UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN
EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO EN SISTEMA DE INFORMACIÓN

TEMA:

ANÁLISIS DE VULNERABILIDAD MS17-010 EN ENTORNOS EMPRESARIALES

ESTUDIANTE:

CEREZO BRAVO STALIN JAVIER

TUTOR:
ING. IVAN RUIZ PARRALES

AÑO:
2023-2024

INDICE

RESUMEN

Para que los países y las organizaciones funcionen, es esencial contar con una seguridad cibernética suficiente para proteger las redes de datos y la información que pasa a través de ellas del riesgo de ataques cibernéticos. La introducción de nuevas tecnologías digitales, junto con la creciente dependencia de las mismas, crea un entorno frágil que no puede ser ignorado para el correcto funcionamiento de diversas funciones en las organizaciones, convirtiéndose en una amenaza potencial para la soberanía nacional.

El aparecimiento del ransomware WannaCry a inicios de mayo de 2017 marcó un hito en la ciberseguridad, impresionando a empresas u organizaciones a nivel mundial, generando una serie de conflictos y pérdidas económicas. La parte central de este ataque radica en la explotación de la vulnerabilidad MS17-010 en sistemas operativos Windows, mostrando las vulnerabilidades relacionas a la gestión de seguridad cibernética de las empresas

Palabras claves: Vulnerabilidades, Amenazas, Cibernética, WannaCry, Tecnologías Entornos empresariales.

ABSTRACT

For countries and organizations to function, it is essential to have sufficient cybersecurity to protect data networks and the information passing through them from the risk of cyber attacks. The introduction of new digital technologies, together with the growing dependence on them, creates a fragile environment that cannot be ignored for the correct functioning of various functions in organizations, becoming a potential threat to national sovereignty.

The appearance of the WannaCry ransomware at the beginning of May 2017 marked a milestone in cybersecurity, impressing companies or organizations worldwide, generating a series of conflicts and economic losses. The central part of this attack lies in the exploitation of the MS17-010 vulnerability in Windows operating systems, showing the vulnerabilities related to the cybersecurity management of companies.

Keywords: Vulnerabilities, Threats, Cybernetics, WannaCry, Technologies Business environments.

PLANTEAMIENTO DEL PROBLEMA

Hoy vivimos una revolución en la gestión, almacenamiento y procesamiento de datos, que facilita a usuarios y empresas garantizar la fiabilidad de su gestión de la información. En esta era de la información, los datos son el activo más valioso, especialmente cuando se trata de información de clientes y usuarios dentro de la organización, por lo tanto, existe una necesidad urgente de que las empresas que quieran crecer en el mercado implementen procesos de seguridad de la información más sólidos y actualizados para evitar la intrusión y el robo de información valiosa.

El aparecimiento del ransomware WannaCry a inicios de mayo de 2017 marcó un hito en la ciberseguridad, impresionando a empresas u organizaciones a nivel mundial, generando una serie de conflictos y pérdidas económicas. La parte central de este ataque radica en la explotación de la vulnerabilidad MS17-010 en sistemas operativos Windows, mostrando las vulnerabilidades relacionas a la gestión de seguridad cibernética de las empresas.

El principal problema reside en la incapacidad de las empresas para anticipar el ataque de WannaCry, por cuanto no se tiene una adecuada atención a la vulnerabilidad MS17-010. A pesar del esfuerzo realizado por Microsoft, al lanzar un parche para corregir esta vulnerabilidad con algunos meses de antelación al ataque, gran cantidad de empresas no efectuaron las actualizaciones necesarias, dejando a sus sistemas informáticos expuestos a el ataque del ransomware.

La propagación rápida y masiva de WannaCry resalta la necesidad crítica de comprender cómo la vulnerabilidad MS17-010 pudo ser explotada con tanta eficacia y cómo las organizaciones podrían haber mitigado este riesgo. Este caso de estudio busca abordar las siguientes preguntas clave; ¿Cómo las organizaciones podrían haber identificado y evaluado proactivamente la vulnerabilidad MS17-010 en sus sistemas antes de la aparición de WannaCry?, ¿Cuáles fueron los desafíos específicos que impidieron que las empresas implementaran parches de seguridad críticos de manera oportuna?, ¿En qué medida la falta de conciencia sobre las amenazas cibernéticas, la complacencia o la subestimación de la importancia de las actualizaciones de seguridad contribuyeron a la vulnerabilidad general?.

Este planteamiento del problema referente al caso de estudio Análisis de Vulnerabilidad MS17-010 en entornos empresariales, instituye la base para investigar a fondo las dinámicas subyacentes que llevaron a la explotación de la vulnerabilidad MS17-010 y proporciona un marco para desarrollar estrategias efectivas de prevención y respuesta ante amenazas cibernéticas similares en entornos empresariales.

JUSTIFICACIÓN

Para que los países y las organizaciones funcionen, es esencial contar con una seguridad cibernética suficiente para proteger las redes de datos y la información que pasa a través de ellas del riesgo de ataques cibernéticos. La introducción de nuevas tecnologías digitales, junto con la creciente dependencia de las mismas, crea un entorno frágil que no puede ser ignorado para el correcto funcionamiento de diversas funciones en las organizaciones, convirtiéndose en una amenaza potencial para la soberanía nacional.

Los problemas involucrados son complejos y se deben desarrollar e implementar estrategias de seguridad informática para abordarlos con el fin de crear una estrategia coherente y efectiva para que los efectos negativos de tales ataques sean controlables y reversibles.

Algunas medidas preventivas consiguen mostrar y reconocer cuándo están siendo atacadas por ransomware y si la información puede ser recuperada de alguna manera. Existen varios tipos y métodos de ataques de ransomware, por lo que es forzoso la realización de un detallado estudio de los distintos tipos de ataques, así como sus procedimientos de mitigación, prevención y recuperación.

Al examinar los países más expuestos al ransomware en los últimos años, comprenderemos en qué mercados se han afianzado los atacantes, por qué el malware ransomware aumentó en 2020 en comparación con años anteriores y qué mercados tienen los sistemas menos seguros. Para ser más cuidadoso, es necesario comprender qué entornos son los más favorecidos por los ciberdelincuentes.

La justificación también reside en la necesidad de resaltar la importancia crítica de la gestión proactiva de parches y actualizaciones en la ciberseguridad empresarial. Examinar por qué muchas organizaciones no implementaron el parche disponible para la vulnerabilidad MS17-010 ofrece perspectivas esenciales.

El análisis detallado de este caso de estudio busca contribuir a la mejora de la resiliencia cibernética empresarial al proporcionar recomendaciones prácticas basadas en las lecciones aprendidas de WannaCry.

Este caso de estudio se justifica no solo por su relevancia histórica y la magnitud del impacto de WannaCry, sino también por la oportunidad que brinda para fortalecer las prácticas de seguridad cibernética en entornos empresariales, abordando directamente la gestión de la vulnerabilidad MS17-010.

OBJETIVOS

Objetivo General

Analizar la evolución del ransomware WannaCry en 2017, centrándose en la explotación de la vulnerabilidad MS17-010 y su impacto en los entornos empresariales.

Objetivos Específicos

Realizar un análisis dinámico para conocer el impacto del ransomware WannaCry en entornos empresariales afectados por la explotación de la vulnerabilidad MS17-010.

Identificar los factores técnicos y organizativos que contribuyeron al éxito del ataque de WannaCry en entornos empresariales.

Documentar las recomendaciones de seguridad específicas y adaptadas a las necesidades de las organizaciones para fortalecer la seguridad cibernética en entornos empresariales.

LÍNEAS DE INVESTIGACIÒN

Este caso de estudio se alinea con la línea de investigación "Sistemas de información y comunicación, emprendimiento e innovación", la cual guarda estrecha relación con el estudio de Desafío de WannaCry, Análisis de Vulnerabilidad MS17-010 en entornos empresariales. Tanto la línea de investigación, como el caso de estudio se combinan con el objetivo de localizar soluciones tecnológicas y fomentar la innovación en el ámbito de la seguridad informática.

La sublínea de investigación "Redes y tecnologías inteligentes de software y hardware" se encuentra vinculada al caso de estudio, por cuanto realiza un análisis detallado de la interacción entre dispositivos.

Al mismo tiempo, la orientación en tecnologías inteligentes propone la utilización de técnicas de aprendizaje, para mejorar el descubrimiento de amenazas en materia de seguridad informática.

Estas líneas de investigación proveen de un marco conceptual apropiado para el Desafío de WannaCry, Análisis de Vulnerabilidad MS17-010 en Entornos Empresariales. Un enfoque interdisciplinario y técnico facilitará la evaluación detallada de riesgos y ofrecerá soluciones innovadoras que contribuirán a fortalecer los sistemas institucionales y la protección de la información.

MARCO CONCEPTUAL

El marco conceptual proporciona el contexto preciso para abordar el caso de estudio sobre WannaCry, Análisis de Vulnerabilidad MS17-010 en Entornos Empresariales.

Cabe recalcar que la ciberseguridad no es sólo la ejecución de medidas de seguridad, sino la capacitación y comprensión de los usuarios, por cuanto el factor humano es la principal causa de infracción de seguridad informática.

De acuerdo a esto, se debe establecer una planificación y estrategia de seguridad que genere capacitaciones al personal que labora en la empresa, sobre prácticas de seguridad informática y el manejo adecuado de la información. Además, las aplicaciones deben actualizarse de forma continua en búsqueda de vulnerabilidades para certificar la prevención de posibles ataques.

Como se estableció, la ciberseguridad es la combinación de estrategias, principios y tácticas que optimizan el control de las vulnerabilidades y amenazas a la información, acrecentando así su integridad y confidencialidad (Robayo, 2022).

Se pueden identificar varios tipos de ataques cibernéticos, pero algunos de ellos son:

Malware

Es un software dañino diseñado para propagarse a través de archivos, correos electrónicos y descargas de sitios web poco fiables con el fin de dañar la computadora, robar archivos y acceder a los derechos del sistema (García, 2022).

Spyware

Programa que realiza un seguimiento de la actividad del usuario en un dispositivo con el fin de hacer un uso indebido de los datos (García, 2022).

Inyección SQL

Es una forma de ataque que contiene la inclusión de código malicioso en una base de datos a través de una consulta SQL, con el objetivo de conseguir datos privados (García, 2022).

Spear Phishing

Se trata de un tipo de engaño digital que se basa principalmente en el correo electrónico con el propósito de obtener acceso no autorizado a información esencial y confidencial. Estos ataques suelen seguir un patrón predecible y pueden afectar tanto a organizaciones del sector público como privado.

Cuando un destinatario hace clic en un enlace dentro de un correo electrónico fraudulento que aparentemente proviene de una institución bancaria, una agencia gubernamental u otra empresa reconocida, se le redirige a un sitio web falso donde se le solicita que proporcione información personal y financiera como su número de tarjeta de débito, detalles de la cuenta bancaria, número de tarjeta de crédito, entre otros. El objetivo principal de este tipo de ataque es el robo de datos financieros y personales (Freire, 2018)

Watering-hole

Este tipo de ciberataque se basa en la observación y el análisis de los sitios web que la víctima potencial visita con frecuencia. A continuación, se instalan programas maliciosos o virus informáticos en estos sitios web, que infectan el ordenador de la víctima y permiten a los piratas

informáticos recopilar diversos tipos de información. Estos ataques utilizan vulnerabilidades de seguridad de día cero, lo que significa que no se hacen públicos hasta que se explota la vulnerabilidad (Freire, 2018).

Man-in-The-Middle

Es llamado ataque de hombre en el medio se origina mediante acciones no autorizadas, como la suplantación de identidad o la duplicación de transacciones, lo que ocasiona una fisura en la seguridad de la red, donde la información se almacena sin consentimiento y se reenvía para engañar al destinatario. Para protegerse de este tipo de ataque es manejando un cifrado sólido entre el servidor y el cliente (Freire, 2018)

Modificación

Este ataque se refiere a las modificaciones ilícitas en el código fuente del software, y los datos enviados a través del canal además pueden ser atacados de manera diferente (García, 2022).

Ataque de denegación de servicio

Es un ataque que bloquea el acceso de los usuarios a los servicios otorgados por el administrador del sistema o de la red. (Freire, 2018).

Ingeniería social

Este tipo de piratería obliga a las víctimas a facilitar información privada, como contraseñas, a los atacantes para obtener acceso a los ordenadores de una empresa (Freire, 2018).

Trashing

Un tipo de ataque que examina la basura de un ordenador (como la Papelera de Reciclaje) en busca de información, suele suponer una grave amenaza para los usuarios que borran información sensible o privada sin borrarla definitivamente (García, 2022).

Ataques de repetición

Es la técnica de interceptar datos o información que se está enviando a través de una red, como puede ser una autenticación a un sistema informático, y luego reenviarla al remitente original sin que el receptor original se dé cuenta de que ha sido interceptada. (L. Quirola, 2019).

Spoofing

La suplantación de identidad es un método de suplantación en línea utilizado por los ciberdelincuentes, normalmente tras una investigación exhaustiva o con el uso de malware. La privacidad de los usuarios y la integridad de los datos están en peligro por las amenazas a la seguridad de la red que utilizan métodos de suplantación (L. Quirola, 2019)

Troyanos

A veces conocidos como caballos de Troya, son programas informáticos que tienen instrucciones ocultas al usuario, de modo que parecen realizar las actividades que el usuario espera que realicen mientras que en secreto llevan a cabo otras operaciones (L. Quirola, 2019)

Virus

Se trata de un conjunto de instrucciones que se introducen en un archivo ejecutable, también conocido como "anfitrión", de tal manera que cuando se ejecuta dicho archivo, el virus se reproduce y se infiltra en otros programas (L. Quirola, 2019)

Gusanos

Un gusano es un programa ejecutable que puede propagarse a través de redes, a veces portando virus o aprovechándose de las vulnerabilidades de los sistemas a los que se conecta para causar daño (L. Quirola, 2019).

Ransomware

El ransomware es un malware que impide que la víctima acceda a datos o sistemas. Para que los usuarios recuperen el acceso a los datos o sistemas, deben pagar un rescate. Cabe señalar que el pago no garantiza que se pueda acceder nuevamente a los datos robados. En general, el ransomware se divide en dos categorías (Deloitte., 2018).

Locker ransomware

Es un ransomware que no cifra los datos, ni el sistema de la víctima. Cuando el software contagia al objetivo, aparece un mensaje falso en la pantalla advirtiendo que se ha bloqueado el acceso del ordenador a páginas web con contenidos sujetos a sanciones legales. Para desbloquear la computadora, la víctima debe pagarle al atacante, por lo que entonces para que esta estafa sea más creíble, el mensaje muestra información como la dirección IP, el ISP o la ubicación geográfica del usuario. (Vidalón-Soldevilla, 2021).

Ransomware Criptolockers

Este tipo de programas maliciosos se diferencian de los anteriores porque en la infección se utilizan algoritmos de cifrado para impedir el acceso a los archivos almacenados en los equipos de los usuarios. Se suelen cifrar archivos ofimáticos y multimedia del equipo del usuario afectado

(Kan, 2018). En este caso, solo conocen la clave de descifrado los cibercriminales y si la víctima quiere recuperar sus ficheros descifrándolos ha de pagarles una cantidad económica por el rescate. Cuando el proceso de cifrado de los ficheros termina, se le muestra al usuario una pantalla donde se le indica los pasos a seguir si quiere recuperar su información cifrada.

Ataques de Ransomware

El 14 de marzo de 2017 Microsoft publica la actualización de seguridad MS17-010 para corregir una vulnerabilidad presente en el protocolo SMB v1 que se utiliza para compartir recursos como archivos e impresoras entre los equipos [123]. Esta vulnerabilidad esta catalogada con el CVE-2017-0144 y afecta a los sistemas Microsoft Windows Vista SP2, Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold y R2, Windows RT 8.1, Windows 10 Gold 1511 y 1607 y a Windows Server 2016. La característica de esta vulnerabilidad es que permite a un atacante remoto ejecutar código arbitrario.

Dos meses después, el 8 de abril de 2017, el grupo de *Hackers malos* "The Sahdow Bokers" publica el exploit EternalBlue que se aprovecha de la vulnerabilidad expuesta en el párrafo anterior.

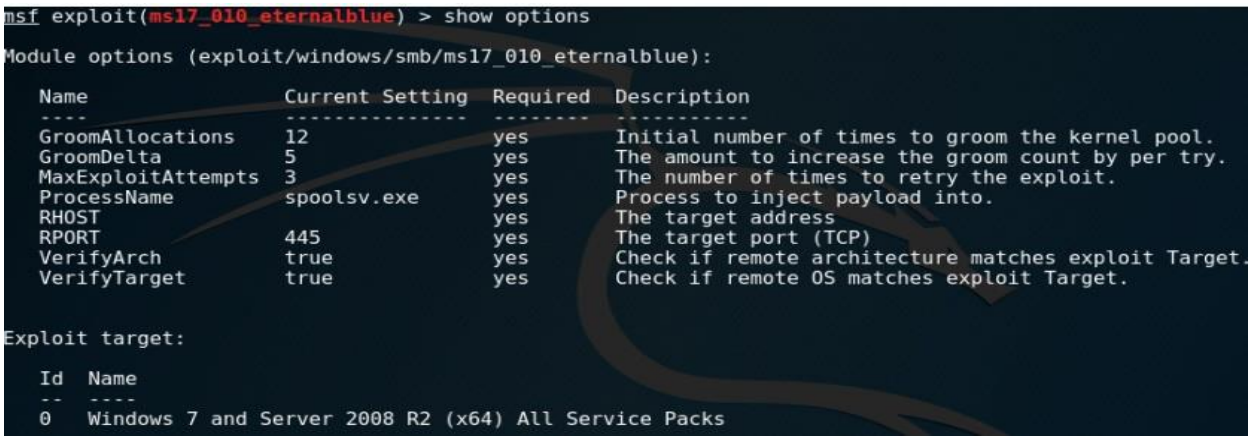

Ilustración 1EternalBlue en Metasploit

Por alguna razón desconocida, quizás falta de concienciación por parte de los usuarios y administradores de sistemas, muchas organizaciones con Windows en sus equipos no aplicaron el parche de seguridad MS17-010 que corregía esta vulnerabilidad (Doodin, 2018).

Otra de las herramientas que fue robada a la NSA por este grupo fue la puerta trasera DoublePulsar (Doodin, 2018). Esta puerta trasera permite dejar a los ciberdelincuentes vía libre al equipo afectado. A continuación, se muestra parte del uso de este exploit en la herramienta Metasploit.

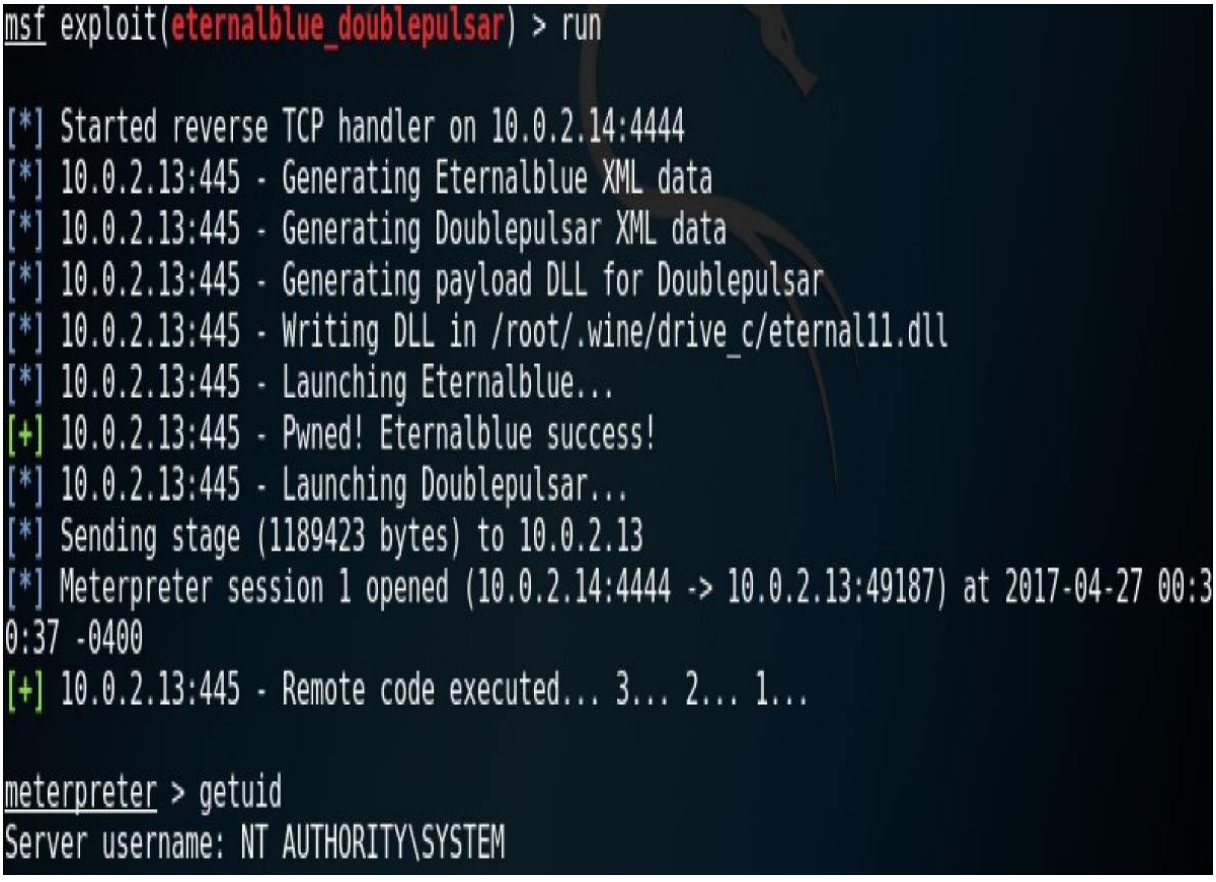

Ilustración 2DoublePulsar en Metasploit

En abril del mismo año, los expertos en seguridad detectan, gracias al escáner de Internet, que más de 107.000 equipos en todo el mundo pueden ser vulnerables a DoublePulsar (Doodin, 2018)

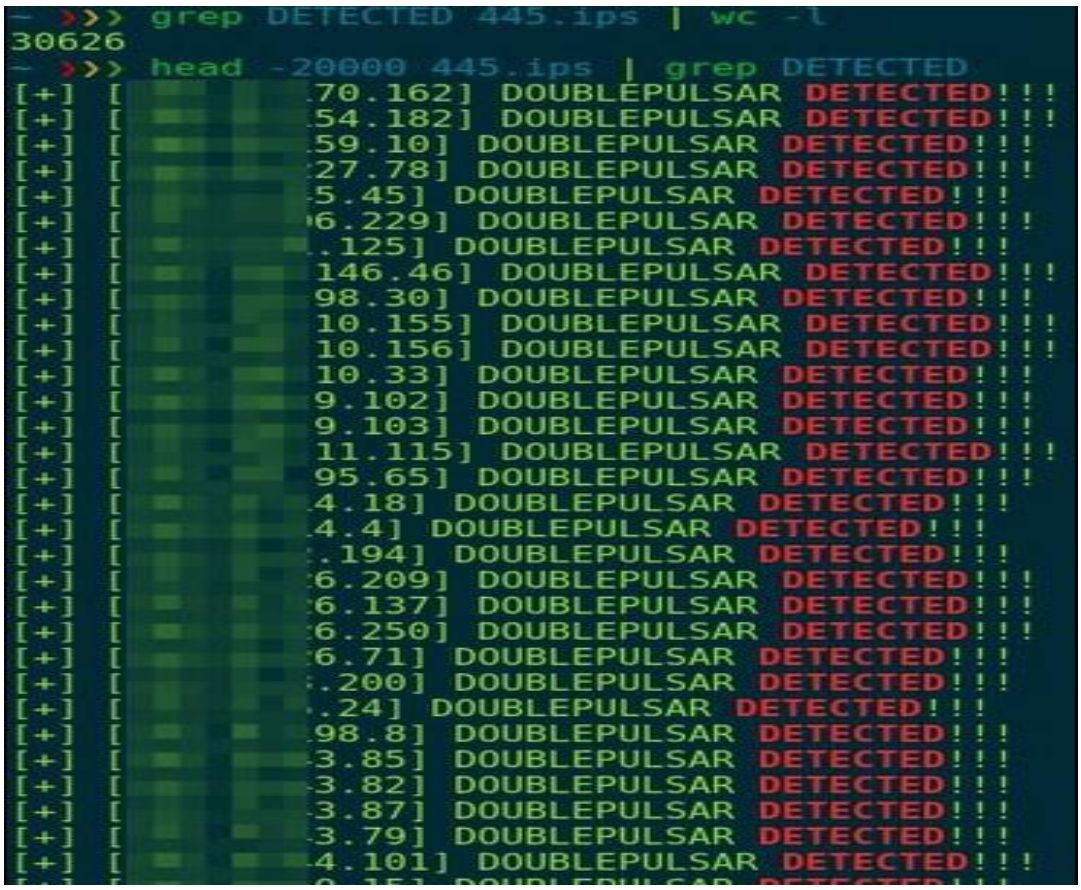

Ilustración 3Resultados parciales del escaneo de DoublePulsar

Los ataques de ransomware más relevantes

Para poder entender y visualizar mejor el progreso del ransomware en los últimos años, se verá que incidentes fueron los que más resaltaron del 2016 al año presente 2021 por su capacidad destructiva, su víctima objetivo e impacto a la organización o redes afectadas. Esto con el propósito de documentar los métodos que usaron y como han evolucionado, así como el denotar las fallas que se tuvieron de parte de las víctimas para haber sucumbido ante el ataque criminal.

WannaCry atacando al mundo

En mayo del 2017 se lanzó un ataque masivo alrededor del mundo, afectando aproximadamente 150 países. El virus enfocaba su ataque en el sistema operativo de Windows, entrando por una de las vulnerabilidades del sistema que existían en ese año, la cual consistía en un protocolo que fallaba del SMB (Server Message Block) del sistema. (Chen, 2018). Wannacry en vez de usar el método de correo electrónico infectado, se infiltró en redes púbicas y escaneaba por sistemas que tuvieran el puerto TCP 445 abierto, el cual pertenecía al SM (Sahi, 2018).

Al entrar al sistema comienza a analizar los archivos y sus contenidos. Aísla al antivirus de sus operaciones para evitar ser detectado. En cuanto termina su análisis el virus encripta con un algoritmo todas las carpetas y archivos ocultándolos del usuario, dejando un mensaje de que la computadora fue infectada y se requiere un pago en criptomonedas para poder tener la contraseña y desencriptar la computadora. (Kan, 2018).

Después de secuestrar al sistema, buscaba formas de expandir su infección por medio de la misma red donde se conectó o por medio de internet. Según los análisis del antivirus “eScan” la India fue de los países más afectados por este ataque con más del 50% de las maquinas afectadas concentrándose dentro de las regiones del país, siendo la región de Madhya la que tuvo mayor concentración de víctimas con un 32.63% de los ataques siendo reportados desde esa locación. (Savita Mohurle, 2018)

Algunas compañías ferrocarrileras en Alemania y Rusia, empresas como FedEx, Nissan, así como departamentos gubernamentales en el Reino Unido fueron gravemente afectadas. Muchas computadoras personales fueron afectadas en escuelas en China. Muchos datos personales e información de las empresas fueron robados o eliminados en el ataque, afectando a las empresas por millones de dolarés. (Savita Mohurle, 2018).

SamSam y la batalla por Atlanta

En el año 2018 la ciudad de Atlanta recibió un paro de actividades repentino. En pocas horas los sistemas administrativos de las diferentes oficinas del ayuntamiento y varios departamentos fueron completamente deshabilitadas por un ataque de ransomware ejecutado por el virus SamSam. Los oficiales de policía tenían que organizar su papelería y emitir órdenes a mano y la plataforma de trabajo de la ciudad estaba sin responder. Años de datos acumulados fueron denegados. La nota dejada por el virus pedía cincuenta y un mil dólares para restaurar los sistemas completamente. (Kraszewski, 2019)

Baltimore contra RobinHood

Los ataques a sistemas gubernamentales crecieron en uso en los últimos años. Siguiendo el ataque en Atlanta, en mayo del 2019 el ransomware conocido como Robinhood atacó la ciudad de Baltimore (Nithya, T., Vijaya, K., Subramanian, D., Balamurugan, E., & Shanmugavel, K, 2020). La oficina de tecnología de la información tuvo que volver a crear alrededor de diez mil credenciales para empleados en turnos dobles diurnos y nocturnos. (James, 2019).

Fujifilm bajo ataque de Qbot Fujifilm

Es un grupo multinacional enfocado en el desarrollo de diferentes productos médicos de alta tecnología con sede en Japón. El primero de junio del 2021 lanzó un comunicado advirtiendo que habían detectado una entrada no autorizada a uno de sus servidores. Al tomar acciones de emergencia, desconectaron sus servidores y parte de la red que estaba infectada. Esto dejó a múltiples aparatos de la marca sin comunicación ni soporte en hospitales alrededor del mundo, además de dejar a la compañía sin formatos de comunicación ni correos electrónicos aislando a sus empleados y administrativos. (Valdeolmillos, 2021).

MARCO METODOLOGICO

Para cumplir con los objetivos del presente caso de estudio se realiza una combinación de las metodologías de investigación exploratoria, descriptiva y explicativa tal y como se expone en los párrafos siguientes.

Para iniciar el estudio de este malware se utiliza una metodología exploratoria que permite conocer el Ransomware de una manera superficial para comenzar a familiarizarnos con este virus.

Posteriormente, se utiliza una metodología descriptiva que nos posibilita profundizar más en el estudio del Ransomware, ya que este método ayuda a poder definir, clasificar y conocer mejor su comportamiento. Además, mediante el uso de esta metodología también se puede estudiar las medidas de protección, tanto técnicas como legales, que existe actualmente en la sociedad española.

Para el estudio del ataque del Ransomware WannaCry se utilizará una metodología explicativa que permite, no solo describir este suceso, sino también buscar los motivos que llevaron a que grandes organizaciones se infectasen con este malware.

Entre las técnicas que se usan para hacer este caso de estudio se encuentra la investigación documental y la recolección de información procedente de numerosas fuentes como son artículos académicos de investigación, libros, noticias y páginas de Internet relacionadas con la seguridad de la información.

Esta estrategia de estudio que se sigue es la más apropiada porque permite comenzar a entender los conceptos básicos y necesarios sobre el virus Ransomware para que, a medida que avanza su lectura, éste pueda entender la problemática que se encuentra detrás de esta amenaza y, de esta forma, pueda reflexionar y concienciarse sobre los riesgos asociados que existen actualmente en los sistemas informáticos.

RESULTADOS

La vulnerabilidad MS17-010 afectaba a los protocolos de compartición de archivos SMB en sistemas operativos Windows. Se identificaron deficiencias en la autenticación, permitiendo a WannaCry propagarse lateralmente en las redes corporativas.

WannaCry utilizó exploits específicos para la vulnerabilidad MS17-010, demostrando una capacidad única para propagarse rápidamente a través de redes conectadas. La explotación se basó en técnicas de ingeniería social y malware para ejecutar código malicioso en sistemas vulnerables.

Las principales barreras para la aplicación de parches incluyeron la falta de conciencia sobre la amenaza, la complejidad de los entornos empresariales, la resistencia al cambio y la falta de procesos efectivos de gestión de parches. La complacencia y la subestimación de la gravedad de la vulnerabilidad MS17-010 también fueron factores contribuyentes.

Se observó un impacto financiero significativo, con pérdidas derivadas de la interrupción operativa, el rescate pagado en casos de ransomware exitoso y la pérdida de clientes debido a la percepción negativa de la seguridad. La falta de preparación y respuesta rápida exacerbó las consecuencias del ataque.

DISCUSIÓN DE LOS RESULTADOS

Los resultados alcanzados en este caso de estudio sobre WannaCry y la vulnerabilidad MS17-010 brindan una visión integral de los desafíos y las oportunidades para fortalecer la seguridad cibernética en entornos empresariales. La discusión se centra en varios aspectos clave.

La falta de aplicación oportuna de parches revela la complejidad inherente en la gestión de vulnerabilidades en entornos empresariales. La coexistencia de sistemas heterogéneos y la necesidad de mantener la continuidad operativa pueden obstaculizar la aplicación ágil de actualizaciones críticas.

Los resultados indican una necesidad apremiante de mejorar la conciencia y la cultura de seguridad organizacional, donde la falta de comprensión de la gravedad de las vulnerabilidades y la resistencia al cambio son barreras importantes que deben abordarse mediante programas continuos de capacitación y concientización.

El impacto financiero y operativo de WannaCry recalca la calidad de la resiliencia empresarial. Las organizaciones que carecían de planes de respuesta a incidentes sólidos experimentaron pérdidas sustanciales. La inversión en medidas proactivas, como sistemas de respaldo y recuperación efectivos, emerge como una estrategia crítica.

Las acciones realizadas por las empresas, las cuales respondieron de manera efectiva a WannaCry destacan la importancia de una buena planificación y ejecución de estrategias de

respuesta a incidentes. Todo esto conllevo al aislamiento de los sistemas comprometidos y la restauración de operaciones minimizando el impacto.

La influencia de factores humanos en la gestión de seguridad es evidente. La falta de conciencia y la cultura de seguridad deficiente contribuyeron significativamente a la falta de aplicación de parches. Abordar estos desafíos requiere un enfoque integral que incluya formación continua, comunicación efectiva y responsabilidad individual.

Las estrategias propuestas para mejorar la gestión de vulnerabilidades ofrecen soluciones prácticas. La automatización de procesos de parcheo, la concienciación continua y la inversión en tecnologías de detección y respuesta avanzada se presentan como elementos clave para mitigar riesgos similares en el futuro.

CONCLUSIONES

El análisis absoluto de WannaCry y la vulnerabilidad MS17-010 en entornos empresariales proporciona conclusiones que tienen implicaciones para la seguridad y la resiliencia empresarial.

La conciencia y la cultura de seguridad son elementos decisivos en la seguridad de los sistemas informáticos, la resistencia al cambio y la complacencia pueden dificultar la aplicación de medidas de seguridad críticas. WannaCry en entornos empresariales, demostró el impacto demoledor que un ataque informático puede ocasionar hablando de términos financieros y operativos. Las empresas afectadas experimentaron pérdidas significativas debido a problemas operativos y pérdida de clientes.

Las empresas que respondieron de manera efectiva a WannaCry destacan la importancia de tener planes de respuesta a incidentes sólidos. La capacidad para aislar rápidamente sistemas comprometidos y restaurar operaciones minimizó el impacto. La preparación y ejecución de estrategias de respuesta son cruciales.

Con este caso de estudio se pudo determinar, como la automatización de procesos de parcheo, la concienciación continua y la inversión en la parte de tecnologías de detección y respuesta avanzada, brindan una alternativa viable para optimizar la resiliencia cibernética. La implementación de estas estrategias debe considerarse como parte integral de la estrategia de seguridad.

RECOMENDACIONES

La implementación efectiva de estas recomendaciones puede fortalecer la resiliencia de las organizaciones frente a amenazas cibernéticas, reduciendo el riesgo de incidentes similares al desafío planteado por WannaCry y la vulnerabilidad MS17-010.

Ejecutar programas de formación continua orientados a seguridad informática para todos los departamentos y a su vez animar a tener una cultura de responsabilidad individual, donde cada uno de los empleados sea consciente del papel importante que tiene dentro de la empresa en la protección contra amenazas informáticas.

Realizar planes de respuesta a incidentes, identificando posibles amenazas y vulnerabilidades a los sistemas informáticos de las empresas. Además, la ejecución de escenarios de ataque donde se puedan realizar pruebas de pentesting para evaluar la eficacia de los protocolos de seguridad.

Implementar soluciones rápidas y eficaces para la detección inmediata de vulnerabilidades, mediante el uso de herramientas de análisis para anticipar y prevenir posibles amenazas.

BIBLIOGRAFÍA

Amado, J. (2020). *SCIELO*. Obtenido de SCIELO: http://www.scielo.org.pe/scielo.php?pid=S1727-558X2020000300011&script=sci_arttext&tlng=pt

Bianchi, N. (2020). *Medium*. Obtenido de Medium: https://medium.com/@nicobf/ibm-watson-analytics-price-ca700859c028

Char, D. S. (2018). *REPOSITORIO.* Obtenido de REPOSITORIO: https://repositorio.unbosque.edu.co/server/api/core/bitstreams/90dab747-26dd-4008-8234-891038e8c191/content

Chen, Q. &. (2018). Automated Behavioral Analysis of Malware A Case Study. *Department of Electrical and Computer Engineering*, 32.

Daniel, L. (2020). inteligencia artificial en salud. *Revsta Innova*, 7.

Deloitte. (2018). *Threat Intelligence and Analytics. Ransomware. Holding Your Data Hostage.* TLP - WHITE.

Doodin, D. (18 de 11 de 2018). *Windows computers may be infected by advanced NSA backdoor.* Obtenido de Windows computers may be infected by advanced NSA backdoor.: https://arstechnica.com/information-technology/2017/04/10000- windows-computers-may-be-infected-by-advanced-nsa-backdoor/

Fernández Fernández, J. L. (2021). *comillas* . Obtenido de comillas: https://repositorio.comillas.edu/xmlui/handle/11531/61801

Freire, K. (2018). *"Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad.* Guayaquil: UCSG.

García, K. (2022). *APLICACIÓN DE HACKING ÉTICO MEDIANTE TEST DE INTRUSIÓN "PENTESTING" PARA LA DETECCIÓN Y ANÁLISIS DE VULNERABILIDADES EN LA RED INALÁMBRICA DE UNA INSTITUCIÓN EDUCATIVA DE LA PROVINCIA DE SANTA.* Santa Elena: UPSE.

health.google. (2020). Obtenido de https://health.google/intl/ALL_mx/health-research/imaging-and-diagnostics/

James, K. (2019). *Protecting Local Governments from Ransomware Attacks*. Obtenido de Protecting Local Governments from Ransomware Attacks: http://www.infosecwriters.com/Papers/kjames_governments_ransomware.pdf

Kan, M. (2018). *Experts worried about ransomware hitting critical infrastructure.* Kendrick St SWashington, EE. UU.: CSO Executive Editorial.

Kraszewski, K. (2019). SamSam and the Silent Battle of Atlanta. *In 2019 11th international conference on cyber conflict*, 1-16.

L. Quirola. (2019). *"ANÁLISIS DE VULNERABILIDADES DE SEGURIDAD INFORMÁTICA DEL SISTEMA DE GESTIÓN MÉDICA SISMEDICALEC, DE LA EMPRESA INCOMSIS.".* Ambato: UTA.

Luna, D. D. (2022). *IntraMed*. Obtenido de IntraMed: https://www.intramed.net/contenidover.asp?contenidoid=59794

Park, O. (2021). *PROQUEST*. Obtenido de PROQUEST: https://www.proquest.com/openview/9691a079da610ce17c0303a54c295cce/1?pq-origsite=gscholar&cbl=2037571

Robayo, H. (2022). *"MODELO DE MEJORA DEL ESTADO DE LA CIBERSEGURIDAD EN LA GOBERNACION DE TUNGURAHUA"*. Ambato: PUCE.

Sahi, S. K. (2018). A study of wannacry ransomware attack. . *International Journal of*, 5-7.

Savita Mohurle, M. P. (2018). A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, 1938.

Topol, E. J. (2019). *REPOSITORIO*. Obtenido de REPOSITORIO: https://repositorio.unbosque.edu.co/server/api/core/bitstreams/90dab747-26dd-4008-8234-891038e8c191/content

Valdeolmillos, C. (4 de 06 de 2021). *MuycomputerPro*. Obtenido de MuycomputerPro: https://www.muycomputerpro.com/2021/06/04/fujifilm-ataque-ransomware

Ventura-Fernández, F. (2021). *SCIELO*. Obtenido de SCIELO: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2664-32432021000100086

Vidalón-Soldevilla, E. (2021). *SCIELO*. Obtenido de SCIELO: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2664-32432021000100086

ANEXOS

Imagen 1: EternalBlue en Metasploit

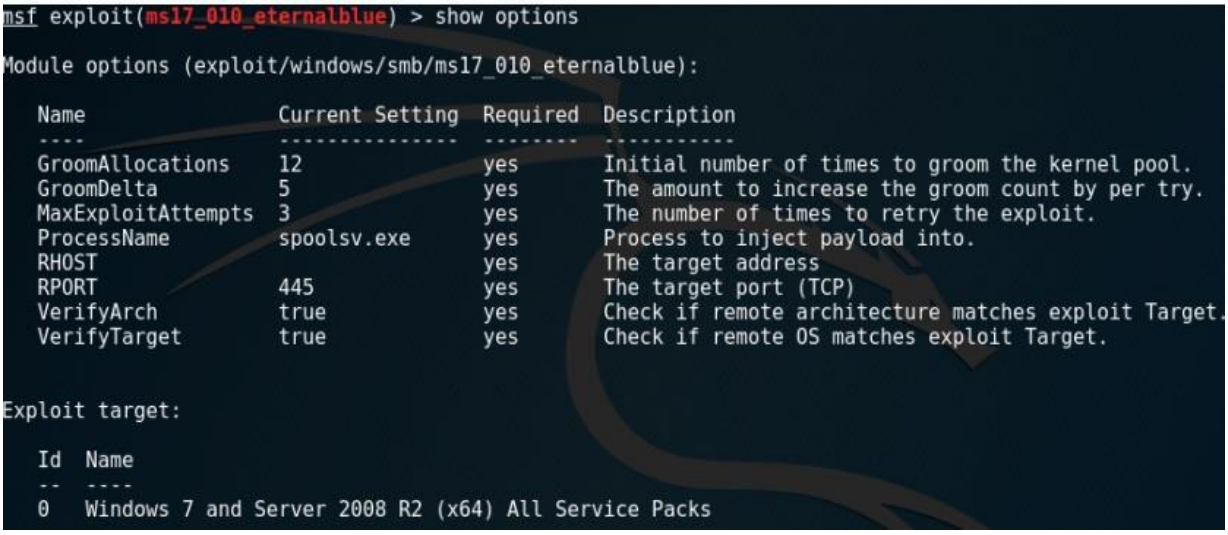

Imagen 2: Exploit en la herramienta Metasploit.

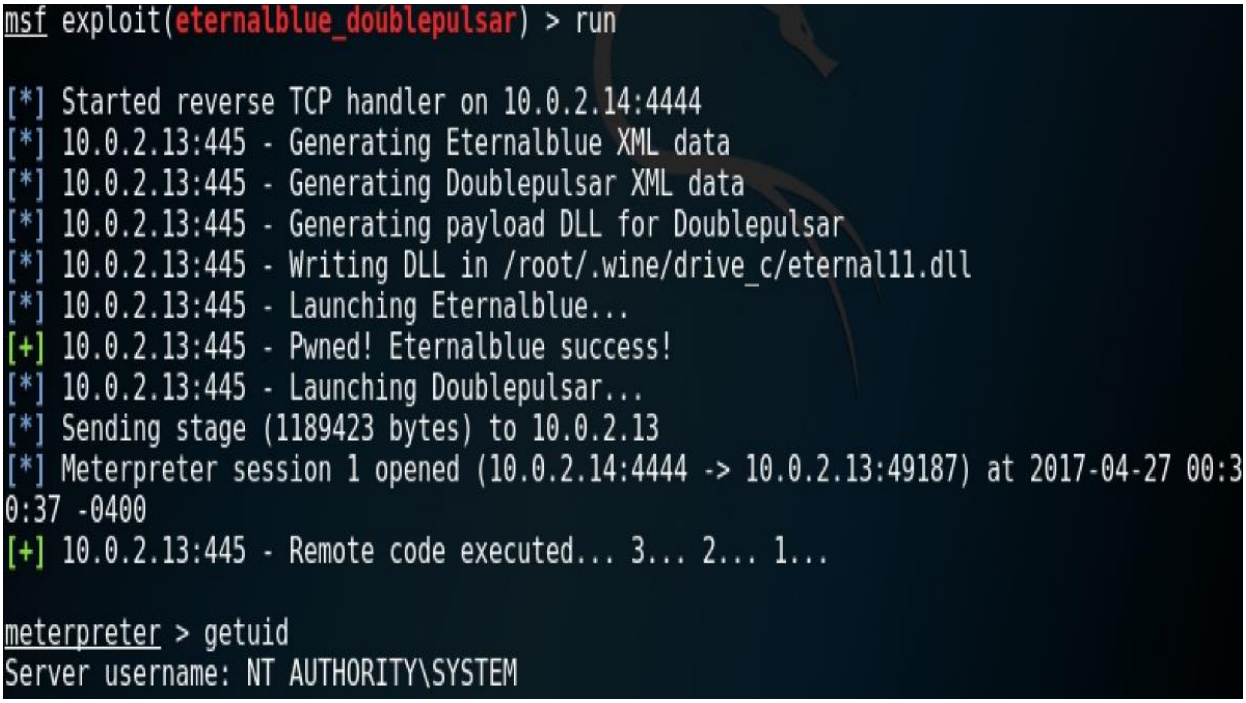

Imagen 3: Resultados parciales del escaneo de DoublePulsar