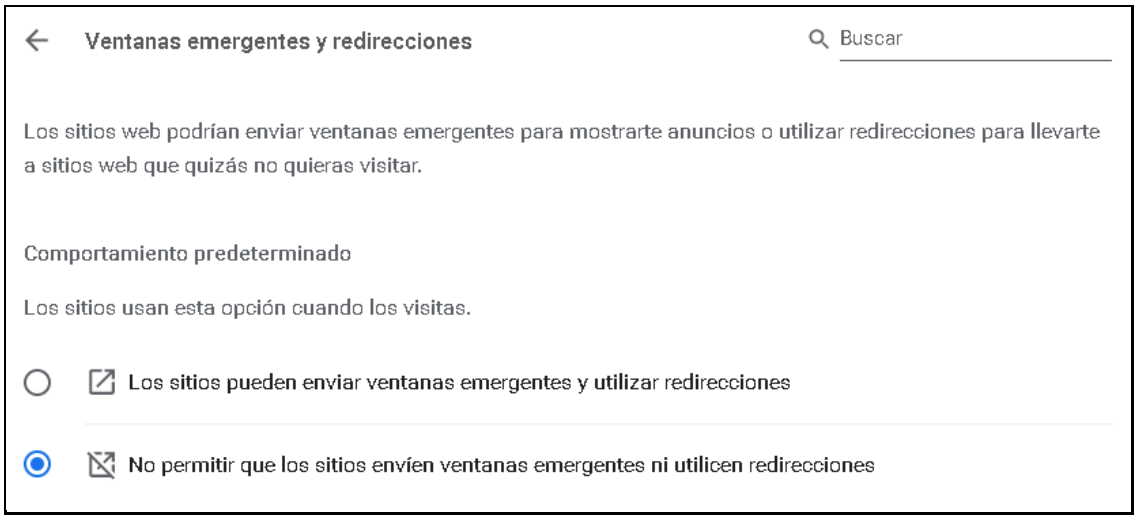

Imagen 10. Configuración de ventanas emergentes en Chrome.

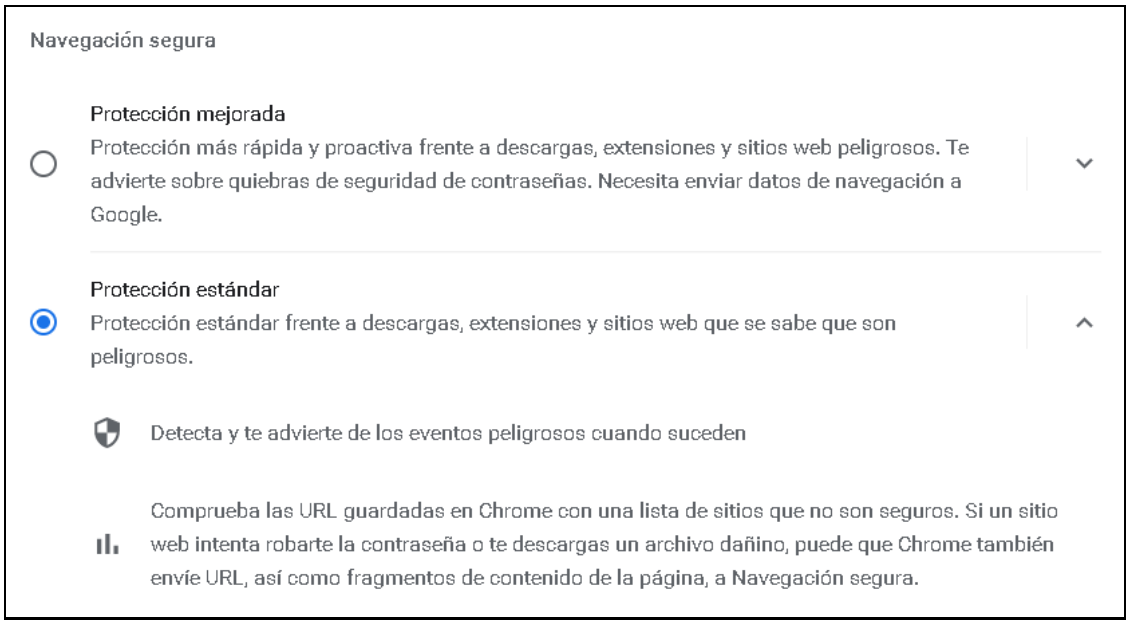

Imagen 11. Configuración de navegación segura en Chrome.

En entornos corporativos, lo habitual es que la configuración del navegador sea administrada de forma remota por el departamento de IT.

3.5. Instalar plugins de seguridad en el navegador

Existen plugins de navegadores web que mejoran la privacidad y ayudan a prevenir ataques de ransomware, por ejemplo, hay plugins que permiten bloquear anuncios maliciosos y ventanas emergentes que reducen las probabilidades de infección por malvertising. Algunos ejemplos son:

- Privacy Badger: Bloquea los anuncios espía y las etiquetas en las páginas web que recogen información sobre los hábitos y preferencias del usuario.
- HTTPS Everywhere: Cifra las comunicaciones con los principales sitios web, lo que hace que su navegación sea más segura.
- NoScript: Permite que Javascript, Java, Flash y otros complementos sean ejecutados solo por los sitios web configurados por el usuario.
- uBlock Origin: Bloquea anuncios de uso general, ventanas emergentes y etiquetas que recogen los hábitos y preferencias del usuario.

Hay que tener en cuenta que algunos sitios web que suministran plugins para navegadores pueden engañar a los usuarios y recopilar datos privados sobre hábitos de navegación sin su consentimiento, por lo que es recomendable verificar la reputación del fabricante del plugin antes de instalarlo.

En entornos corporativos, lo habitual es que ciertos plugins del navegador sean administrados de forma remota por el departamento de IT.

3.6. Deshabilitar las macros en archivos de Office

Tal y como se expuso en el Capítulo 2, las macros de Microsoft Office permiten automatizar ciertas tareas en la suite de Microsoft Office, pero pueden ser empleadas para instalar ransomware en el dispositivo de la víctima.

Aunque las macros están deshabilitadas de forma predeterminada en las últimas ediciones de Microsoft Office, es importarte asegurarse de que no las habilitamos en documentos descargados de Internet o que hayan sido recibidos a través de correo electrónico no deseado.

Para evitar correr el riesgo, es aconsejable abrir aquellos archivos de Office enviados por correo utilizando un visor de documentos, lo más práctico en estos casos es usar un visor online como, por ejemplo, el visor de documentos de algún servicio de almacenamiento en la nube como Google Docs, OneDrive o Dropbox.

En entornos corporativos, la medida más recomendable a tomar es deshabilitar las macros siguiendo una política de grupo si no fuesen necesarias, o habilitar el 'modo lectura' de Microsoft Office.

3.7. Deshabilitar WSH

WSH o Windows Script Host es un lenguaje de scripting que viene de serie con todas las versiones de Windows desde Windows98.

El propósito de los scripts WSH, es el mismo que el de las macros de Office, es decir, automatizar tareas, en el caso de los scripts de WSH, tareas llevadas a cabo dentro del sistema operativo Windows.

En términos generales, el scripting es una herramienta que dota de gran potencia a cualquier sistema operativo, sin embargo, puede resultar un problema de seguridad cuando el script proviene de una fuente no confiable como, por ejemplo, un archivo adjunto o un sitio web malicioso.

Para reducir el riesgo de seguridad, es aconsejable deshabilitar la ejecución de scripts de WSH en todos aquellos dispositivos conectados a la red y en servidores cuando no se use de forma habitual.

Para deshabilitar Windows Script Host en un equipo con Windows10, es necesario editar el registro de Windows (ver imagen 12), en el siguiente link se detallan las instrucciones de configuración:

Cómo deshabilitar Windows Script Host

Para confirmar que WSH se ha deshabilitado correctamente, creamos un archivo de texto y le cambiamos la extensión de *.txt a *.vbs. Al intentar ejecutarlo, recibiremos el siguiente mensaje de error:

"Acceso a Windows Script Host deshabilitado en este equipo. Póngase en contacto con su administrador para obtener más detalles".

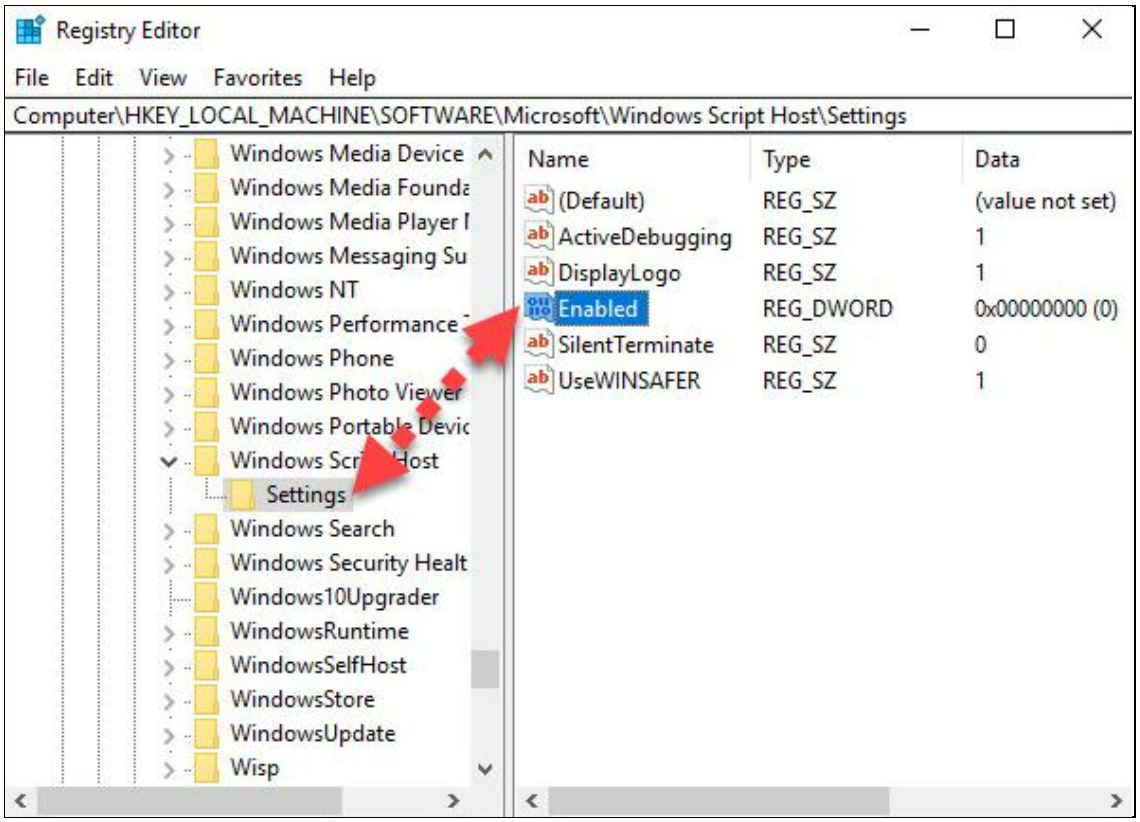

Imagen 12. Deshabilitar Windows Script Host en el registro de Windows.

3.8. Deshabilitar Powershell 2.0

PowerShell es una interfaz de línea de comandos que tiene la posibilidad de ejecutar scripts para facilitar la automatización de tareas de configuración y administración, permitiendo interactuar, tanto con el sistema operativo como con otros programas propios de Microsoft.

Algunas familias de ransomware se apoyan en PowerShell para llevar a cabo la ejecución en memoria, lo que ayuda a evadir la detección de los antivirus.

Windows10 instala por defecto PowerShell para todos los usuarios, concretamente la versión 5.0, sin embargo, además de instalar esta versión, también deja habilitadas otras versiones como PowerShell 2.0, versión ya obsoleta y con mantenimiento descontinuado.

Para comprobar si tenemos habilitada la consola PowerShell 2.0 en Windows10, tan solo debemos abrir una ventana de esta consola con permisos de administrador y ejecutar el siguiente comando:

Get-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2

En caso de tener la versión 2.0 de PowerShell habilitada, podríamos estar en peligro dado que mientras que PowerShell 5.0 cuenta con protección contra malware, la versión 2.0 no lo tiene, y los ciberdelincuentes fácilmente podrían hacer una llamada al motor de la versión 2.0 para llevar a cabo sus ataques.

Para deshabilitar PowerShell 2.0, debemos ejecutar el siguiente comando:

Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root

Sin embargo, si no hubiera necesidad de usar Powershell, se recomienda deshabilitar la ejecución de scripts en Powershell mediante políticas de grupo o restringir por completo el acceso a la interfaz de línea de comandos.

Windows PowerShell tiene cuatro políticas de ejecución diferentes:

- Restricted: Prohíbe ejecutar scripts.
- AllSigned: Solo permite ejecutar scripts firmados por un editor de confianza.
- RemoteSigned: Las secuencias de comandos descargadas deben estar firmadas por un editor de confianza antes de poder ejecutarlas.
- Unrestricted: Todos los scripts de se pueden ejecutar.

Para establecer la política de ejecución restringida se debe ejecutar el siguiente comando:

powershell Set-ExecutionPolicy -ExecutionPolicy Restricted

3.9. Limitar los permisos de usuario

Hay muy pocas familias de ransomware que necesiten privilegios de administrador para funcionar correctamente, ya que la mayoría de ellas, dependen del nivel de permisos del usuario que se encuentra autenticado.

Sin embargo, el uso de cuentas de usuario con pocos privilegios es una medida efectiva contra diferentes tipos de malware, ya que una cuenta de usuario con permisos limitados no puede instalar programas ni realizar modificaciones importantes en la configuración del sistema operativo, como, por ejemplo, agregar o modificar claves del registro.

Muchos estudios muestran que el uso de una cuenta de usuario con permisos limitados ayuda a limitar los efectos de la mayoría de las infecciones de malware, por ejemplo, un estudio llevado a cabo por un partner de McAfee en 2017 reveló que el 94% de las vulnerabilidades reportadas por Microsoft podían remediarse usando cuentas de usuario estándar [28].

Con el lanzamiento de Windows Vista en 2007, Microsoft introdujo una nueva característica de seguridad para solicitar el consentimiento del usuario cuando se requieran llevar a cabo modificaciones en los archivos o configuración del SO, a esta característica se la denominó, User Account Control (UAC).

Las modificaciones en el sistema operativo pueden provenir de aplicaciones, usuarios, procesos o cualquier forma de malware. Cuando el sistema operativo detecta que se está intentando modificar la configuración o alguno de los archivos del sistema, mostrará un mensaje por pantalla avisando al usuario y solicitando su consentimiento expreso.

En Windows10, el nivel de seguridad proporcionado por la característica de UAC se establece a través del panel de control (ver imagen 13), en el siguiente link se detallan las instrucciones de configuración:

Cómo ajustar el nivel de seguridad de UAC

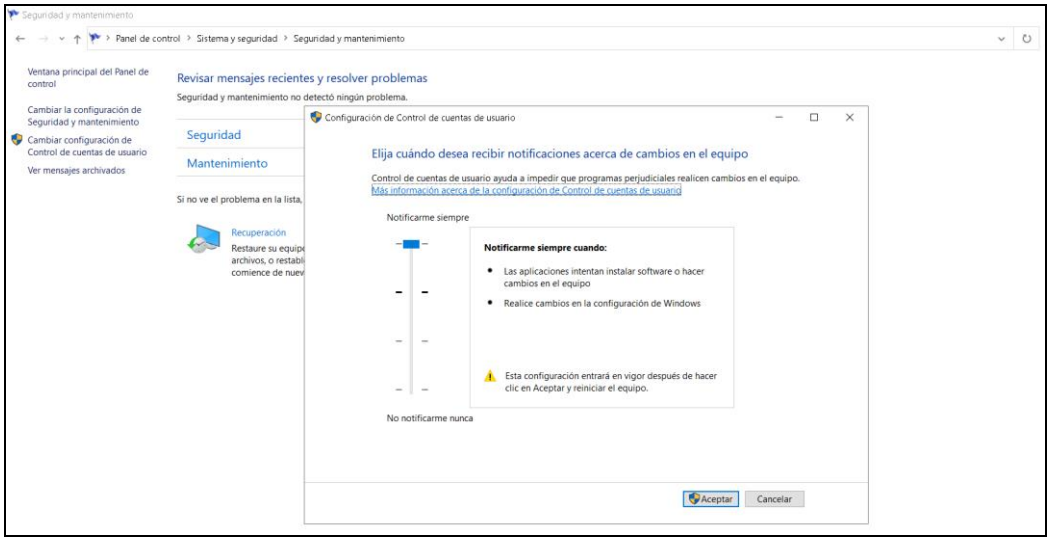

Imagen 13. Configuración del nivel de seguridad de la UAC en Windows10.

Aunque las familias más modernas de ransomware pueden eludir la UAC e infectar el dispositivo sin requerir el consentimiento del usuario, habilitar la UAC sigue siendo aconsejable especialmente para usuarios con permisos de administración.

3.10. Instalar software con licencia

Algunos usuarios no están dispuestos a comprar una licencia de software comercial y optan por descargar software pirata lo que les expone a ser infectados con malware y a ser denunciados por piratería a la BSA, la asociación de los principales fabricantes de software.

Los programas descargados de sitios web que alojan contenido pirateado suelen venir asociados con un programa ejecutable llamado Crack.exe, Patch.exe o Keygen.exe que desbloquea la versión de prueba y lo hacen funcionar como el de pago, estos archivos ejecutables, pueden incluir ransomware.

Al riesgo que supone instalar software pirateado se suma el hecho de que las versiones no genuinas de sistemas operativos no suelen recibir actualizaciones lo que puede comprometer la seguridad del dispositivo a largo plazo.

Un estudio llevado a cabo sobre el impacto de WannaCry reveló que una buena parte de los dispositivos que fueron infectaron en China y Rusia utilizaban versiones pirateadas del SO Windows que no podían recibir actualizaciones [29].

En estos casos, aun cuando Microsoft haya remediado la vulnerabilidad y haya publicado el parche, los dispositivos continuaran siendo vulnerables.

3.11. Evitar memorias USB no confiables

En la actualidad, la distribución de malware mediante memorias USB ha caído en desuso debido a la proliferación de servicios en la nube que permiten transferir datos de unos dispositivos a otros. Aun así, la propagación de malware mediante memorias USB sigue siendo uno de los vectores de ataque a tener en cuenta.

Cuando un dispositivo USB se encuentra infectado con ransomware, la víctima corre el riesgo de dañar los archivos almacenados en el dispositivo al cual se encuentra conectado.

Además, en el caso de las familias de ransomware más modernas, también se corre el riesgo de que el ransomware se propague automáticamente por la red a la que se encuentra conectado el dispositivo infectado, por tanto, se debe evitar conectar memorias USB que provengan de una fuente no confiable en los equipos de trabajo o del hogar.

En caso de que fuera necesario ver el contenido de una memoria USB no confiable, es aconsejable hacerlo en un entorno virtualizado sin conexión a la red, de este modo, si la memoria USB se encuentra infectada con ransomware, evitaremos propagarlo por la red y dañar el dispositivo anfitrión.

3.12. Proteger los dispositivos móviles

Los dispositivos móviles, especialmente aquellos con sistema operativo Android, son el principal objetivo de los ataques de ransomware.

Para reducir la superficie de ataque, es recomendable tomar las siguientes contramedidas:

- Evitar ‘rootear’ el dispositivo ya que permitirá que todas las acciones se ejecuten con acceso de administrador y se expongan archivos del SO.
- Mantener actualizado el sistema operativo y las aplicaciones instaladas.
- Instalar aplicaciones de una fuente de confianza como, por ejemplo, de Google Play en dispositivos Android y de Apple Store en dispositivos iPhone.
- En dispositivos Android, conceder acceso a Google para analizar el estado.
- Evitar hacer clic en enlaces incrustados en correos electrónicos y mensajes SMS que provengan de fuentes poco confiables.
- Evitar descargar y ejecutar archivos adjuntos en correos electrónicos que provenga de fuentes sospechosas.
- Instalar soluciones antimalware especializadas en dispositivos móviles.

- Cuando se instale una nueva aplicación, comprobar los permisos requeridos.
- En entornos corporativos, configurar una lista negra de aplicaciones.
- Configurar copias de seguridad en la nube de los datos almacenados.
- Se debe evitar la conexión a la red corporativa usando una conexión WiFi-gratuita como las disponibles en lugares públicos como aeropuertos.
- Utilizar contraseñas seguras para proteger el dispositivo.
- En los dispositivos móviles corporativos se recomienda el uso de software de cifrado que dificulte la extracción de datos en caso de pérdida o robo.

3.13. Evitar puntos de carga públicos

Cuando conectamos un dispositivo a un punto de carga público, por ejemplo, un aeropuerto o una estación de tren, corremos el riesgo de ser víctimas de un ataque de extracción de jugo (juice jacking attack).

Los ataques de extracción de jugo permiten obtener acceso no autorizado e incluso inyectar ransomware en el dispositivo de la víctima, una vez que el dispositivo ha sido infectado, el ransomware se propagará a otros dispositivos cuando nos conectemos a una red.

Para evitar correr el riesgo de sufrir un ataque de extracción de jugo, es aconsejable, disponer de una fuente portable de energía (powerbank).

3.14. Hacer copias de seguridad

Actualmente, la forma más segura de restaurar los datos comprometidos por un ataque de ransomware sin pagar el rescate, es tener una copia de seguridad:

Cuando se diseña una estrategia de backup, hay que considerar lo siguiente:

- Priorizar los datos de acuerdo con su importancia para el usuario.
- Los datos más importantes deben copiarse a medida que se modifican.
- Una vez que se finaliza la copia, se debe desconectar el medio de almacenamiento de la copia de seguridad del dispositivo.
- Verificar la disponibilidad de los archivos de backup periódicamente.
- No se debe confiar únicamente en una copia de seguridad, sobre todo si se encuentra en la nube ya que un ataque de ransomware podría sobrescribir los datos con una versión cifrada de los mismos.

A continuación, se describirán brevemente las 2 características de backup más conocidas que vienen de serie con el sistema operativo Windows.

Habilitar la característica de copia oculta (Shadow Copy)

VSS (volumen shapshot service) es un servicio de backup disponible en Windows a partir del lanzamiento de WindowsXP.

Las copias de seguridad realizadas con VSS se denominan snapshots y pueden ser creadas de forma automática por Windows o manualmente por el usuario para almacenarse en el disco duro local o en uno externo.

En Windows10, VSS se configura en la ventana de propiedades del sistema a la cuál podemos acceder bien a través del panel de control o mediante la ejecución del comando *sysdm.cpl* (ver imagen 14), en el siguiente link se detallan las instrucciones:

[Configuración de VSS en Windows10]

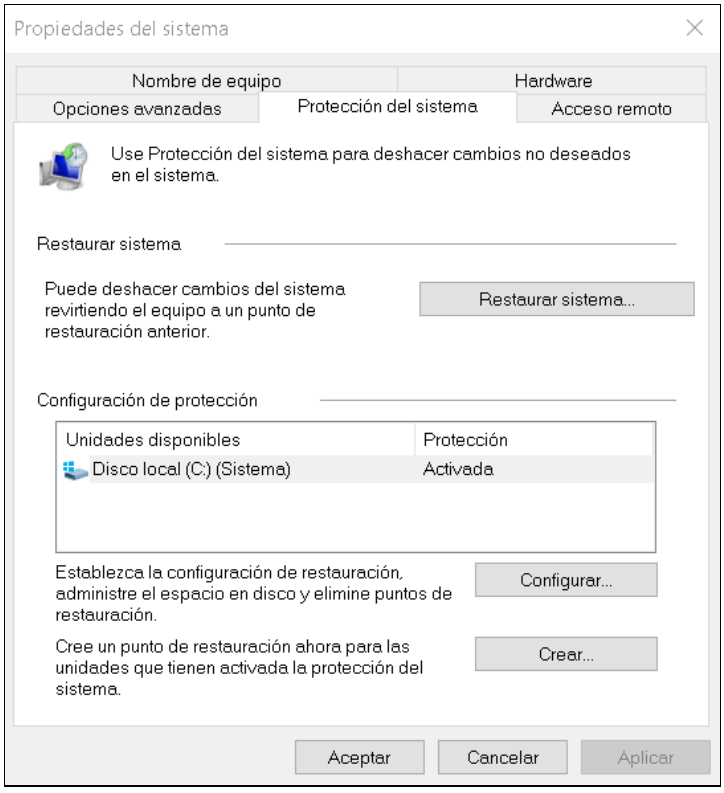

Imagen 14. Propiedades del sistema en Windows10.

Aunque el servicio VSS es una buena solución de copias de seguridad, no está destinado a reemplazar la rutina regular de backup que debe configurarse para ejecutarse con frecuencia para proteger los datos más importantes en una ubicación externa ya que las familias de ransomware más modernas eliminan los snapshots generados por el servicio VSS del dispositivo de la víctima y su recuperación no siempre es posible ya que requiere el uso de herramientas muy sofisticadas como las que se usan en un análisis forense.

Windows Backup

Aunque hay muchas soluciones en el mercado para automatizar las copias de seguridad, el sistema operativo Windows10 incorpora una herramienta de backup que nos permite hacer copias completas y automatizarlas.

Las copias completas llevadas a cabo por esta herramienta incluyen archivos de instalación, configuración, aplicaciones y todos los archivos almacenados en el disco duro principal.

La herramienta de backup se encuentra en el panel de control (ver imagen 15), el siguiente link detalla las instrucciones a seguir para configurar un backup en windows10 que se ejecute automáticamente de forma periódica:

Cómo configurar la automatización de backup en Windows10

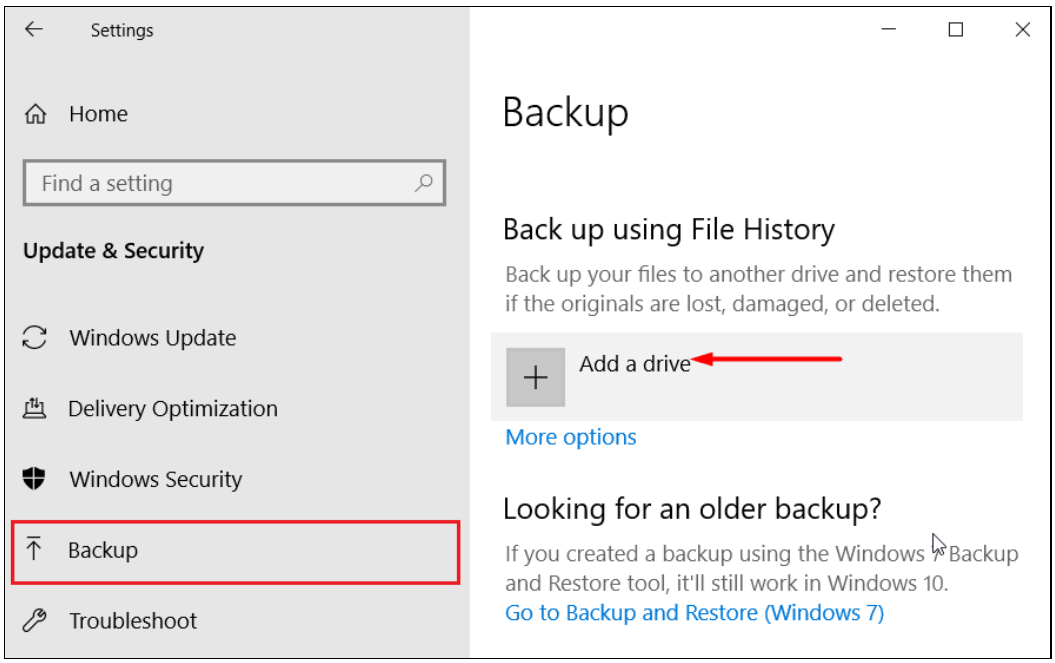

Imagen 15. Pantalla de configuración de backup en Windows 10.

3.15. Reforzar la seguridad del sistema operativo

Una buena configuración del sistema operativo es esencial para limitar la superficie de ataque de un dispositivo. La configuración de seguridad de un equipo de usuario es diferente de la de un servidor dado que se utilizan en contextos completamente distintos.

Esta sección está exclusivamente destinada a tratar aspectos de la configuración del sistema operativo Windows que contribuyen a fortalecer la defensa contra ataques de ransomware en dispositivos de usuario.

La configuración del sistema operativo en dispositivos de tipo servidor, será cubierta en el siguiente capítulo.

Mostrar extensiones de archivo

La extensión de los archivos en Windows está oculta de forma predeterminada.

Obviamente, esto dificulta el reconocimiento de archivos maliciosos, por ejemplo, un archivo de ransomware ejecutable podría tener la extensión *filename.docx.exe* y mostrar un icono de Microsoft Word; en este caso, solo aparecerá la extensión **.docx*, haciendo que este archivo parezca inofensivo.

Para ver la extensión real de un archivo en Windows 10, debemos seguir las instrucciones detalladas en el siguiente link:

Cómo mostrar las extensiones de archivos en Windows

Deshabilitar la característica de Autoplay y Autorun

Siempre que se inserta un dispositivo de almacenamiento extraíble, como una memoria USB, un disco duro externo, un disco CD/DVD/ Blu-ray o una tarjeta SD en nuestro dispositivo, Windows examinará su contenido y mostrará la ventana emergente de reproducción automática preguntando qué acción se desea realizar con el medio insertado.

La característica de ejecución automática de Windows o Autoplay está activada de forma predeterminada en las ediciones anteriores a Windows Vista, lo que permite que los programas maliciosos se ejecuten desde un dispositivo externo tan pronto como sean insertados.

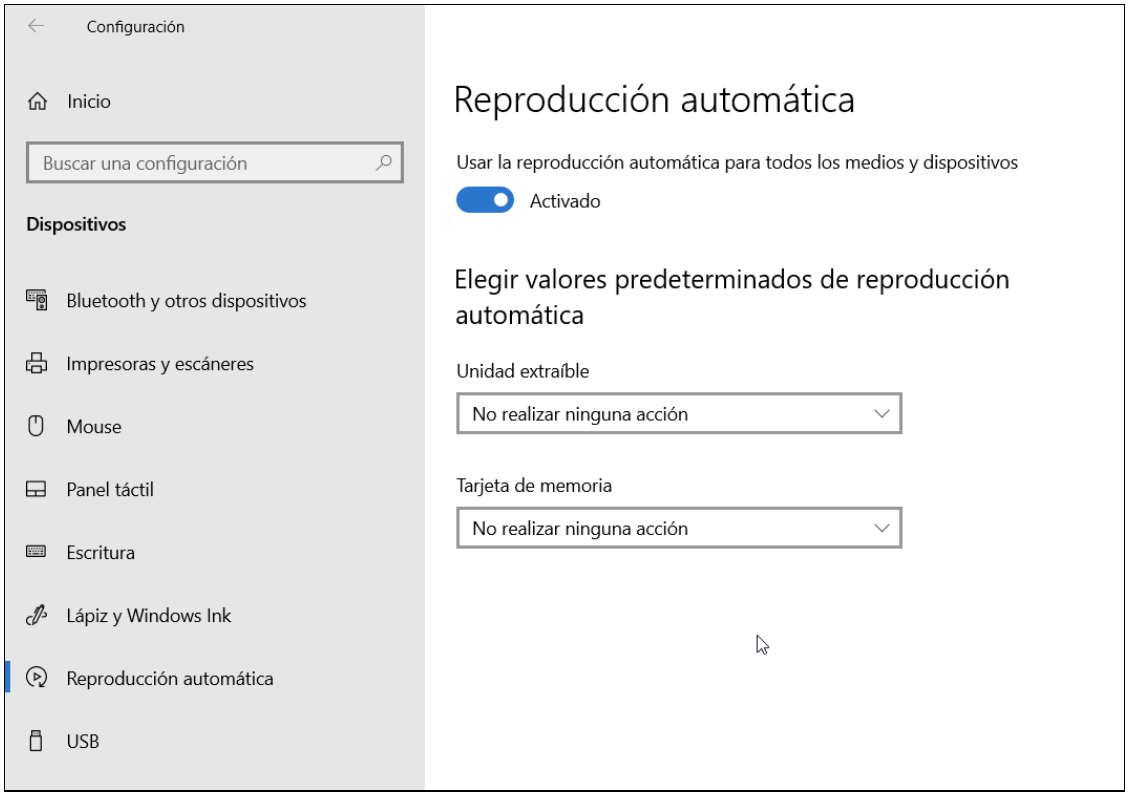

Imagen 16. Configuración segura de Autoplay en Windows10.

A partir de Windows Vista, Microsoft redujo este riesgo de seguridad mostrando el cuadro de diálogo de reproducción automática cada vez que se inserta un medio extraíble y preguntando al usuario qué quiere hacer con él.

Aunque las ediciones modernas de Windows dejan de ejecutar Autorun automáticamente, el usuario todavía está a un paso de ejecutar un programa potencialmente malicioso si selecciona ejecutar un programa en el cuadro de diálogo AutoPlay.

Por esta razón, es recomendable desactivar ambas funciones para aumentar la protección contra un ataque de ransomware a través de memorias USB.

La característica de Autorun es diferente de Autoplay, mientras AutoPlay muestra una ventana emergente, Autorun buscará el archivo *autorun.inf*, que ejecutará automáticamente el programa asociado especificado en dicho archivo.

En caso de tratarse de ransomware, nuestro dispositivo se infectaría al instante y después dependiendo de la familia a la que perteneciera, se podría propagar automáticamente a los dispositivos conectados a la misma red.

En Windows10, la característica de Autorun se configura a través del editor de políticas de grupo y la de Autoplay en el panel de control (ver imagen 16).

En el siguiente link se detallan las instrucciones que hay que seguir para deshabilitar las características de Autoplay y Autorun en Windows10:

Cómo deshabilitar Autoplay y Autorun en Windows10

Habilitar directivas de restricción de software

Las directivas de restricción de software o SRP (software restriction policies), son un mecanismo de seguridad integrado en todas las ediciones de Windows (excepto Windows Home) que permite la configuración de reglas para controlar la ejecución de aplicaciones y scripts que no son confiables.

Por ejemplo, podemos usar SRP para establecer que los únicos directorios en los que está permitido ejecutar programas sean:

- C:\Windows
- C:\Archivos de programa
- C:\Archivos de programa (x86).

En entornos corporativos, es habitual que el departamento de IT habilite SRP como directiva de grupo en todos los dispositivos conectados a la red utilizando el servicio de dominio de Microsoft Active Directory.

Es importante aclarar que SRP no es un antivirus, de hecho, SRP no puede evitar que el ransomware se copie a sí mismo en el disco duro, sin embargo, puede evitar que se ejecute.

Para lograr la persistencia entre reinicios algunos tipos de ransomware se copian a sí mismos en el directorio home del usuario, de este modo, pueden ejecutarse cada vez que el usuario inicia sesión y propagarse a otros dispositivos de la red a los que la víctima tiene acceso.

Además, cuando un archivo se descarga de Internet o del correo electrónico generalmente se almacena en la carpeta %APPDATA% del directorio home del usuario autenticado. Para mitigar el riesgo de infección, podemos configurar SRP para que prohíba la ejecución de aplicaciones desde el directorio home.

La configuración de SRP en Windows10 se lleva a cabo a través del editor de directivas de grupo (ver imagen 17), en el siguiente link se detallan las instrucciones de configuración:

Cómo configurar directivas de restricción de software en Windows10

Una vez que el usuario intente ejecutar una aplicación desde un directorio no permitido, recibirá un mensaje de error indicando que el administrador del sistema bloqueó la aplicación.

Tal y como se verá en el próximo capítulo, en entornos corporativos, lo habitual es usar Windows AppLocker en lugar de SRP.

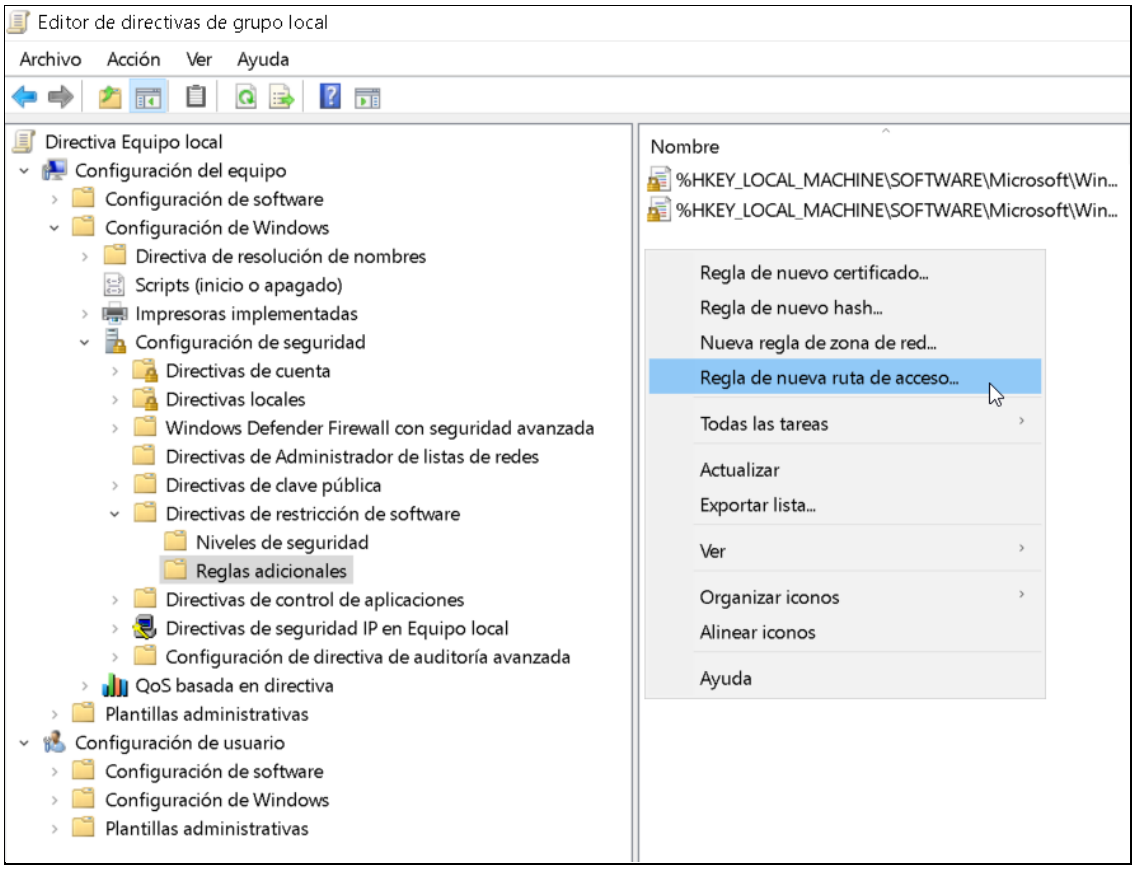

Imagen 17. Configuración de regla de nueva ruta de acceso con SRP.

Capítulo 4

Métodos de defensa en equipos de empresa

En la actualidad, gobiernos y redes corporativas son los principales objetivos de ciberataques por dos motivos, el primero es que en estos entornos se maneja información sensible y bastante confidencial y el segundo es que las redes de organismos gubernamentales y las redes corporativas suelen tener superficies de ataque grandes y diversas lo que crea el caldo de cultivo perfecto.

El modelo de defensa más común hasta hace 10 años se basaba en crear un perímetro alrededor de las redes corporativas protegido por firewalls lo que permitía aislar la red interna de la externa, hoy en día, la mayoría de las empresas suministran acceso remoto a la red interna a sus empleados, partners y proveedores de servicios de IT lo que hace que una estrategia de defensa de la red interna basada en perímetros y firewalls se haya quedado anticuada.

En la actualidad, los ciberataques pueden superar la seguridad perimetral suministrada por los firewalls e infectar los dispositivos cuando, por ejemplo, un empleado abre un archivo adjunto de correo electrónico en su equipo.

Para contrarrestar esta amenaza, las empresas deben implementar una estrategia de defensa multinivel que no se centre únicamente en proteger el acceso a la red interna, sino que también proteja los equipos de trabajo, los servidores, los dispositivos de red y también los datos.

A las estrategias de defensa multinivel se les conoce como estrategias de defensa en profundidad o DiD (defense in depth) y abordan diferentes vectores de ataque para proteger todo el sistema de IT corporativo tanto de ataques internos como externos.

En este capítulo, se abordarán los principales elementos de seguridad que toda organización debe considerar para proteger una red de ataques de ransomware.

4.1. Diseñar una política de gestión de parches

Para mantener los sistemas de IT seguros contra ransomware y otros tipos de malware, las empresas deben aplicar una política de gestión de parches que defina claramente los controles y restricciones de parches para reducir las amenazas de ciberseguridad.

Una buena política de gestión de parches incluye la actualización de todos los dispositivos donde se encuentren almacenados activos digitales, incluyendo: dispositivos de red como puntos de acceso WiFi, routers, firewalls, sistemas IDS, servidores, equipos de sobremesa, portátiles, impresoras, dispositivos de almacenamiento, teléfonos, tablets y cualquier dispositivo con conexión a Internet además de sistemas operativos, aplicaciones, soluciones antivirus, sistemas de bases de datos y plugins.

Obviamente, la aplicación de parches no se puede llevar a cabo con unos pocos clics, primero hay que identificar que actualizaciones y parches es necesario instalar y luego se deben probar en entornos de test que normalmente se encuentran virtualizados.

En empresas de gran tamaño con cientos e incluso miles de dispositivos informáticos donde la aplicación manual de parches resulta una tarea abrumadora se suelen emplear herramientas para automatizar el proceso de parcheo, algunas de las más populares son:

- Microsoft System Center Configuration Manager (SCCM)
- Windows Patch Management
- SolarWinds Patch Manager

4.2. Reforzar la seguridad en las oficinas

En el campo de la ciberseguridad, a las medidas que restringen el acceso a las instalaciones, equipos y recursos se les conocen como seguridad física.

La seguridad física tiene la misma importancia que la ciberseguridad dado que, un ciberdelincuente puede superar todos los controles establecidos y propagar el ransomware a través de la red corporativa si logra obtener acceso físico a un equipo conectado a la red.

Para reforzar la seguridad física, es importante que se establezcan controles en aquellos lugares donde se encuentren equipos conectados a la red corporativa y que se apliquen normas de actuación a todos los actores con acceso a la misma como, por ejemplo:

- Hacer un inventario de todos los equipos informáticos.
- Restringir el acceso a las instalaciones con sistemas de control de acceso.
- Utilizar sistemas de videovigilancia para monitorizar las oficinas de forma remota; las cámaras deben cubrir claramente todas las áreas sensibles.
- Restringir el acceso a cualquier área dentro de la oficina que contenga equipos sensibles, en estos lugares, solo el personal de IT autorizado debe disponer de acceso.
- Aplicar normas para que los empleados no dejen su equipo de trabajo desatendido.
- Mantener los servidores de almacenamiento centrales en salas cerradas.
- Desconectar todos los dispositivos que no requieran acceso a la red.
- Mantener los equipos portátiles en un lugar cerrado cuando no se usen.
- No proporcionar acceso a la red corporativa a visitantes.
- Hacer cumplir la política de seguridad física a todos los visitantes, por ejemplo, proporcionándoles una tarjeta que suministre acceso limitado a ciertas áreas.

4.3. Segmentar la red

La segmentación de una red consiste en dividirla en segmentos o subredes utilizando componentes como firewalls, routers, balanceadores, puertas de enlace y VPNs.

La segmentación de la red es una contramedida eficaz para luchar contra el ransomware ya que ayuda a limitar los daños ocasionados, limita la propagación y dificulta el acceso a los segmentos de red donde se almacena la información más sensible.

Además de aislar los datos más sensibles en segmentos seguros, la segmentación de una red contribuye a aumentar el tiempo requerido para que el atacante descubra y analice la infraestructura corporativa, exponiéndolo más a ser descubiertos por firewalls y sistemas de detección de intrusos (IDS).

Al segmentar una red, el tráfico entre diferentes segmentos pasará a través de firewalls lo que permite instalar soluciones especializadas de tipo antiransomware que permiten detener la propagación entre los diferentes segmentos de la red (ver imagen 18).

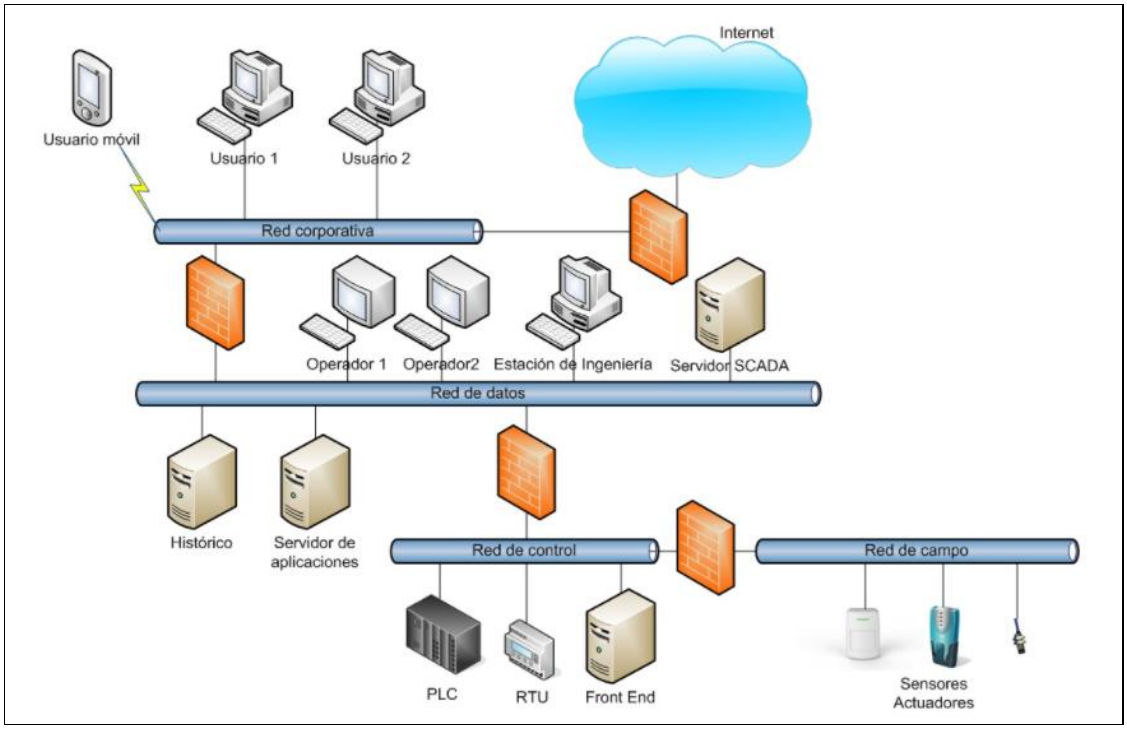

Imagen 18. Esquema de una red segmentada por Firewalls.

4.4. Utilizar soluciones antiransomware

Tener una única solución de antivirus no es suficiente para detener los ataques de ransomware. En la actualidad, existen muchos productos especializados en la detección de ransomware que proporcionan una capa adicional de defensa.

Las mejores soluciones antiransomware utilizan análisis de comportamiento y detección basada en la nube para detectar y detener el ransomware, estas técnicas superan los métodos de detección basados en firmas que todavía emplean la mayoría de los antivirus.

Mientras que los antivirus se centran en capturar malware en una etapa temprana, los programas antiransomware tienen características especializadas que los antivirus tradicionales no ofrecen.

Los mejores productos antiransomware son capaces de evitar que el ransomware complete el procedimiento de cifrado, pueden monitorizar operaciones de manipulación de archivos, ejecutar archivos sospechosos en un entorno virtual y realizar copias de seguridad en tiempo real de los archivos críticos para luego almacenarlas en contenedores seguros.

A continuación, se listan alguna de las soluciones antiransomware que hay en el mercado:

- Bitdefender antiransomware
- Malwarebytes antiransomware solution
- Kaspersky antiransomware tool

4.5. Aplicar el principio del mínimo privilegio

Como se mencionó en el capítulo anterior, el uso de cuentas de usuario con permisos limitados es una medida efectiva contra diferentes tipos de malware.

Salvo que fuese imprescindible, limitar el uso del usuario administrador, aplicando el principio del mínimo privilegio a los operadores de los sistemas, es una medida que prevendría la entrada y propagación de malware.

Para ello, debe existir una correcta concordancia entre las credenciales y la asignación de permisos, de tal manera que la capacidad de ejecución de un usuario ‘normal’ esté perfectamente limitada con respecto a la de un usuario con privilegios de administración.

Los permisos de administración representan un problema para la seguridad al permitir la ejecución libre de programas o el acceso a directorios sensibles.

En entornos corporativos, lo habitual es que los administradores de IT utilicen una cuenta con permisos limitados durante su trabajo diario y que las cuentas de administrador sean empleadas solo para llevar a cabo tareas de mantenimiento y administración.

Los lugares más habituales para emplear cuentas de usuario con permisos limitados son en los equipos de usuario y en el acceso a recursos compartidos en la red.

4.6. Gestionar vulnerabilidades

Desde la perspectiva de la ciberseguridad, una vulnerabilidad es cualquier debilidad encontrada en un sistema informático que puede ser explotada para comprometer su seguridad o alterar el comportamiento habitual del mismo.

La gestión de vulnerabilidades consiste en identificar vulnerabilidades en los sistemas de IT y luego trabajar para eliminar los riesgos antes de que sean explotadas, disponer de un programa de gestión de vulnerabilidades es fundamental para proteger los sistemas de IT de ciberataques.

Por lo general, el proceso de gestión de vulnerabilidades abarca 4 fases: descubrimiento, reporting, priorización y respuesta. Durante la fase de descubrimiento se enumeran todos los activos de IT de la organización, tanto hardware como software que son susceptibles de ser vulnerables, para simplificar esta tarea se emplean programas de gestión de inventario de IT.

En la fase de reporting se emplean programas de análisis de vulnerabilidades para obtener informes de las vulnerabilidades encontradas en los activos de IT.

A continuación, se listan algunas de las más populares:

- Nessus
- OpenVAS
- BurpSuite

Luego se priorizan de acuerdo con su riesgo para la seguridad y finalmente se aplican las correcciones para remediarlas comenzando por las más críticas.

4.7. Firewalls

Hasta ahora, cualquier estrategia de defensa de una red corporativa comenzaba con la instalación de un firewall en el perímetro de la red, sin embargo, las soluciones de firewall tradicionales, que utilizan el filtrado de paquetes a través de la inspección de puertos y protocolos, ya no son adecuadas para detener los ataques de malware más sofisticados.

Los cambios continuos en el uso de aplicaciones, la creciente aparición de amenazas de ciberseguridad, el comportamiento del usuario y las infraestructuras de red cada vez más complejas requieren la adopción de nuevas soluciones de firewall que inspeccionen el contenido de paquetes para identificar el tráfico independientemente del puerto y del protocolo de red empleado.

En la actualidad, existen dos tipos de firewalls: software y hardware.

Los firewalls de software requieren de administración por parte de personal de IT especializado y deben instalarse en cada dispositivo conectado a la red, es por esta razón que las empresas más pequeñas que cuentan con un personal de IT muy reducido suelen optar por instalar firewalls de hardware.

Los firewalls modernos conocidos como firewalls de nueva generación (NGFW) incorporan herramientas avanzadas como antivirus, antimalware y antispam, y admiten conexiones VPN.

Mediante el uso de firewalls de nueva generación, el administrador de red puede identificar las aplicaciones que están generando el tráfico, restringir aquellas que no estén autorizadas, bloquear los protocolos que supongan un riesgo para la seguridad y cerrar los puertos que no se usen para prevenir posibles ataques.

Tal y como se expuso en el Capítulo 2, la explotación del protocolo RDP es uno de los vectores de ataque empleados para distribuir ransomware, una contramedida para paliar el riesgo que supone el uso de RDP en la red corporativa sería bloquear el puerto predeterminado (3389) desde la red externa mediante un firewall y configurar su uso a través de una VPN.

4.8. Sistemas de detección y prevención de intrusiones

Los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) tienen como ventaja respecto a los firewalls tradicionales, el que toman decisiones de control de acceso basándose en el contenido del tráfico, en lugar de hacerlo basándose en direcciones o puertos.

Tanto los IDS como los IPS inspeccionan el tráfico de red examinando y analizando los paquetes en busca de datos sospechosos. La principal diferencia entre un IDS y un IPS es el tipo de acción que llevan a cabo cuando detectan un ataque en sus primeras fases.

El contraste entre un IPS y un IDS radica en que este último es reactivo, pues alerta ante la detección de un posible intruso, mientras que el primero es proactivo, pues establece políticas de seguridad para proteger el equipo o la red de un posible ataque.

El procesamiento de IDS e IPS se basa en la inspección total de cada bit de cada paquete de datos intercambiado. El tráfico de datos es clasificado e inspeccionado en su totalidad por todos los filtros relevantes antes de que se permita su salida, lo que se realiza analizando la información del encabezamiento de cada paquete, como puertos y direcciones IP.

Como resultado de la clasificación e inspección del tráfico, se genera una firma digital que representa el patrón que sigue el tráfico entrante y saliente de acuerdo con los protocolos, puertos, direcciones IP y tipo de contenido, la firma resultante se busca en la base de datos de firmas para averiguar si el tráfico se corresponde con una secuencia de ataque.

La base de datos de firmas de ciberataques es el componente principal de cualquier sistema IPS/IDS, contiene patrones de ataque conocidos y anomalías de protocolo por lo que debe actualizarse periódicamente para incorporar los patrones y anomalías que se correspondan con nuevos ciberataques.

Por ejemplo, en caso de un ataque de ransomware que utilice un exploit kit como vector de ataque, un IPS puede detener el código malicioso antes de llegar al destino y también puede bloquear la conexión con los servidores de comando y control (C&C) si alguno de los equipos de usuario resulta infectado.

En la actualidad, muchos proveedores de IPS/IDS están integrando sus productos con firewalls para crear una única solución que pueda aplicarse en el perímetro de redes corporativas, a este tipo de productos se les denomina productos de gestión unificada de amenazas o UTM, las siglas de Unified Threat Management.

Un UTM unifica las funcionalidades de un antivirus, un firewall, un IDS/IPS con técnicas de antiphising, antimalware, antispam, filtrado de contenido y tecnología VPN y WiFi.

4.9. Sandboxing

Los firewalls de nueva generación utilizan firmas y métodos de detección heurísticos para bloquear los ataques de malware.

Sin embargo, en la actualidad, dado el creciente número de amenazas, estos métodos de detección no son suficientes, especialmente para contrarrestar las vulnerabilidades de día cero y los ataques dirigidos.

En el contexto de la arquitectura de redes, el sandboxing de red se está convirtiendo en una capa de seguridad a considerar cuando se diseña el perímetro de las redes.

El sandboxing de red se basa en el envío de archivos infectados a un entorno virtual aislado (sandbox) que permite analizar su comportamiento sin comprometer la seguridad. Si el archivo en cuestión resulta ser malicioso, se rechazará, de lo contrario, se marcará como válido y se le permitirá pasar el perímetro de la red.

Muchos fabricantes de firewalls de nueva generación ofrecen un espacio aislado en la nube por suscripción, donde los archivos sospechosos son enviados para analizar su comportamiento cuando son ejecutados.

Sin embargo, todavía existen limitaciones, por ejemplo, algunos tipos de malware son capaces de detectar si están siendo ejecutados en un entorno de sandbox para decidir si ejecutar el código malicioso o ejecutar un código arbitrario para evadir los sistemas de detección y análisis de comportamiento.

4.10. Seguridad en los DNS

Algunos tipos de ransomware, necesitan comunicarse con un servidor para recibir instrucciones y propagarse por la red, tal y como se vio en el Capítulo 1, a este servidor se le denomina servidor de comando y control o C&C.

Bloquear el acceso a dominios maliciosos es una contramedida eficaz para prevenir la infección y la propagación de ransomware.

Por ejemplo, es aconsejable bloquear el acceso al dominio de la red TOR ya que tal y como se vio en el Capítulo 3, muchas familias de ransomware utilizan esta red para enconder el servidor de C&C, de este modo, evitamos que el atacante pueda enviar órdenes para configurar el comportamiento del ransomware.

En la actualidad, existen muchos sitios web que ofrecen listas de dominios y URLs reconocidas por emplearse para distribuir malware y llevar a cabo ataques de phishing, estas listas pueden usarse para configurar el firewall.

Algunas de las listas más populares son:

- Ransomware tracker
- Malware Domain
- Open Phish

El bloqueo de acceso a dominios maliciosos también puede llevarse a cabo mediante un servidor proxy centralizado ya que permite restringir todo el tráfico de salida desde la red interna hacia Internet, aunque en entornos corporativos lo más habitual es usar servicios de DNS seguros.

Los servicios de DNS seguros añaden una capa adicional de seguridad al proceso de resolución de DNS proporcionando las siguientes capacidades:

- Filtrado de contenido. Permite bloquear sitios para adultos y otro contenido no deseado, sin requerir software en las computadoras y dispositivos.
- Bloqueo de malware y phishing. Permite bloquear sitios que contengan virus, estafas y otros contenidos peligrosos.
- Protección contra botnets. Bloquea la comunicación con servidores de botnet conocidos.
- Bloqueo de publicidad. Este es otro tipo de filtrado de contenido, en el que se concentran específicamente algunos servicios de DNS.

Algunos de los servicios de DNS seguros más conocidos son:

- OpenDNS
- Comodo
- Yandex.DNS

4.11. Usar Honeypots

Un honeypot es un activo de red falso que se utiliza para engañar a los ciberdelincuentes cuando intentan obtener acceso no autorizado o comprometer la seguridad.

Se despliegan en la red bajo la apariencia de objetivos de alto valor para los ciberdelincuentes como, por ejemplo, un servidor de archivos o un servidor de base de datos, las empresas suelen utilizar honeypots para detectar a los intrusos y desviarlos de los activos de red de verdad.

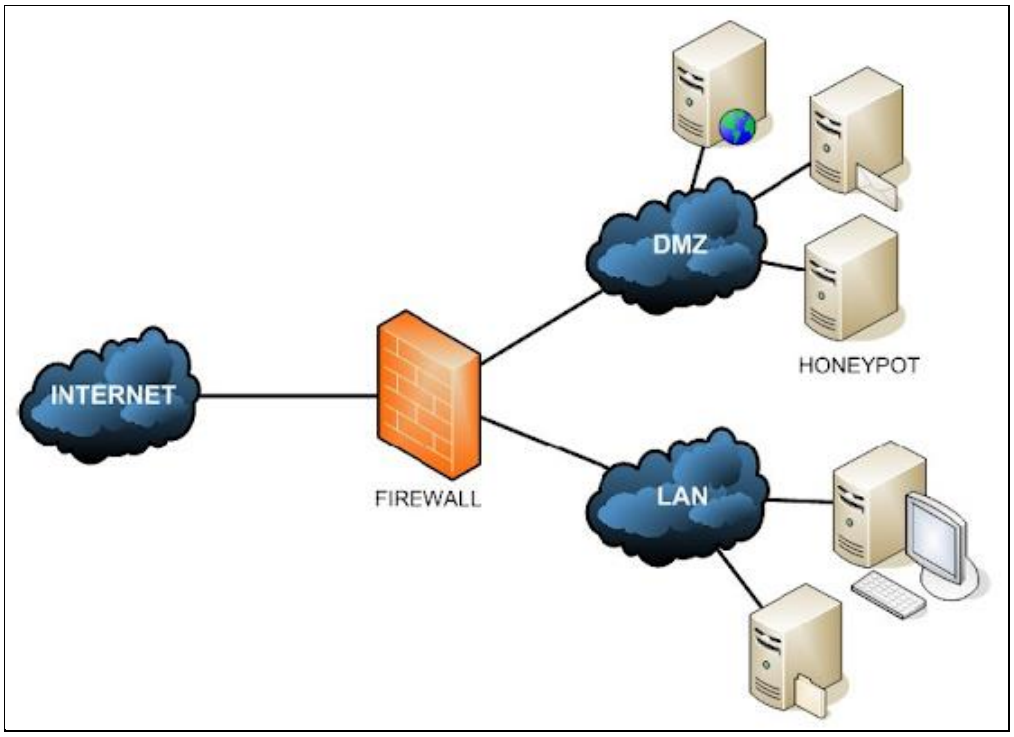

Imagen 19. Uso de un honeypot en la zona desmilitarizada.

Por ejemplo, para protegerse de un posible ataque de ransomware, lo habitual es configurar el firewall de modo que todo el tráfico que no cumpla con los criterios de seguridad sea desviado a una zona desmilitarizada entre la red externa y la red interna.

La zona desmilitarizada es el lugar ideal para desplegar un honeypot bajo la apariencia de un sitio web que expone datos falsos que se encuentran almacenados en un servidor de base de datos o de archivos (ver imagen 19), de este modo, si el ransomware compromete con éxito la información almacenada, se notificará al administrador del sistema para que tome las medidas necesarias.

Sin embargo, el valor más importante que suministra un honeypot es el estudio del comportamiento de los atacantes y de las técnicas que emplean a fin de examinar la efectividad de las medidas de seguridad aplicadas.

4.12. Seguridad del correo electrónico

Como se mencionó en el Capítulo 2, el correo electrónico es el vector de ataque más empleado para distribuir ransomware.

Las técnicas más extendidas son el phising, el envío de links que apuntan a sitios web que contienen exploit kits y el envío de archivos adjuntos que contienen malware o bien el propio ransomware.

A continuación, se abordan las medidas de seguridad necesarias que toda organización debería implementar para proteger su red del ransomware enviado por correo electrónico.

Reglas para filtrar los correos de spam

Como se trató en el Capítulo 2, el spam es ampliamente usado en campañas publicitarias para promociones comerciales, sin embargo, también se puede usar para propagar malware o adquirir información confidencial, como credenciales de inicio de sesión a través de phising.

Los siguientes son algunos métodos para reducir la cantidad de mensajes de spam recibidos:

- Aplicar filtros por contenido y por dirección IP
- Ofuscar las direcciones de correo que enviemos en los mensajes para hacerlas legibles para humanos pero difíciles de capturar para sistemas de automatización como bots.
- Usar direcciones de correo secundarias para registrarnos en servicios online.
- Deshabilitar el HTML en los correos electrónicos de la bandeja de entrada para prevenir la ejecución de scripts embebidos en links e imágenes.

Bloquear archivos adjuntos

Como se ha mencionado anteriormente, una de las formas más comunes para infectar los dispositivos es mediante el envío de archivos adjuntos.

Para contrarrestar este riesgo, es recomendable configurar el servidor de correo electrónico para bloquear ciertos tipos de archivos que a menudo suelen ser empleados para llevar a cabo ataques de ransomware o phising.

En caso de que se desee enviar un tipo de archivo catalogado como peligroso, existen soluciones como, por ejemplo, usar un medio de almacenamiento en la nube para cargar el archivo bloqueado y luego enviar el enlace de descarga al destinatario o simplemente se puede cambiar la extensión del archivo.

La mayoría de los usuarios suele pensar que los archivos ejecutables (*.exe), son los únicos tipos de archivos que no deberían abrirse cuando se reciben a través del correo electrónico, sin embargo, la realidad es que hay una gran cantidad de tipos de archivos que pueden usarse para ejecutar código malicioso.

La siguiente lista, muestra algunas de las extensiones de archivos que no deberían abrirse cuando se reciben en el correo electrónico:

EXE, MSI, MSP, APPLICATION, GADGET, MSC, JAR, CMD, VB, VBS, VBE, JSE, PS1, PS2, MSH, MSH1, MSH2, MSHXML, SCF, LNK, INF, REG, WSH

Los archivos de Microsoft Office también pueden contener código malicioso en forma de macros, por tanto, hay que tener cuidado de no ejecutar macros de Office que se han enviado desde orígenes desconocidos.

Para concluir, tampoco es aconsejable abrir archivos comprimidos que se encuentren protegidos con contraseña (*.zip, *.rar), ya que los atacantes emplean este truco para evitar que los antivirus puedan analizar el contenido.

4.13. Usar contraseñas seguras

Muchos usuarios que navegan por la red utilizan contraseñas que son poco robustas y fáciles de adivinar para los ciberdelincuentes.

El problema reside en que seguimos haciendo uso de estas sin ser conscientes de los peligros que esta práctica conlleva.

Contraseñas como “12345” o “password” son solo algunos de los ejemplos de este tipo de claves “sencillas”, que más que aportarnos seguridad ponen en riesgo todo aquello que estemos tratando de proteger.

Según un estudio realizado por la empresa Deloitte, casi el 90% de las contraseñas de los usuarios de todo el mundo son vulnerables a los ataques de los ciberdelincuentes [30].

Por tanto, es muy importante establecer una política de contraseñas seguras y robustas que obligue a los usuarios a cumplir con requisitos de complejidad, rotación y no reutilización.

En los sistemas operativos Windows, es posible habilitar una directiva de contraseñas de forma fácil y rápida, a través del editor de directivas de grupo, en el siguiente link se detallan las instrucciones de configuración:

Configuración de directivas de contraseñas de usuario en Windows10

4.14. Reforzar la seguridad en conexiones remotas

Como se expuso en el Capítulo 2, el protocolo RDP permite a un usuario acceder de forma remota a su dispositivo, sin embargo, puede explotarse para infectar la máquina con ransomware si se emplean credenciales con contraseñas débiles.

Si no vamos a usar RDP de forma frecuente, lo más seguro es deshabilitarlo, en caso contrario, es conveniente considerar los siguientes aspectos:

- Cuando se configuren las credenciales para el acceso por RDP, se debe utilizar una contraseña segura, es decir, debe tener al menos 15 caracteres, incluir números, combinaciones de caracteres en minúscula y mayúscula, caracteres especiales y no debe incluir espacios en blanco.

- Habilitar la autenticación de nivel de red (NLA) para conexiones RDP, en Windows10, se consigue a través del panel de control:

  Cómo configurar la autenticación de nivel de red en RDP

- Cambiar el número de puerto predeterminado de RDP de 3389 a otro, esto debería agregar una capa adicional de seguridad para engañar a las herramientas de escaneo de puertos, en Windows10, la configuración del puerto predeterminado de RDP, se lleva a cabo modificando el registro.

  Cómo modificar el puerto predeterminado para conexiones RDP

- Asegurarse de que el sistema operativo se encuentra actualizado para prevenir cualquier tipo de ataque al protocolo RDP.

- Usar reglas de firewall para limitar el acceso por RDP a un rango específico de direcciones de IP.

- Aplicar directivas de seguridad para bloquear aquellas cuentas de usuario que lleven a cabo múltiples intentos fallidos de inicio de sesión por RDP.

Otra forma de reforzar la seguridad en conexiones remotas es usar una VPN (Virtual Private Networking) ya que permite acceder a servicios online desde cualquier lugar sin necesidad de exponerlos en Internet.

En caso de usar una VPN, la habilitación de la autenticación de dos pasos proporciona una capa extra de seguridad al requerir a los usuarios suministrar un mecanismo de autenticación adicional además de la contraseña.

4.15. Uso de dispositivos USB

En un contexto empresarial, el uso de dispositivos USB no se puede prohibir por completo, sin embargo, se recomienda implementar algunas medidas de seguridad para mitigar los riesgos asociados con los dispositivos USB:

- Se debe evitar conectar dispositivos USB directamente a equipos conectados a la red, cuando se desee transferir archivos, en su lugar, se deben cargar los archivos necesarios desde el dispositivo USB a un repositorio de archivos central donde se pueda acceder a ellos.

- Todos los dispositivos USB deben analizarse primero en busca de malware en un equipo aislado antes de conectarlos a la red corporativa.

- Se debe hacer cumplir una política de uso de dispositivos USB.

- En el caso de archivos PDF y de Microsoft Office, se recomienda el análisis mediante antivirus antes de proceder a su apertura.

- Se recomienda el uso de software de protección contra escritura para evitar que se alteren o eliminen los archivos almacenados en el dispositivo USB.

- En caso de que la empresa facilite dispositivos USB a sus empleados, se recomienda que soporten protección y cifrado mediante PIN.

4.16. Habilitar directivas de restricción de software

En entornos corporativos, la instalación de un antivirus en equipos de usuario y de firewalls en el perímetro de la red no es suficiente para protegerse contra ataques de ransomware.

La aplicación de listas blancas y de reglas que controlen las aplicaciones que pueden ejecutarse en el sistema operativo se considera la medida más eficaz para defenderse de malware desconocido que aún no se ha descubierto, además de otras amenazas que aprovechan las vulnerabilidades de día cero.

En Windows, hay dos mecanismos de seguridad integrados para implementar políticas de control de aplicaciones en toda la empresa: SRP y AppLocker.

En el capítulo anterior, se abordó el uso de SRP como medida de prevención y defensa contra ataques de ransomware en equipos de usuario, sin embargo, en entornos corporativos, lo habitual es usar Windows AppLocker.

Windows AppLocker dispone de una mejor integración con el directorio activo y permite ejercer un control más granular basándose en la asignación de 3 tipos de reglas a usuarios y grupos específicos:

- *Reglas basadas en rutas del sistema de archivos (path rules)*

  Permiten controlar los directorios desde los cuales está permitido ejecutar aplicaciones.

- *Reglas basadas en códigos hash (file hash rules)*

  Permiten restringir la ejecución basándose en el código hash del archivo ejecutable de la aplicación, su uso permite la elaboración de listas blancas y negras de aplicaciones.

- *Reglas basadas en el editor del ejecutable (publisher rules)*

  Permiten restringir la ejecución basándose en la firma digital y los atributos extendidos del archivo ejecutable de una aplicación como, por ejemplo, el nombre del producto del que forma parte el archivo, el nombre original del archivo y el número de versión.

Al igual que SRP, Windows AppLocker puede configurarse en el editor de políticas de grupo.

Cómo crear directivas de restricción de software con AppLocker

4.17. Prevenir la perdida de datos

Las soluciones de prevención de pérdida de datos o DLP (data loss prevention) son sistemas que están diseñados para detectar fugas de datos y prevenirlas mediante técnicas de monitorización.

El objetivo principal de una solución DLP es vigilar el flujo de datos dentro de una organización a través de todos los canales de comunicación, como el correo electrónico, mensajería instantánea, formularios web, dispositivos USB y cualquier otro medio para detener la fuga de información.

Las soluciones DLP funcionan en base a la política de seguridad establecida por la organización o por una de cumplimiento normativo como el RGPD.

Una solución DLP detectará cualquier violación de las reglas impuestas de inmediato e implementará medidas de protección como, por ejemplo, enviar una alerta, cifrar los datos o terminar la sesión del usuario para evitar que se filtre información confidencial de manera intencional o accidental.

Las soluciones DLP monitorizan los datos en tres estados:

- **En reposo**, es decir, cuando los datos residen en unidades de almacenamiento como bases de datos y servidores de archivos.

- **En tránsito**, es decir, cuando los datos se mueven a través de la red corporativa y/o hacia redes externas como Internet mediante el correo electrónico o el tráfico generado por software malintencionado.

- **En uso**, es decir, cuando los datos se procesan en equipos informáticos que se encuentran conectados a la red.

Otro de los propósitos de una solución DLP es evitar la pérdida de datos.

Cuando se produce un ataque de ransomware, los datos se cifran negándole el acceso al propietario de los datos, en determinados casos, la recuperación de datos cifrados puede ser imposible, por ejemplo, en el caso de ransomware NotPetya, tal y como se expuso en el Capítulo 2, la destrucción de los datos es total.

Las soluciones DLP permiten informar al administrador de IT con anticipación sobre cualquier tráfico inusual o un cambio en los datos almacenados, por ejemplo, debido al comienzo de la ejecución de la rutina de cifrado del ransomware y pueden alertar al administrador para que aísle el dispositivo infectado o el segmento de red.

4.18. Mantener una estrategia efectiva de backup

La defensa más importante contra los ataques de ransomware es contar con una estrategia eficaz de copia de seguridad o backup y recuperación de datos, todas las empresas que diseñen una estrategia de backup deberían al menos considerar la adopción de las siguientes medidas:

- Las copias de seguridad deben emplearse para proteger los datos que son fundamentales para la continuidad del negocio en caso de infección.

- Las copias de seguridad deben mantenerse almacenadas en un segmento de red que se encuentre aislado de la red corporativa y al que no se pueda acceder a través de Internet.

- Se debe considerar tener varias copias de la copia de seguridad (al menos 3 copias), las copias de seguridad en la nube son una opción segura porque se encuentran fuera de la red corporativa, sin embargo, debe evitarse hacer copias de seguridad de los datos en tiempo real en la nube de forma continua, ya que algunas familias de ransomware tienen la capacidad de cifrar las copias de seguridad en la nube.

- Si un ataque de ransomware resulta exitoso, se debe detener cualquier copia de seguridad que se encuentre en proceso de inmediato para evitar que el ransomware ejecute la rutina de cifrado sobre la misma.

- El medio empleado para llevar a cabo la copia de seguridad (un servidor de archivos, una unidad extraíble o una carpeta compartida en la red) no debe permanecer conectado permanentemente al sistema que contiene los datos que se desean copiar para evitar infectarlo en caso de que el ransomware consiga colarse en la red corporativa.

- El servidor donde se encuentren almacenadas las copias de seguridad debe emplear un sistema operativo con una configuración de seguridad reforzada, preferiblemente una variante de Linux, ya que se sabe que Windows es un objetivo común de los ataques de ransomware.

- La integridad de las copias de seguridad debe comprobarse continuamente para asegurarse de que existan copias de todos los datos críticos.

- Se debe probar el proceso de recuperación con regularidad para garantizar una alta disponibilidad en caso de que se necesite.

- Se deben cifrar las copias de seguridad a fin de cumplir con el RGPD, además, subir copias de seguridad a la nube puede resultar un riesgo cuando no se cuentan con las medidas de seguridad adecuadas.

4.19. Evaluar la seguridad de los sistemas anualmente

Evaluar la seguridad de los sistemas permite verificar si existen problemas de seguridad.

Para una evaluación más realista, se debe considerar la posibilidad de realizar una prueba de penetración completa o pentesting. Un pentesting es un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas.

Estas auditorías comienzan con la recogida en fuentes de acceso público de información sobre la empresa, los empleados, usuarios, sistemas, equipamientos y continúa con un análisis de vulnerabilidades que se intentarán explotar, incluso con técnicas de ingeniería social.

Finalmente, se realiza un informe que indica si los ataques han tenido éxito y en caso afirmativo porqué y que información o acceso se ha obtenido, es decir, se simulan ataques tal y como los llevaría a cabo un ciberdelincuente que quisiera hacerse con el control del sistema.

4.20. Hacer cumplir las políticas de seguridad

Una política de seguridad es un conjunto de reglas y procedimientos que una organización aplica a sus empleados cuando utiliza sus sistemas de IT para mantener la seguridad de sus activos y recursos de IT.

Todas las personas de una organización deben comprender su obligación de proteger los datos y los activos de IT, por tanto, toda política de seguridad debe incluir sanciones cuando alguien no cumple con las regulaciones.

Las siguientes son las áreas más importantes que deben incluirse en cualquier política de seguridad dentro de una organización:

- Política de contraseñas
- Política de uso del correo electrónico
- Política de uso de Internet
- Política de uso de dispositivos móviles
- Política de acceso remoto
- Política de administración de parches
- Política de gestión de vulnerabilidades
- Política de cifrado de datos
- Política de seguridad física

Independientemente del tamaño de una organización, tener una política de seguridad es esencial para abordar todas las posibles amenazas a la seguridad y sugerir contramedidas antes de que ocurran.

4.21. Formación en ciberseguridad

Un buen programa de formación en ciberseguridad educará a los empleados sobre las diferentes amenazas de ciberseguridad a las que se pueden enfrentar y les enseñara a identificar los puntos de entrada que pueden usar los atacantes para acceder a la red corporativa y qué medidas de precaución deben tomar para evitar el acceso no autorizado a los activos digitales de la organización.

De todos los elementos que forman parte de un programa de formación en ciberseguridad, la defensa contra el phishing es el más importante ya que sigue siendo el vector de ataque número uno, por tanto, es primordial que los usuarios aprendan a reconocer las diversas técnicas empleadas en los correos electrónicos de phising para que de este modo sepan reconocerlos.

En el Anexo III del presente trabajo fin de master se aborda en detalle la formación en ciberseguridad como mecanismo de prevención.

Capítulo 5

Plan de respuesta a ataques de ransomware

Un plan de respuesta a incidentes es un conjunto de instrucciones que utiliza el personal de IT en las organizaciones para mitigar, detectar, responder y recuperarse de incidentes de ciberseguridad.

El propósito final de un plan de respuesta a incidentes es prevenir cualquier daño a los sistemas de IT que pueda conducir a una violación de datos o a una interrupción del servicio.

El equipo responsable de implementar el plan de respuesta a incidentes es el equipo de respuesta a incidentes de seguridad informática o CSIRT (Computer Security Incident Response Team).

El CSIRT está compuesto por profesionales de IT con formación en ciberseguridad y entre sus responsabilidades se encuentra la comunicación con las diferentes partes dentro de una organización, la contención del daño, la recuperación de incidentes de seguridad, la comunicación con entidades externas como la prensa, las fuerzas del orden y otras partes afectadas, así como las partes interesadas y los clientes.

En este capítulo, se analizan los elementos principales de un plan de respuesta a incidentes de ransomware desde una perspectiva genérica utilizando las recomendaciones basadas en el ciclo de vida de respuesta a incidentes del NIST (ver imagen 20).

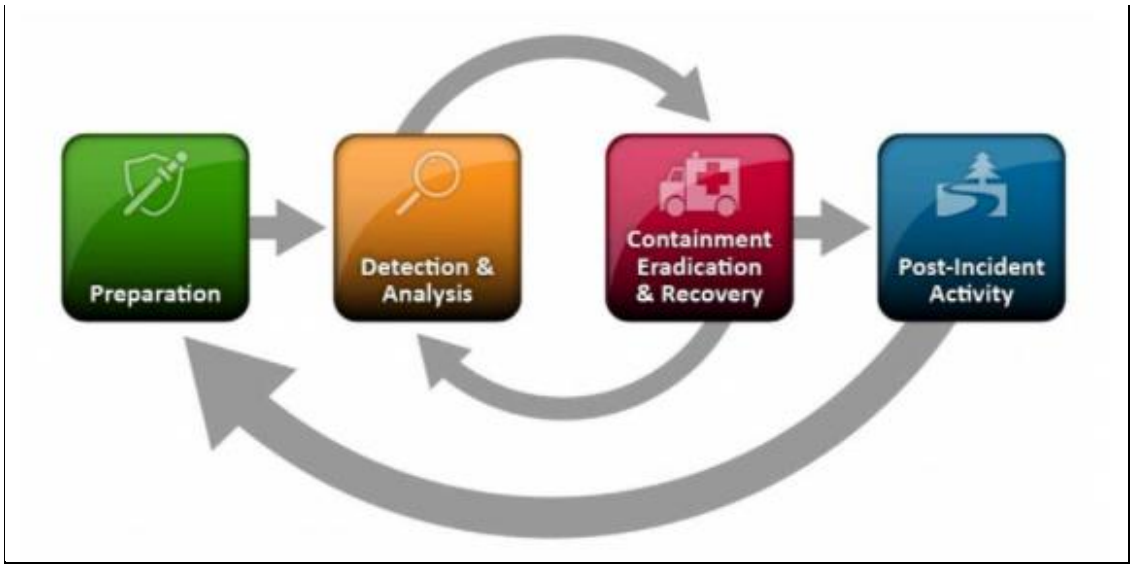

Imagen 20. Ciclo de vida de respuesta a incidentes del NIST.

5.1. Preparación

Los elementos de la fase de preparación se trataron en detalle en los capítulos 3 y 4 del presente trabajo fin de master.

En la fase de preparación, la organización describe los pasos y las contramedidas que deben implementarse para proteger el entorno de trabajo de ataques de ransomware.

Esta fase se considera la más importante, ya que describe principalmente los pasos de mitigación y prevención que deben implementarse ya que tener una estrategia de defensa sólida de varios niveles puede detener un ataque antes de que pueda penetrar en el entorno de trabajo.

En la fase de preparación toda organización deberá tener en cuenta lo siguiente:

- Quién ha de realizar la gestión de los incidentes dentro de la organización

- Donde está la documentación necesaria sobre los sistemas y redes que se usan en la organización.

- Definir cuál es la actividad normal que permita detectar actividades sospechosas que sean indicios de incidentes.

- Con quién tendremos que contactar en caso de incidencia, por ejemplo, en el caso de servicios externalizados, el responsable es el proveedor de servicios de IT, también es útil, en caso de sufrir un incidente, contactar con algún dentro de respuesta ante incidentes como puede ser INCIBE-CERT, en el que nos indicaran como podemos recuperar nuestros archivos si existiera alguna forma.

Las siguientes recomendaciones deben cubrirse en la fase de preparación de cualquier plan de respuesta a incidentes de ransomware:

Formación en ciberseguridad

Formar a los usuarios en ciberseguridad ayuda a prevenir ataques de ransomware al hacer que los usuarios sean conscientes de cómo los ciberdelincuentes pueden penetrar e infectar los sistemas de IT mediante técnicas como el phising.

Los ataques de ransomware deben incorporarse en todos los programas de capacitación en ciberseguridad para que los usuarios puedan reportar incidentes una vez descubiertos para evitar que el ransomware se propague por la red.

La formación en ciberseguridad es abordada en detalle en el Anexo III del presente trabajo fin de master.

Protección de equipos conectados a la red

Se debe fortalecer la seguridad de todos los dispositivos conectados a la red corporativa, aquí se incluye la aplicación de configuraciones seguras tanto en el navegador como en el sistema operativo y en los protocolos de red como RDP.

También se incluye la instalación de soluciones de antivirus, antimalware, antiransomware, mantener el sistema operativo actualizado, controlar la ejecución de archivos ejecutables y otras contramedidas que contribuyan a que los equipos sean más resistentes a la infección por ransomware.

Protección de la red

Se deben proteger los puntos de entrada a la red mediante sistemas de prevención de intrusiones (IPS), sistemas de detección de intrusiones (IDS) y firewalls, implementar la segmentación de red para aislar las redes infectadas, instalar soluciones antispam en los servidores de correo electrónico, escanear todos los archivos adjuntos de correo electrónico entrante y saliente, implementar medidas de seguridad física en las oficinas etc.

Políticas de seguridad

Se debe tener una política de seguridad actualizada y asegurarse de que se aplique a todos los usuarios que accedan a los activos y recursos de IT de la organización como, por ejemplo, documentos, CRM, bases de datos, etc.

Plan de respuesta a incidentes

Cada organización debe tener un plan de respuesta a incidentes claro y actualizado que defina las funciones y responsabilidades de cada empleado una vez que se detecta un incidente de ransomware, el plan de respuesta a incidentes debe ir acompañado de un plan de recuperación de desastres para restaurar la operativa a un estado normal.

5.2. Detección y análisis

Los incidentes de ransomware se pueden detectar de varias maneras:

- ✓ Una ventana cubre toda la pantalla y bloquea el acceso al equipo.
- ✓ Se encuentran archivos cifrados en la unidad de disco o archivos con extensiones extrañas que no se pueden abrir.
- ✓ El fondo del escritorio se ha reemplazado por una nota de rescate.
- ✓ Se encuentran archivos de texto o HTML que contienen instrucciones de pago de un rescate en cada carpeta donde se han encontrado archivos cifrados.

Una vez que se ha producido la infección, en la fase de análisis, la organización debe poner todos sus esfuerzos y atención en responder a las siguientes preguntas:

¿Cómo consiguió el ransomware penetrar en el equipo infectado?

Para responder a esta pregunta, debemos recurrir al capítulo 2 del presente trabajo fin de master donde se abordaron los diferentes vectores de ataque empleados para distribuir ransomware. Los más comunes son los siguientes:

- ✓ Archivos adjuntos en correos electrónicos y links maliciosos.
- ✓ Vulnerabilidades en el navegador web
- ✓ Software pirata
- ✓ Dispositivos USB
- ✓ Macros maliciosas de Office

El análisis de como el ransomware consiguió penetrar en la organización puede retrasarse hasta la última fase (acciones posteriores).

¿Qué tipo de ransomware ha causado la infección?

Para responder a esta pregunta, existen algunos servicios online que pueden ayudar con el proceso de identificación, como, por ejemplo:

- ID Ransomware

  Se trata de un servicio gratuito que hasta la fecha detecta más de 1000 tipos de ransomware y que avisa al usuario si existe una herramienta que le permita restaurar los archivos infectados. Para usar este servicio, tanto solo tenemos que subir un archivo que contenga la nota de rescate o un archivo infectado.

- No More Ransom

  Para usar este servicio debemos subir uno de los archivos infectados, la nota de rescate o introducir la dirección de correo facilitada en la nota de rescate o la dirección del monedero Bitcoin donde se debe depositar el rescate.

- VirusTotal

  Se trata de un servicio online para analizar archivos, para usarlo, tan solo tenemos que subir el archivo infectado.

Identificar la variante de ransomware es esencial para planificar las fases posteriores. En caso de no disponer de recursos propios para resolver el incidente o necesitemos contar con expertos para su resolución, se deberá escalar el incidente.

5.3. Contención

Una vez que se ha identificado que un equipo ha sido infectado con ransomware, debemos seguir los siguientes pasos para su contención:

1. Aislar el equipo infectado de la red

   Esto puede conseguirse desconectando el cable de red o cualquier conectividad inalámbrica que pueda estar en uso para evitar la propagación de la infección a otros dispositivos a través de la red.

2. Cambiar todas las contraseñas de red y de cuentas online

3. Adquirir un volcado de memoria del equipo infectado

   Esto puede resultar útil más adelante para encontrar el vector de ataque correcto mediante el uso de herramientas de análisis forense y capturar información sobre la rutina de cifrado implementada por el ransomware, lo que puede ayudar a descifrar los datos comprometidos.

   Si no es posible obtener un volcado de memoria del equipo infectado, podemos poner el equipo en estado de hibernación y buscar ayuda de un profesional forense para examinar la memoria.

4. Clonar el disco duro

   Se recomienda realizar una clonación completa del disco duro, de esta manera, se podrá mantener el dispositivo original y así intentar recuperar los datos sobre el clon.

   Si no existiera solución hoy, es posible que en el futuro sí la haya, por lo que se podrían llegar a recuperar los archivos comprometidos.

5. Comprobar y asegurar los sistemas de copia de seguridad

   Se deben desconectar los sistemas de copia de seguridad de la red y realizar un análisis de los datos de la copia de seguridad para asegurarse de que estén libres de infección.

6. Limitar la conectividad

   Deshabilitar la conectividad con discos duros externos, memorias USB, unidades de red o servicios en la nube que estuvieran conectados con el equipo infectado.

7. Limitar la conectividad con Internet de los servidores más críticos en la organización hasta descubrir y erradicar la fuente de infección.

8. Determinar el alcance de la infección

   Se deben comprobar las siguientes ubicaciones para hacer una estimación del daño causado por la infección:

   - ✓ Unidades de disco y carpetas compartidas en la red
   - ✓ Unidades de red conectadas al equipo infectado
   - ✓ Cuentas conectadas a medios de almacenamiento en la nube.
   - ✓ Dispositivos USB conectados al equipo infectado
   - ✓ Otros dispositivos externos conectados al equipo infectado como, por ejemplo, tarjetas SD, teléfonos móviles, tablets, portátiles, etc.

9. Denunciar el incidente a las autoridades

   - ✓ Grupo de delitos telemáticos de la guardia civil
   - ✓ Brigada de investigación tecnológica de la policía nacional

5.4. Erradicación

Una vez que se ha contenido la infección del ransomware, hay que erradicarlo de los equipos infectados. La erradicación depende en gran medida del vector de ataque empleado por el ransomware que causó la infección.

Por ejemplo, si el ransomware penetra en la red corporativa a través de un archivo adjunto en un correo electrónico, se deben eliminar todos los correos electrónicos recibidos en el servidor de correo y evitar que todos los usuarios abran cualquier correo electrónico con archivos adjuntos hasta que se identifique el correo electrónico malicioso.

También se debe considerar aislar cualquier equipo, o incluso todo el segmento de red donde se haya abierto el correo electrónico sospechoso hasta que se verifique que no hay más infecciones de ransomware en ese segmento.

En caso de que el vector de ataque fuera la ejecución de un exploit kit a través del navegador web, entonces se debe considerar bloquear el acceso a sitios web maliciosos y realizar un análisis de todos los dispositivos con conexión a internet infectados para actualizar o eliminar todos los componentes utilizados para propagar la infección como, por ejemplo, navegadores web o plugins con versiones vulnerables.

También es recomendable cambiar las contraseñas empleadas por los usuarios que se vieron afectados por el ataque de ransomware, tanto para la cuenta de usuario corporativa como para las empleadas para acceder a servicios de almacenamiento en la nube.

En caso de que se haya realizado un clon del disco duro, se debe utilizar una herramienta de antivirus o antimalware actualizada, es muy importante eliminar el ransomware y sus posibles mecanismos de persistencia antes de recuperar los datos ya que, si no se hace, podrían volver a ser cifrados.

Una vez que se ha conseguido desinfectar el disco duro clonado podremos iniciar el proceso para intentar recuperar los archivos comprometidos.

Finalmente, y como última opción para recuperar la actividad, se procedería con la reinstalación del equipo infectado con el software original y se procedería en la fase de recuperación a restaurar la copia de seguridad más reciente.

5.5. Recuperación

En términos generales, la recuperación puede llevarse a cabo de 3 formas:

Restaurar el último backup disponible

Se trata de la solución más común para luchar contra el ransomware, sin embargo, requiere de una buena solución y estrategia de backup.

Antes de proceder, debemos asegurarnos de que existe una copia de seguridad completa para todos los equipos infectados, en equipos con sistema operativo Windows, es conveniente revisar si el sistema operativo se encuentra configurado para hacer un shapshot periódico del sistema de archivos.

Los snapshots mantienen una versión anterior del sistema de archivos, en estos casos, tendremos que evaluar la perdida de datos para determinar si merece la pena restaurar el sistema de archivos a la fecha del snapshot.

Intentar usar un software de descifrado

Debido a la amenaza creciente y continua de los ataques de ransomware, fabricantes de antivirus y de herramientas de seguridad, están invirtiendo en la creación de herramientas criptográficas que permiten descifrar los archivos infectados por algunas familias de ransomware.

Cada herramienta solo puede recuperar datos infectados por una variante específica de ransomware, es decir, no existe una herramienta general para todos los tipos de ransomware.

A continuación, se proporcionan dos sitios web donde se pueden descargar herramientas de descifrado para diferentes familias de ransomware:

1. No More Ransom

   Se trata de un proyecto colaborativo avalado por la EUROPOL y que cuenta con una base de datos de ataques de ransomware, así como las soluciones (si existieran).

2. Blog de KnowBe4

   Se trata de un sitio web donde podemos encontrar una lista con más de 100 herramientas de descifrado gratuitas.

Si no fuera posible encontrar una herramienta de descifrado en los sitios web mencionados anteriormente, tendremos que recurrir a los sitios web de los principales fabricantes de antivirus en busca de herramientas de descifrado, algunos de ellos disponen de sitios web con herramientas gratuitas que nos permiten restaurar los archivos cifrados por ciertas variantes de ransomware:

- Herramientas de descifrado de Kaspersky
- Herramientas de descifrado de Avast
- Herramienta de recuperación de McAfee
- Herramientas de descifrado de Avg

Muchas familias de ransomware eliminan los archivos originales una vez que los han cifrado, esto abre la posibilidad de recuperar el archivo original mediante el uso de herramientas de recuperación o de técnicas de análisis forense.

Pagar el rescate

Esta opción debería ser considerada como último recurso, aunque la recomendación es que no se acceda a pagar el recate que exigen los ciberdelincuentes, los motivos son los siguientes:

- Pagar no garantiza que se vuelva a tener acceso a los datos, hay que recordar que estamos tratando con ciberdelincuentes, de acuerdo con algunos estudios publicados, la mitad de las víctimas de ransomware no recuperan los archivos infectados después de pagar el rescate [31].

- Si se accede al pago, existe la posibilidad de ser objeto de ataques posteriores dado que los ciberdelincuentes ya saben que estamos dispuestos a pagar.

- Puede que los ciberdelincuentes soliciten una cifra mayor una vez que hayamos pagado.

- Pagar el rescate fomenta el negocio de los ciberdelincuentes.

5.6. Acciones posteriores

Una vez cerrado el incidente debemos registrar todos los datos sobre el mismo, como, por ejemplo, la cantidad y tipo de usuarios afectados, la cantidad y tipo de equipos afectados, segmentos de red afectados, las acciones tomadas, los resultados obtenidos, etc.

De este modo, se pueden detectar mejoras en el procedimiento de actuación en caso de que se repita un incidente similar.

Capítulo 6

Consecuencias de una infección

El impacto y las consecuencias posteriores a una infección de ransomware son muy negativos sobre todo cuando se produce una fuga de información.

Por un lado, la filtración de información puede dañar la imagen pública de la empresa y por tanto impactar negativamente en el negocio, generando desconfianza e inseguridad en clientes y por otro, la publicación de información puede generar consecuencias a terceros: grupos externos de usuarios y otras organizaciones cuyos datos se hayan hecho públicos.

Determinar las consecuencias y el impacto de un incidente de fuga de información es una tarea muy compleja que depende de muchos factores, en este capítulo vamos a analizar algunos de estos factores que servirán como base de cara a establecer las consecuencias y el posible nivel de impacto.

6.1. Estimación de las consecuencias

Básicamente, hay 4 consecuencias que se derivan de un incidente de fuga de información:

- *Daño de imagen*. Genera un impacto negativo en la organización y lleva implícita pérdida de confianza lo que puede conllevar una pérdida de clientes y por tanto de ingresos.

- *Consecuencias legales*. Podrían conllevar sanciones económicas o administrativas si no se cumplen los procedimientos dispuestos en el reglamento general de protección de datos (RGPD).

- *Consecuencias económicas*. Estrechamente relacionadas con las anteriores, se encuentran dentro de aquellas que suponen un impacto negativo a nivel económico, con una disminución de la inversión, negocio, etc.

- *Otras consecuencias*. Son aquellas que afectan o suponen un impacto negativo en ámbitos muy diversos, como, por ejemplo, el ámbito político, diplomático, institucional o gubernamental, entre otros.

Todas estas categorías están relacionadas entre sí y suelen darse conjuntamente, la diferencia estará en función del escenario, donde cada una de ellas tendrá un peso.

A grandes rasgos, hay dos factores que determinarán el escenario, lo cual nos permitirá determinar las posibles consecuencias: el tipo de organización afectada por la fuga de información y el tipo de información que se ha filtrado.

El tipo de organización

El peso de las consecuencias será diferente si el incidente afecta a la administración pública o si se trata de una entidad privada:

- *Administración pública*

  El posible daño e imagen es un factor que cobra importancia desde un punto de vista político, sin embargo, las consecuencias económicas, así como las sanciones debidas al incumplimiento de la legislación, son limitadas.

- *Entidades del sector privado*

  Las consecuencias que tienen mayor peso son aquellas de carácter económico, ya que, a diferencia de las administraciones, el sector privado sí está expuesto a sanciones económicas.

El tipo de información

Otro de los factores adicionales que definen el escenario es el tipo de información que se ha filtrado ya que las consecuencias pueden ser muy distintas:

- *Información confidencial o restringida*

  Aquella información que consideremos crítica para los procesos de la organización, por ejemplo, datos de clientes, contabilidad o datos de los propios trabajadores.

- *Información no confidencial*

  El hecho de su divulgación impactaría en la imagen de la empresa, pero el peso del impacto económico será menor.

- *Datos de carácter personal*

  Cualquier dato que identifique o que pueda ser asociado a una persona identificada, su divulgación o difusión pueden conllevar sanciones para la organización que ha sufrido el incidente.

- *Otros datos*

  Serán aquellos que no son datos de carácter personal, generalmente relacionados con terceros, información técnica u operativa

Para obtener una escala de valor de las consecuencias, es necesario contar con una valoración objetiva tanto de los factores comentados como de otros factores, siguiendo un procedimiento de análisis de riesgos.

6.2. Consecuencias legales

Existe un conjunto de normativas y leyes que ponen especial énfasis en el uso y tratamiento de datos de carácter personal, dentro del tratamiento de datos de carácter personal se han de considerar las fugas de información, ya que, en muchas ocasiones, estos incidentes terminan con la difusión o publicación de datos de carácter personal, dichas normativas prevén sanciones de tipo económico para este tipo de delitos.

Por ejemplo, el **artículo 33 del RGPD**, regula la notificación de una violación de seguridad de los datos personales a la autoridad de control, que en este caso es la agencia española de protección de datos (AEPD) y el **artículo 12 del RGPD**, regula la obligación de notificación a los afectados cuando entrañe un alto riesgo para los derechos y libertades.

La ocultación del incidente de fuga de información también puede ser motivo de sanción por parte de la agencia española de protección de datos (AEPD), ya que entre sus tareas se encuentra detectar fugas de información, por lo tanto, si una empresa oculta un incidente de fuga de fuga de información y la AEPD lo detecta, la sanción podría ser importante.

Por otro lado, el **artículo 82 del RGPD** reconoce el derecho a indemnización al interesado por parte del responsable o encargado del tratamiento por los daños sufridos a causa de una infracción del reglamento.

Concretamente, el **artículo 83, apartado 4, del RGPD**, establece para el caso de incumplimiento del deber de notificación multas administrativas de 10 millones de euros como máximo, con cuantía equivalente al 2% del volumen del negocio total anual global del ejercicio financiero anterior si se tratara de una empresa.

Conclusiones

En este último capítulo se recopilan las conclusiones obtenidas y el posible trabajo futuro que puede surgir.

Las principales conclusiones, a modo de resumen son:

- El ransomware es un tipo de malware que inhabilita el dispositivo de un usuario mediante el cifrado de los archivos, con el objetivo de solicitar el pago de un rescate a cambio de recuperar el acceso a los mismos, en este caso, estamos ante una extorsión.

- En algunos casos, el ransomware roba información confidencial y la envía al atacante con el propósito de amenazar con hacerla pública, en este caso, estamos ante un chantaje.

- Los vectores de ataque más habituales son el correo electrónico, la navegación por sitios web inseguros, la instalación de software pirata y la explotación del protocolo RDP.

- Se deben implementar la mayor cantidad de medidas preventivas a fin de evitar la penetración del ransomware en la red.

- La formación en ciberseguridad es una de las piezas clave en toda estrategia de defensa contra el ransomware.

- Se recomienda navegar por Internet con precaución, evitando sitios de dudosa procedencia, y mantener los dispositivos actualizados.

- En caso de infección, no se recomienda pagar el rescate, en su lugar, hay que reportar el problema a las autoridades y buscar ayuda técnica especializada para solucionar el incidente.

- El éxito de ciberataques como el de WannaCry y la aparición de nuevos modelos de negocio como RaaS que facilitan la distribución de ransomware y lo convierten en un negocio lucrativo para los ciberdelincuentes debe empujar a las organizaciones a tomarse en serio la ciberseguridad.

- Aunque el conocimiento del ransomware se está incrementando, los atacantes están perfeccionando las técnicas de infección y aprendiendo nuevas formas para evadir los sistemas de defensa y evitar ser detectados por lo que es importante mantenerse al día en cuestiones de ciberseguridad.

Con respecto al posible trabajo futuro:

- En la actualidad, el móvil supera al PC como dispositivo principal de acceso a internet, por tanto, es cuestión de tiempo que acaben apariendo nuevas variantes de ransomware especializadas en atacar dispositivos móviles, la anticipación es clave por lo que nuevas técnicas y herramientas de defensa deberían de estudiarse.

- Como se ha expuesto en el trabajo, a parte de las copias de seguridad, otra forma de recuperar los archivos cifrados por el ransomware es el empleo de software de descifrado. El uso de la criptografía como arma de defensa contra el ransomware es otra de las líneas de trabajo que merecería la pena investigar.

- El ransomware of things o RoT, es un ataque relativamente nuevo vinculado con los dispositivos de IoT. A diferencia del ransomware tradicional, que trata de robar datos o información impidiendo que el usuario pueda utilizarlos hasta que pague un rescate, los ataques de tipo RoT están destinados a nuevas tecnologías como asistentes virtuales, cámaras de seguridad y drones con el objetivo de tomar el control de estos y solicitar un rescate a cambio de devolver el control a la víctima.

  Dado el auge que van a tener los dispositivos de IoT en el futuro debido a su valor para transformar la industria en la nueva era digital, se hace indispensable un estudio de la amenaza que puede suponer los ataques de tipo RoT en el futuro.

Glosario

- **IEEE.** Son las siglas de “Institute of Electrical and Electronics Engineers”, es decir, instituto de ingenieros eléctricos y electrónicos, es una asociación mundial dedicada a la normalización y desarrollo en áreas técnicas.

- **NSA.** Son las siglas en inglés de “National Security Agency”, es decir, agencia de seguridad nacional, es la agencia de inteligencia a nivel nacional del departamento de defensa de los Estados Unidos.

- **C&C**. Son las siglas de “Command and Control”, hacen referencia a servidores controlados que se utilizan para enviar comandos a sistemas comprometidos por malware y recibir datos robados de una red.

- **IoT**. Son las siglas de “Internet of things”, hacen referencia a la red de objetos físicos que incorporan sensores, software y otras tecnologías con el fin de conectar e intercambiar datos con otros dispositivos a través de internet.

- **TOR.** Son las siglas de “The Onion Router”, se trata de un proyecto cuyo objetivo principal es el desarrollo de una red distribuida superpuesta sobre Internet que proporciona anonimato en la red.

- **Cybersecurity Ventures.** Es un organismo de investigación y divulgación líder mundial que se encarga de proporcionar datos confiables acerca de economía en la red y estadísticas relacionadas con la ciberseguridad.

- **Esteganografía**: Es una técnica que permite ocultar información en imágenes, como, por ejemplo, scripts, código malicioso, etc.

- **ARPANET**: Se trata de una red creada en 1969 por el departamento de defensa de los Estados Unidos para poder establecer una comunicación entre los distintos organismos gubernamentales del país, siendo una de las primeras formas de lo que hoy conocemos como Internet.

- **Tampering**: Significa modificar o eliminar un recurso sin autorización, en el contexto de la ciberseguridad, el tampering se refiere a la manipulación de archivos y flujos de información con el objetivo de obtener acceso no autorizado a un recurso.

- **INCIBE-CERT.** Es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Asuntos Económicos y Transformación Digital.

- **NIST.** Son las siglas de “National Institute of Standards and Technology”, es decir, instituto nacional de estándares y tecnología, una agencia de la administración de tecnología del departamento de comercio de los Estados Unidos cuya misión es promover la innovación y la competencia industrial.

Referencias

[1]. [10/2021]. CybersecurityVentures. Ransomware damage report

[2]. [10/2021]. Cisco. Security report

[3]. [10/2021]. Wikipedia. AIDS Trojan

[4]. [10/2021]. Wikipedia. Criptovirología

[5]. [10/2021]. Ivanti. The History of the Ransomware Threat

[6]. [10/2021]. Fireeye. A new method to monetize scareware

[7]. [10/2021]. Krebsonsecurity, Inside a 'Reveton' Ransomware Operation

[8]. [10/2021]. Trendmicro. Ransomware: Past, Present, and Future

[9]. [10/2021]. Darkreading. Ransomware has evolved and its name is Doxware

[10]. [10/2021]. Cybersecurityventures, Ransomware damage report

[11]. [10/2021]. Cbsnews, WannaCry ransomware attack losses

[12]. [10/2021]. Wikipedia. Shadow Brokers

[13]. [10/2021]. Kasperskycontenthub. KSN Report: Ransomware and cryptominers

[14]. [10/2021]. Malwarebytes. Cybercrime tactics and techniques: Q2 2018

[15]. [10/2021]. Cybersecurityventures. Cybercrime Damages $6 Trillion By 2021

[16]. [10/2021]. StatCounter. OS market share worldwide Jan 2018/Jan 2019

[17]. [10/2021]. Datto. Datto's Global State of the Channel Ransomware Report 2018

[18]. [10/2021]. Vadesecure. Ransomware Statistics 2017

[19]. [10/2021]. Statista. Spam email traffic share

[20]. [10/2021]. Netskope. Ongoing email campaign spreading globeimposter

[21]. [10/2021]. Elie. Users really do plug in usb drives they find

[22]. [10/2021]. Gdata. Ransomware tries to worm

[23]. [10/2021]. Wikipedia. Stuxnet

[24]. [10/2021]. Microsoft. Locky malware lucky to avoid it

[25]. [10/2021]. Acronis. RaaS DataKeeper

[26]. [10/2021]. Infosecinstitute. How to discover open drp ports with shodan

[27]. [10/2021]. WeliveSecurity. Ataque masivo del ransomware Revil

[28]. [10/2021]. ComputerWorld. 94% of Microsoft vulnerabilities can be easily mitigated

[29]. [10/2021]. F-Secure, "What You Need to Know About WannaCry Now"

[30]. [10/2021]. Osi. Sabías que el 90% de las contraseñas son vulnerables?

[31]. [12/2021]. BleepingComputer. Only half of those who paid a ransomware

Bibliografía

Nihad A. Hassan
Ransomware Revealed
Apress, 2019

[09/2021]. Kanbanize. ¿Qué es Kanban?

[09/2021]. ViewNext. Uso de Kanban en proyectos de desarrollo

[09/2021]. Wikipedia. PMBOK

[09/2021]. Wikipedia. Information Technology Infrastructure Library

[10/2021]. KivuConsulting. The history of ransomware

[10/2021]. ResearchGate. Ransomware evolution target and safety measures

[10/2021]. Wikipedia. Ataques ransomware WannaCry

[10/2021]. Wikipedia. Ransomware

[10/2021]. Upguard. Types of malware

[10/2021]. Wikipedia. Malware

[10/2021]. HackingTutorials. Malware types explained

[10/2021]. ResearchGate. Ransomware attacks análisis threats and prevention

[10/2021]. WeliveSecurity. Formas en que el ransomware se puede comportar

[10/2021]. ResearchGate. Trends in malware attacks against US healthare

[10/2021]. Statista.Major operating Systems targeted by ransomware

[10/2021]. Wikipedia. Phising

[10/2021]. Trendmicro. Types of phising

[10/2021]. Wikipedia. Ataque de abrevadero

[10/2021]. AVG. What is malvertising

[10/2021]. PaloAltoNetworks. What is an exploit kit

[10/2021]. PandaSecurity. Ransomware y macros

[10/2021]. Kaspersky. ¿Qué son los exploits y por qué es una amenaza?

[10/2021]. Redeszone. Try2Cry un ransomware que se abre camino por pendrive

[10/2021]. Upguard. What is ransomware as a service

[10/2021]. WeliveSecurity. Crecieron ataques fuera bruta dirigidos RDP en pandemia

[10/2021]. Securelist. REvil ransomware attack on msp companies

[10/2021]. OSI. ¿Qué es una vulnerabilidad zero day?

[10/2021]. PCRisk. Pirated software led to a ransomware incident

[10/2021]. Microsoft. Microsoft desactiva la red botnet trickbot

[10/2021]. Ijser. Virus Detection techniques and their limitations

[10/2021]. Norton. 5 reasons why software updates and patches are important

[10/2021]. Owasp. Guía contra ransomware

[10/2021]. Cisa. Ransomware guide september 2020

[10/2021]. Sophos. Como protegerse de ransomware

[11/2021]. Incibe. Ransomare, medidas preventivas I

[11/2021]. Incibe. Ransomare, medidas preventivas II

[11/2021]. Vmware. 17 Best practices to protect against ransomware

[11/2021]. Tripware. 30 ransomware prevention tips

[11/2021]. KnowBe4. The best ways to stop malware and ransomware

[11/2021]. Norton. What is juice jacking

[11/2021]. Windows OS hub. How to block ransomware using SRP

[11/2021]. Windows Tech Community. AppLocker another layer in the defense in depth

[11/2021]. Blog Emsisoft. How to secure RDP from ransomware attackers

[11/2021]. TheSslStore. USB Flash Drive Malware, How it Works

[11/2021]. Shophos. When malware goes mobile

[11/2021]. Mimecast. Risk of ransomware speeds the need to patch

[11/2021]. Mimecast. The importance of physical security in the workplace

[11/2021]. OpenSourcedWorkplace. Complete guide to physical security

[11/2021]. Techrepublic. Honeypot reveals tactics used by cybercriminals

[11/2021]. Blog avast. Strong password ideas

[11/2021]. CSOOnline. 6 DNS services protect against malware and unwanted content

[11/2021]. Umbrella Cisco. Using DNS layer security for ransomware attack prevention

[11/2021]. Wikipedia. Data loss prevention software

[11/2021]. Redeszone. Desactivar Powershell 2 en Windows10

[12/2021]. Incibe. Ransomware: Una guía de aproximación para el empresario

[12/2021]. Incibe. Ransomware: Procedimiento de gestión de ciberincidentes

[12/2021]. Iberley. Fugas de información o violaciones de seguridad en el RGPD

[12/2021]. Incibe. Ransomware: Una guía de aproximación para el empresario