UIDE

Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Análisis de Detección y Mitigación de Ransomware BlackCat con Tecnología SIEM

AUTOR: Ing. Barba Ayala Edwin Alexander

AUTOR: Ing. Germán Toapanta Danny Javier

AUTOR: Ing. Jara Morillo Walter Sebastián

AUTOR: Ing. Ortega Noroña Jhonny Fabricio

Aprobación Del Tutor

Yo, Jaime Ibarra Jiménez, certifico que conozco a los autores/as del presente trabajo siendo los responsables exclusivos tanto de su originalidad y autenticidad, como de su contenido.

JAIME IBARRA

DIRECTOR DE TESIS

CERTIFICACIÓN DE AUTORÍA

Nosotros, Barba Ayala Edwin Alexander, Germán Toapanta Danny Javier, Jara Morillo Walter Sebastián y Ortega Noroña Jhonny Fabricio, declaramos que bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedo mis derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Apellidos y Nombres	Número de Identificación
Barba Ayala Edwin Alexander	1600739336
Danny Javier Germán Toapanta	1004904312
Jara Morillo Walter Sebastián	1727371211
Ortega Noroña Jhonny Fabricio	1718334947

Apellido y Nombre	Firma
Barba Ayala Edwin Alexander	
Danny Javier Germán Toapanta	
Jara Morillo Walter Sebastián	
Ortega Noroña Jhonny Fabricio	

DEDICATORIA

A mis queridos padres, con infinito amor y gratitud, dedico esta tesis a ustedes. Gracias por ser mi apoyo incondicional, por creer en mí en todo momento y por enseñarme el valor del esfuerzo y la perseverancia. Sus palabras de aliento y su ejemplo de dedicación han sido mi mayor inspiración a lo largo de este camino. Sin su amor y respaldo, este logro no habría sido posible.

Edwin Alexander Barba Ayala

A mi madre, con un amor que desborda y una gratitud que no conoce límites, dedico este proyecto de titulación a ti, mi modelo a seguir y mi guerrera incansable. Gracias por ser mucho más que un apoyo constante: eres mi inspiración diaria, mi ejemplo de valentía y mi fuerza inquebrantable. Tus palabras de aliento y tu ejemplo de dedicación han sido la brújula que ha guiado mis pasos hacia el éxito. Sin tu amor, coraje y respaldo incondicional, este logro que hoy celebro no habría sido posible.

Walter Sebastián Jara Morillo

A mis padres, con gran cariño y agradecimiento, los cuales han estado conmigo en todo momento tanto personal como profesional. Gracias porque me impulsan a mejorar y ustedes han sido mi inspiración ya que siempre han creído en mí, a ustedes decido esta tesis ya que han sido la parte fundamental en mi vida. Sin su cariño y perseverancia no podría haber culminado este nuevo logro.

Danny Javier Germán Toapanta

A mi familia, por su infinito apoyo y paciencia a lo largo de los años, han sido un pilar fundamental en mi desarrollo personal y profesional. Sus mensajes de aliento, en diferentes etapas de mi vida, han sido mi motivación en este largo camino. Esta tesis es un tributo a ustedes, mi fuente inagotable de fortaleza y amor en mi búsqueda de conocimiento y superación.

Jhonny Fabricio Ortega Noroña

AGRADECIMIENTO

Queremos expresar nuestro más sincero agradecimiento a nuestras familias, quienes han sido nuestro pilar fundamental durante el desarrollo de esta tesis sobre ciberseguridad. Su apoyo incondicional y paciencia inagotable nos han dado la fuerza necesaria para superar cada desafío.

Agradecemos especialmente a nuestros padres, por inculcarnos el valor del esfuerzo y la dedicación, y por creer siempre en nosotros. A nuestros hermanos y amigos, gracias por su comprensión y por brindarnos momentos de distracción que nos permitieron recargar energías.

Finalmente, extendemos nuestro agradecimiento a todas aquellas personas que, de una u otra manera, contribuyeron con su apoyo moral y emocional a la culminación de este proyecto. Sin ustedes, este logro no habría sido posible.

RESUMEN

El proyecto de investigación "Análisis de Ransomware BlackCat para Detección y Mitigación con Tecnología SIEM Wazuh" se erige como un pilar fundamental para fortalecer las defensas cibernéticas en Ecuador y enfrentar la creciente amenaza del ransomware BlackCat. Este estudio, enmarcado dentro de la maestría en ciberseguridad, se enfoca en desarrollar estrategias robustas para la detección y mitigación de este tipo de ataques, aprovechando la potencia del SIEM Wazuh y la implementación de scripts en Python para la respuesta activa.

Las pruebas se realizaron en entornos controlados que replican las condiciones operativas de instituciones gubernamentales ecuatorianas, utilizando equipos con sistemas operativos Windows 7, 8 y 10. Esto permite abordar la diversidad tecnológica presente en el país y garantizar la efectividad de las soluciones propuestas.

La metodología adoptada es de enfoque mixto, combinando análisis técnico de informes especializados con pruebas prácticas en laboratorio. Se llevarán a cabo exhaustivos análisis estáticos y dinámicos del ransomware BlackCat para comprender sus mecanismos de acción y desarrollar contramedidas efectivas.

La implementación de SIEM Wazuh se considera crucial en este proyecto, ya que permite una detección proactiva de amenazas mediante la configuración de reglas específicas. Destacan las capacidades de Wazuh para monitorear el comportamiento del ransomware y generar alertas en tiempo real, lo que contribuirá significativamente a fortalecer las defensas cibernéticas en Ecuador.

Además, se enfatizará la importancia de la educación y la concienciación sobre ciberseguridad, así como la necesidad de implementar prácticas de seguridad sólidas y procesos de respuesta eficientes. Se propondrán recomendaciones específicas para mejorar las políticas de seguridad y la preparación ante posibles ataques.

Este proyecto representa un esfuerzo integral para abordar una amenaza cada vez más prevalente en el entorno digital ecuatoriano. Se espera que los resultados obtenidos contribuyan no solo a fortalecer las defensas cibernéticas en el país, sino también a enriquecer el conocimiento en el campo de la ciberseguridad a nivel global.

ABSTRACT

The research project "Analysis of BlackCat Ransomware for Detection and Mitigation with SIEM Wazuh Technology" stands as a fundamental pillar to strengthen cyber defenses in Ecuador and face the growing threat of BlackCat ransomware. This study, framed within the master's degree in cybersecurity, focuses on developing robust strategies for the detection and mitigation of this type of attacks, leveraging the power of SIEM Wazuh and the implementation of Python scripts for active response.

The tests will be carried out in controlled environments that replicate the operating conditions of Ecuadorian government institutions, using computers with Windows 7, 8 and 10 operating systems. This allows addressing the technological diversity present in the country and guaranteeing the effectiveness of the proposed solutions.

The methodology adopted is a mixed approach, combining technical analysis of specialized reports with practical laboratory tests. Extensive static and dynamic analysis of the BlackCat ransomware will be carried out to understand its mechanisms of action and develop effective countermeasures.

The implementation of SIEM Wazuh is considered crucial in this project, as it enables proactive threat detection through the configuration of specific rules. Wazuh's capabilities to monitor ransomware behavior and generate real-time alerts stand out, which will significantly contribute to strengthening cyber defenses in Ecuador.

In addition, the importance of cybersecurity education and awareness will be emphasized, as well as the need to implement sound security practices and efficient response processes. Specific recommendations will be proposed to improve security policies and preparedness for potential attacks.

In summary, this project represents a comprehensive effort to address an increasingly prevalent threat in the Ecuadorian digital environment. It is expected that the results obtained will contribute not only to strengthening cyber defenses in the country, but also to enriching knowledge in the field of cybersecurity globally.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

a. CAPITULO 1

1. Introducción

Contexto de la ciberseguridad:

La ciberseguridad surge como mecanismo de control del ciber riesgo. De forma más precisa, podemos definir la ciberseguridad como el conjunto de técnicas, procedimientos y protocolos encaminados a la protección de la información vinculada a los usuarios de las ciber tecnologías. Esta protección demanda la custodia no solo de la información en sí, sino también de todos los elementos precisos para su correcta gestión. Es decir, la ciberseguridad tiene como objetivo proteger todo tipo de activo o recurso de valor para una persona, empresa u organización. (Arroyo Guardeño, 2020)

Las instituciones gubernamentales están inmersas en un entorno tecnológico dinámico y complejo, donde el uso generalizado de sistemas informáticos y la constante conectividad exponen a estas entidades a amenazas cibernéticas. Entre estas amenazas, el ransomware ha surgido como una de las más prominentes y perjudiciales para la seguridad de la información.

Evolución del Ransomware a través de los años:

Ransomware es un tipo de malware que ha evolucionado hasta convertirse en una amenaza importante para los activos de datos y los recursos informáticos de los usuarios. Su modus operandi consiste en cifrar los archivos del usuario, inutilizarlos y, posteriormente, exigir el pago por la clave de descifrado. Estos archivos pueden incluir una amplia gama de activos de datos, como

documentos, archivos comprimidos, bases de datos, fotografías, correos electrónicos.(Cen et al., 2024)

Las víctimas tienen la opción de pagar un rescate para mantener su reputación o pagar una tarifa para descifrar y restaurar sus datos. El primer ataque de ransomware conocido fue lanzado en 1989 por Joseph L. Popp, un científico evolutivo. Desde entonces, el ransomware ha pasado por tres etapas distintas de evolución: germinación, activa y epidémica (Cen et al., 2024).

Dentro de la categoría de ransomware, la variante denominada "BlackCat" ha demostrado ser una amenaza significativa, comprometiendo la integridad y confidencialidad de la información crítica. Este escenario plantea desafíos sustanciales para la seguridad cibernética de las instituciones gubernamentales, que constantemente buscan fortalecer sus defensas ante la evolución constante de estas amenazas.

En respuesta a esta realidad, se presenta el proyecto de investigación titulado "Análisis de Detección y Mitigación de Ransomware BlackCat con tecnología SIEM". El propósito fundamental de este proyecto es realizar un examen exhaustivo de los posibles vectores de ataque asociados a BlackCat y desarrollar estrategias efectivas de detección y mitigación.

Este proyecto se centra en fortalecer las capacidades de detección y respuesta ante posibles ataques de ransomware, contribuyendo así a la seguridad cibernética integral de los diferentes sistemas de computación utilizados por personas e instituciones. La aplicación de metodologías avanzadas y tecnologías especializadas se convierte en un aspecto crucial para proporcionar a las diferentes entidades las herramientas necesarias para enfrentar esta amenaza.

La importancia de esta investigación radica en su enfoque proactivo hacia los desafíos que representa un ransomware en el ámbito cotidiano. A través de un análisis técnico detallado y la evaluación de percepciones de usuarios y conocedores de ciberseguridad, se busca obtener una comprensión completa de la amenaza BlackCat.

En resumen, la combinación de análisis técnico y evaluación de percepciones proporcionará una visión integral de la amenaza, permitiendo el desarrollo de estrategias preventivas y la implementación de medidas efectivas para salvaguardar la infraestructura digital de una entidad o un computador personal. Este proyecto no solo aborda las preocupaciones actuales, sino que también establece un marco sólido para la anticipación de futuras amenazas cibernéticas.

2. Revisión de Literatura/Marco Teórico

La revisión de literatura desempeña un papel crucial al contextualizar el proyecto "Análisis de Detección y Mitigación de Ransomware BlackCat con tecnología SIEM" en el panorama actual de ciberseguridad. Este marco teórico busca ofrecer una visión integral de las tendencias y desafíos que enfrenta la seguridad cibernética, con un enfoque específico en la evolución del ransomware y el papel clave que desempeña la tecnología SIEM.

La variante BlackCat ha emergido como una amenaza significativa, comprometiendo la integridad y confidencialidad de la información crítica. Para comprender completamente esta amenaza, es esencial explorar las modalidades delictivas en constante evolución que utilizan tácticas cada vez más sofisticadas. BlackCat, al igual que otras cepas de ransomware, explota la

falta de conocimiento de los usuarios, infiltrándose de manera sigilosa y causando daños substanciales cuando se activa.

La estrategia del ransomware se asemeja al antiguo truco del caballo de Troya, donde la aparente benignidad oculta un potencial perjudicial. Este análisis permite identificar similitudes, ya que el ransomware se oculta en archivos que aparentan ser inofensivos, siguiendo un patrón de infiltración engañoso. La comparación se extiende a la estrategia del caballo de Troya, donde los troyanos percibieron el caballo como un símbolo de victoria antes de enfrentar graves consecuencias. De manera similar, BlackCat opera en la sombra hasta activarse, causando estragos en la seguridad informática.(Pereira & Huey, 2022)

En este contexto, es crucial explorar a fondo las diversas estrategias de mitigación disponibles. Además de contar con soluciones tecnológicas como SIEM (Tecnología de Información y Gestión de Eventos de Seguridad), es fundamental implementar prácticas de seguridad sólidas y educar a los usuarios sobre las amenazas potenciales. Las estrategias de respaldo de datos y la segmentación de redes también son componentes clave en la defensa contra el ransomware. Un enfoque holístico que combine tecnología, procesos y concienciación es fundamental para mitigar eficazmente esta amenaza en constante evolución.

Los sistemas SIEM se centran en acumulación de datos que recopila registros de eventos generados por herramientas de monitoreo, agregación de registros que combina registros similares, eventos, estandarización de registros que convierte registros heterogéneos en un formato común, correlación de registros que combina múltiples eventos normalizados en un único evento

correlacionado y almacenamiento de registros que almacena todos los registros (Raja & Vasudevan, 2017)

Al profundizar en la literatura disponible sobre ransomware y su relación con tecnologías como SIEM, se pueden identificar enfoques innovadores y mejores prácticas que pueden ser aplicadas en la protección de sistemas y datos críticos

Este análisis crítico de la literatura establece la base para comprender la amenaza del ransomware BlackCat y subraya la necesidad imperante de fortalecer las defensas cibernéticas. La siguiente sección detallará la metodología de investigación, delineando cómo abordaremos este desafío y contribuiremos al avance de la ciberseguridad en diferentes entornos.

3. Objetivos

Objetivo General:

- Analizar y mitigar la amenaza del ransomware BlackCat utilizando la tecnología SIEM Wazuh para fortalecer la ciberseguridad en entornos gubernamentales y empresariales en Ecuador.

Objetivos Específicos:

- Realizar un análisis detallado del ransomware BlackCat, incluyendo su comportamiento y métodos de propagación.
- Implementar y configurar el SIEM Wazuh en un entorno controlado para detectar actividades asociadas al ransomware BlackCat.
- Desarrollar un script en Python para la respuesta activa, capaz de prevenir y mitigar los ataques de ransomware basados en las detecciones de Wazuh.
- Evaluar la eficacia del SIEM Wazuh en la detección temprana y mitigación del ransomware BlackCat a través de pruebas en sistemas operativos Windows 7, 8 y 10.
- Proponer recomendaciones para la mejora continua de las estrategias de ciberseguridad contra ransomware en entidades gubernamentales y empresariales.

4. Alcance

Análisis del Ransomware BlackCat:

Estudio del comportamiento del ransomware, sus vectores de ataque, métodos de cifrado y evaluación del impacto en diferentes sistemas operativos (Windows 7, 8 y 10).

Implementación del SIEM Wazuh:

Despliegue del SIEM Wazuh en un entorno de laboratorio replicando las condiciones de entornos gubernamentales y empresariales.

Configuración de reglas específicas para la detección de actividades maliciosas asociadas con BlackCat.

Desarrollo y Pruebas del Script en Python:

Creación de un script en Python para la respuesta activa a incidentes detectados por Wazuh.

Pruebas del script en diferentes entornos operativos para validar su efectividad.

Evaluación de la Eficacia:

Medición de la eficacia del SIEM Wazuh en la detección y mitigación del ransomware.

Análisis de datos recopilados durante las pruebas para identificar patrones y mejorar las reglas de detección.

5. Justificación

Relevancia y Necesidad:

La creciente incidencia de ataques de ransomware, como BlackCat, representa una amenaza significativa para la seguridad de la información en organizaciones de todo el mundo, incluyendo Ecuador. Las instituciones gubernamentales y empresas enfrentan riesgos sustanciales de pérdida de datos, interrupción de servicios y daños financieros. Este proyecto es fundamental para mejorar las capacidades de defensa cibernética en el país, proporcionando herramientas y estrategias para detectar y mitigar estas amenazas de manera proactiva.

Innovación y Contribución:

El uso del SIEM Wazuh, combinado con un script de respuesta activa en Python, representa un enfoque innovador para la gestión de incidentes de seguridad. Este proyecto no solo aborda la amenaza específica del ransomware BlackCat, sino que también establece un marco adaptable para enfrentar futuras variantes de ransomware y otros tipos de ciberamenazas. La investigación contribuirá al conocimiento global en ciberseguridad y servirá como referencia para futuras iniciativas similares.

Beneficios Esperados:

Fortalecimiento de las defensas cibernéticas en entornos gubernamentales y empresariales.

Reducción del riesgo de incidentes de ransomware y minimización del impacto de ataques exitosos.

Mejora continua de las estrategias de ciberseguridad basadas en la experiencia y los datos obtenidos durante el proyecto.

Creación de un entorno más seguro y resiliente frente a amenazas cibernéticas, beneficiando a la sociedad en general al proteger la infraestructura crítica y los datos sensibles.

b. CAPITULO 2

i. Metodología de Investigación:

La metodología de investigación para el proyecto "Análisis de Detección y Mitigación de Ransomware BlackCat con tecnología SIEM" se diseñó para proporcionar un enfoque integral y riguroso que garantice la obtención de un análisis claro y completo. La estructura metodológica adopta un enfoque mixto, combinando elementos cuantitativos y cualitativos para obtener una comprensión completa de la amenaza del ransomware BlackCat y evaluar la efectividad de las contramedidas propuestas.

ii. Diseño de la Investigación:

Se ha optado por un diseño de investigación exploratorio con el fin de llevar a cabo un análisis exhaustivo de la amenaza del ransomware BlackCat y evaluar la efectividad de la implementación de contramedidas utilizando la tecnología SIEM. Este enfoque flexible y abierto permitirá una exploración detallada del fenómeno en cuestión, facilitando la generación de nuevas ideas y la identificación de variables relevantes para proponer estrategias eficaces de mitigación.

"El diseño de investigación exploratorio se utiliza para investigar fenómenos poco conocidos o comprendidos, con el objetivo de generar nuevas ideas, identificar variables relevantes y desarrollar hipótesis para investigaciones futuras. Este enfoque es flexible y abierto, permitiendo al investigador adaptar el estudio a medida que se recopilan datos y surgen nuevas ideas. Los métodos cualitativos y cuantitativos pueden emplearse en un diseño exploratorio, dependiendo del tipo de datos que se esté investigando y los objetivos del estudio." (Creswell, 2014).

iii. Población y Muestra:

La población objetivo de este estudio está constituida por entornos empresariales, personales, gubernamentales y organizaciones similares que podrían ser susceptibles a ataques de ransomware. La muestra se seleccionará de manera estratégica, enfocándose en entidades con experiencias previas o potencialmente vulnerables a la cepa BlackCat. La combinación de datos cuantitativos y cualitativos permitirá una evaluación exhaustiva de la situación.

iv. Recopilación de Datos:

Datos Cuantitativos: Se recopilarán datos mediante encuestas estructuradas, evaluando la percepción de los usuarios y expertos sobre la amenaza del ransomware BlackCat y la eficacia percibida de las soluciones de SIEM. Se utilizarán análisis estadísticos para interpretar los resultados cuantitativos.

Datos Cualitativos: Se realizarán análisis de informes técnicos y revisiones de literatura para comprender a fondo incidentes pasados de ransomware BlackCat. El análisis temático se aplicará a los datos cualitativos, identificando patrones y tendencias.

v. Ransomware Blackcat ALPHV

ALPHV, también conocido como BlackCat o Noberus, es una familia de ransomware que se implementa como parte de las operaciones de Ransomware como servicio (RaaS). ALPHV está escrito en el lenguaje de programación Rust y admite la ejecución en Windows, sistemas operativos basados en Linux (Debian, Ubuntu, ReadyNAS, Synology) y VMWare ESXi.

Blackcat se comercializa como ALPHV en foros de cibercrimen, pero los investigadores de seguridad lo llaman comúnmente BlackCat debido al ícono de un gato negro que aparece en su sitio de filtración. Se ha observado que ALPHV se implementa en ataques de ransomware desde el 18 de noviembre de 2021.(Pereira & Huey, 2022)

En las versiones últimas del ransomware BlackCat no permite la ejecución de la muestra sin el conocimiento previo del valor ***"—access-token".***

Las principales características de esta familia son:

- Eliminación de las copias de seguridad locales.
- Eliminación de los snapshots en sistemas ESXi.
- Eliminación de los eventos del sistema.
- Configuración en formato JSON cifrada con parte del parámetro "-- access-token"
- Propagación por la red, haciendo uso de PsExec y credenciales de administrador.
- Uso combinado de los algoritmos Salsa20 y RSA, para la realización del cifrado de los ficheros.

vi. Flujo de infección

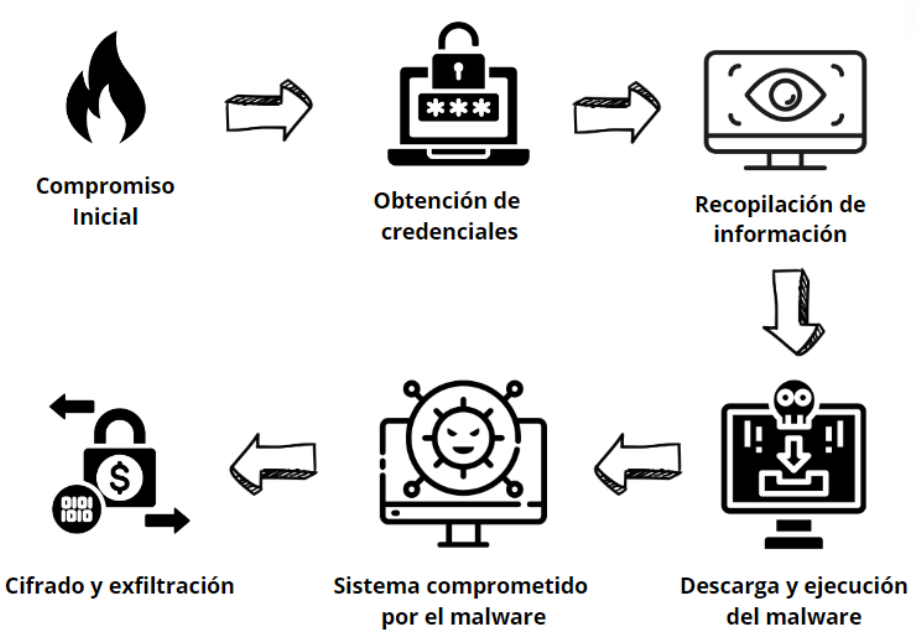


Figura 1 Flujo de Infección

Teniendo en cuenta la forma en que se han realizado los ataques con este malware, el flujo de infección que termina derivando en que la detonación del ransomware puede variar de unos casos a otros.

Dado que el ransomware no posee altas capacidades para propagarse a través de Internet, el proceso de compromiso inicial es llevado a cabo por operadores humanos.

Una vez comprometido el sistema, los atacantes recopilan credenciales e información sobre la víctima hasta que deciden ejecutar el ransomware que cifrará toda la información y con el cual habrá concluido el ataque

Al igual que otros operadores de ransomware, el grupo detrás de BlackCat estaría tratando de llevar a cabo un modelo de doble extorsión. Siguiendo este modelo, además de reclamar una suma de dinero en criptomonedas a cambio de descifrar la información, amenazan con filtrar los datos que han robado, venderlos al mejor postor si las víctimas se niegan a pagar o sencillamente haciéndolos accesibles al público y devaluando la marca.(Santos, 2022)

Solo filtrará archivos que contengan las siguientes extensiones y estén dentro del umbral de tamaño de archivo:*.bmp, .doc, .docx, .dwg, .ipt, .jpeg, .jpg, .msg, .pdf, .png, .pst, .rdp, .rtf, .sql, .txt, .xls, .xlsx, .zip*.

vii. Wazuh

Wazuh, como plataforma de seguridad de acceso libre y código abierto, fusiona las funciones de XDR y SIEM para salvaguardar las cargas de trabajo en diversos entornos, ya sean locales, virtuales, en contenedores o en la nube. Su amplio uso por parte de organizaciones de todos los tamaños, tanto a nivel mundial como local, subraya su eficacia en la protección de los activos de datos frente a posibles amenazas, beneficiando tanto a entidades empresariales como a individuos preocupados por la seguridad.(Görmez et al., 2023)

1. Funcionamiento

La funcionalidad esencial de Wazuh se basa en la interacción entre sus tres componentes principales: el agente de Wazuh, el servidor de Wazuh y el panel de control de Wazuh. El agente, desplegado en los dispositivos monitoreados, recopila datos relevantes sobre la actividad del sistema y los envía al servidor. Este último, a su vez, analiza los datos utilizando decodificadores

y reglas predefinidas para identificar posibles amenazas. Finalmente, el panel de control proporciona una interfaz intuitiva para visualizar y analizar estos datos, permitiendo una respuesta eficiente a las amenazas detectadas.

2. Componentes y Arquitectura:

Agente de Wazuh

El agente de Wazuh es el corazón de la operación. Se despliega en los puntos finales que se desean monitorear, como servidores, estaciones de trabajo o dispositivos en la nube. Este agente recopila datos de actividad del sistema, como registros de eventos, información de integridad de archivos y configuraciones del sistema, y los transmite al servidor para su análisis.

Servidor de Wazuh

El servidor de Wazuh es el componente central encargado de procesar y analizar los datos recibidos del agente. Utiliza decodificadores y reglas para interpretar la información y detectar posibles amenazas. Además, gestiona la configuración y actualización de los agentes de forma remota.

Panel de Control de Wazuh

El panel de control de Wazuh, por su parte, proporciona una interfaz web para visualizar y analizar datos, con paneles preconfigurados para diferentes tipos de eventos de seguridad y cumplimiento normativo, entre otros aspectos. Además de instalarse en equipos como computadoras portátiles, servidores o máquinas virtuales, los agentes de Wazuh pueden monitorear

dispositivos sin necesidad de agente, como firewalls o routers, utilizando métodos como Syslog o SSH.(Tomás Guerra, 2019)

3. Características principales de Wazuh

Recopilación de datos: Wazuh SIEM puede recopilar datos de registros de eventos y de actividad de sistemas, aplicaciones y dispositivos en tiempo real. Esto incluye registros de seguridad del sistema operativo, registros de aplicaciones, registros de firewall, registros de red, etc.

Normalización de datos: Wazuh normaliza los datos recopilados de diferentes fuentes para facilitar su análisis y correlación. Esto permite una comprensión coherente de los eventos de seguridad, independientemente de la fuente de origen.

Detección de amenazas: Wazuh utiliza reglas de detección predefinidas y personalizables para identificar posibles amenazas de seguridad, como intrusiones, malware, comportamiento anómalo, etc. Estas reglas se basan en indicadores de compromiso (IOC), patrones de comportamiento y firmas de malware.

Análisis de comportamiento: Además de las reglas de detección específicas, Wazuh puede realizar análisis de comportamiento para identificar actividades inusuales o sospechosas en los sistemas, lo que puede indicar una posible intrusión o compromiso.

Correlación de eventos: Wazuh SIEM es capaz de correlacionar eventos de seguridad de múltiples fuentes para identificar patrones y relaciones entre diferentes eventos. Esto ayuda a

detectar ataques sofisticados que pueden pasar desapercibidos al analizar eventos de manera individual.

Generación de alertas: Cuando se detecta una actividad sospechosa o un evento de seguridad relevante, Wazuh SIEM puede generar alertas en tiempo real para notificar a los administradores de seguridad sobre la amenaza potencial.

Integración con otras herramientas: Wazuh SIEM se integra con otras herramientas de seguridad y sistemas de gestión para proporcionar una visión completa de la postura de seguridad de una organización. Esto incluye integraciones con soluciones de análisis de registros, análisis de vulnerabilidades, gestión de incidentes, etc.

El siguiente diagrama muestra la arquitectura de conexión de Wazuh:

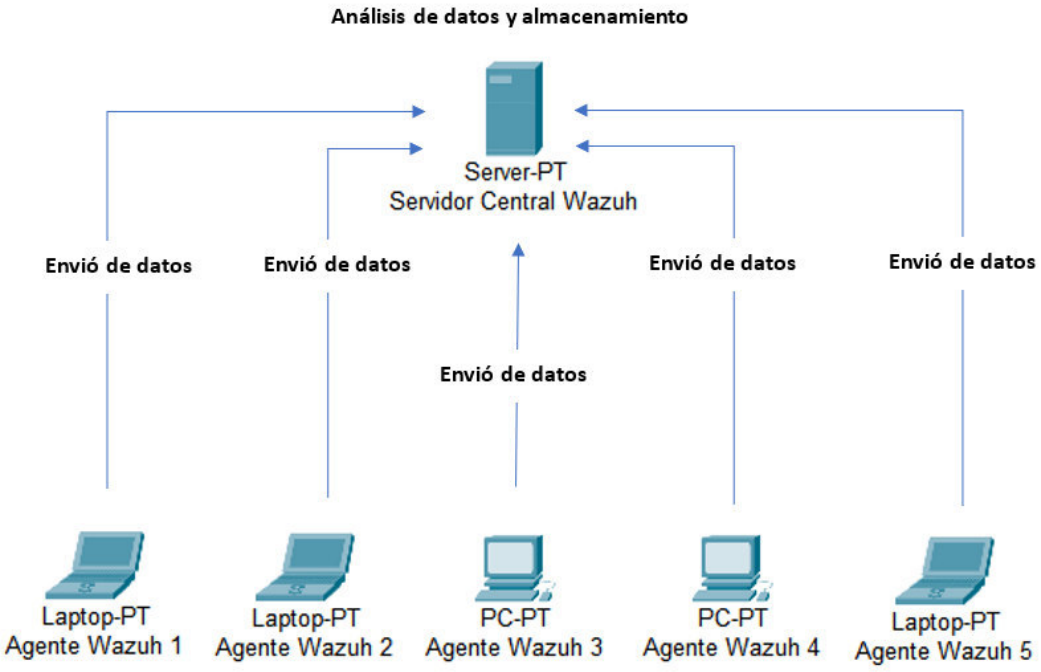


Figura 2 Arquitectura SIEM Wazuh con Agente

viii. Sysmon

SYSMON, desarrollado por Mark Russinovich y su equipo en Sysinternals (ahora parte de Microsoft), es una herramienta de supervisión y registro de eventos diseñada para sistemas operativos Windows. Surgió en respuesta a la necesidad de tener una mayor visibilidad y control sobre la actividad del sistema, especialmente en entornos empresariales donde la seguridad y el rendimiento son críticos. Funciona interceptando y registrando eventos del sistema a nivel del kernel, lo que le permite capturar una amplia gama de actividades, como la creación de procesos, cambios en el registro, acceso a archivos, conexiones de red y más. SYSMON utiliza reglas de configuración flexibles que permiten a los administradores personalizar qué eventos desean monitorear y cómo desean que se registren. (Smiliotopoulos et al., 2022)

Esta capacidad de personalización lo hace extremadamente versátil y adecuado para una variedad de casos de uso, incluida la detección de amenazas, la respuesta a incidentes, el cumplimiento normativo y el análisis forense. Al proporcionar una visión detallada de la actividad del sistema, SYSMON ayuda a los administradores a identificar y responder rápidamente a comportamientos sospechosos o maliciosos, lo que fortalece la seguridad de la infraestructura informática. Su popularidad y utilidad lo han convertido en una herramienta esencial en el arsenal de muchos profesionales de TI y expertos en seguridad cibernética. Desde su lanzamiento inicial, SYSMON ha evolucionado continuamente con nuevas características y mejoras para mantenerse al día con las demandas cambiantes del paisaje de seguridad informática en constante evolución.

Listas CDB

Las listas CDB (Comma-Delimited Browser Display) son un componente importante en Wazuh que se utiliza para realizar búsquedas rápidas y eficientes en grandes conjuntos de datos. Las listas CDB en Wazuh son archivos de texto plano que contienen registros de datos en formato CSV, donde cada línea representa un registro y los campos están separados por comas. Estas listas se utilizan principalmente para almacenar datos que se necesitan buscar o comparar con frecuencia, como direcciones IP maliciosas, nombres de dominio sospechosos, hashes de archivos conocidos por ser maliciosos, entre otros.

Wazuh proporciona herramientas para gestionar y utilizar estas listas CDB de manera eficiente, lo que facilita la búsqueda y correlación de datos durante el análisis de seguridad.

Cómo se utilizan las listas CDB en Wazuh:

Las listas CDB se utilizan en Wazuh para realizar consultas rápidas sobre conjuntos de datos específicos. Por ejemplo, se pueden buscar direcciones IP sospechosas en una lista CDB de direcciones IP maliciosas. Wazuh proporciona reglas predefinidas que utilizan estas listas CDB para detectar actividades maliciosas. Por ejemplo, una regla puede comparar las direcciones IP encontradas en los registros del firewall con una lista CDB de direcciones IP conocidas de botnets. Además, los usuarios pueden crear sus propias reglas personalizadas para utilizar listas CDB en Wazuh según sus necesidades específicas de seguridad. (Wazuh, 2024)

Cómo implementar listas CDB en Wazuh:

Para implementar listas CDB en Wazuh, primero necesitas crear o adquirir las listas de datos que deseas utilizar. Estas listas pueden contener direcciones IP maliciosas, nombres de

dominio sospechosos, hashes de archivos maliciosos, etc. Una vez que tengas las listas CDB, puedes cargarlas en el directorio de listas de Wazuh. Por lo general, este directorio se encuentra en /var/ossec/lists. Después de cargar las listas CDB, puedes utilizarlas en las reglas de Wazuh para realizar búsquedas y correlaciones de datos durante el proceso de monitoreo y detección de amenazas. Es importante mantener actualizadas las listas CDB para garantizar la eficacia de las reglas de detección que las utilizan. Puedes programar actualizaciones periódicas de las listas o realizar actualizaciones manuales según sea necesario. (Wazuh, 2024)

ix. Implementación de SIEM Wazuh:

La infraestructura de SIEM Wazuh se desplegará en un entorno controlado, replicando el ambiente operativo de diferentes escenarios, como lo es un computador personal en una red doméstica. Se configurarán reglas específicas para la detección de comportamientos maliciosos asociados con el ransomware BlackCat, utilizando file hashes en listas CDB para la identificación y un script en Python para prevenir posibles ataques.

1. Análisis de Datos:

Para los datos cuantitativos, se utilizarán técnicas estadísticas como análisis descriptivo e inferencial. El análisis cualitativo implica la identificación de patrones emergentes y la codificación temática.

Esta metodología integral permitirá obtener una comprensión profunda de la amenaza del ransomware BlackCat y evaluar la efectividad de las contramedidas implementadas. Los resultados obtenidos se presentarán en las secciones posteriores, contribuyendo al avance del

conocimiento en ciberseguridad y la mejora de prácticas preventivas y de respuesta ante amenazas similares.

2. Python

Python es un lenguaje de programación, el código fuente escrito por el programador en este lenguaje de alto nivel son traducidas por el intérprete a un lenguaje entendible por la máquina (lenguaje máquina). Este proceso se repite cada vez que se ejecutan las diferentes instrucciones de que consta un programa.(Algar Díaz & Fernández de Sevilla Vellón, 2019)

Python dispone de un intérprete por línea de comandos en el que se pueden introducir sentencias, cada sentencia o instrucción se ejecuta y produce un resultado visible, que ayuda a clarificar la comprensión del código escrito y verifica la validez de los resultados de la ejecución de pequeñas porciones de código de forma inminente. (Torres, 2020)

Este lenguaje soporta el paradigma de programación orientada a objetos y ofrece en muchas ocasiones una manera cómoda para la elaboración de programas con componentes reutilizables.

3. Función os.remove:

Esta función, parte de la biblioteca estándar de Python, se utiliza para eliminar archivos del sistema de archivos. Se proporciona la ruta completa del archivo que se desea eliminar como argumento, y la función se encarga de realizar la eliminación.

```
import os
os.remove("ruta/del/archivo.exe ")
```

Tabla 1 Biblioteca de Python + Sintaxis

c. CAPITULO 3

i. Resultados

La muestra de ransomware BlackCat analizada tiene el siguiente hash SHA256:

Descripción	**HASH SHA256**
BlackCat (Binario PE de Windows V1)	731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161

Tabla 2 hash SHA256

ii. Información del Análisis

Información obtenida mediante el programa Detect It Easy.

1.Tipo de Archivo	PE32, Ejecutable en 32 bits (Figura 3)
2.Tamaño en bytes	2.93 MiB(mebibyte) (Figura 3)
3.Sistema operativo	Windows (95) [I386, 32-bit, GUI] (Figura 3)
4.Punto de entrada	Su punto de entrada es 004014c0 (Figura 3)
5.Arquitectura de la Aplicación	I386, 32-bit (Figura 3)
6.Entorno Gráfico	Graphics User Interface GUI (Figura 3)
7.Fecha y hora del archivo	2021-12-07 17:13:05 (Figura 3)
8.Compilador o compiladores empleados	MinGW (Minimalist GNU for Windows) (Figura 3)
9.Enlazadores	GNU linker Id (GNU Binutils) (2.30) [GUI32] (Figura 3)
10.Gráfico de visualización	Figura 4
11. Hash SHA256	Figura 5
12.Porcentraje de entropía y su grafico	Figura 6
13. Clasificación del Virus Total	Figura 7

Tabla 3 Análisis

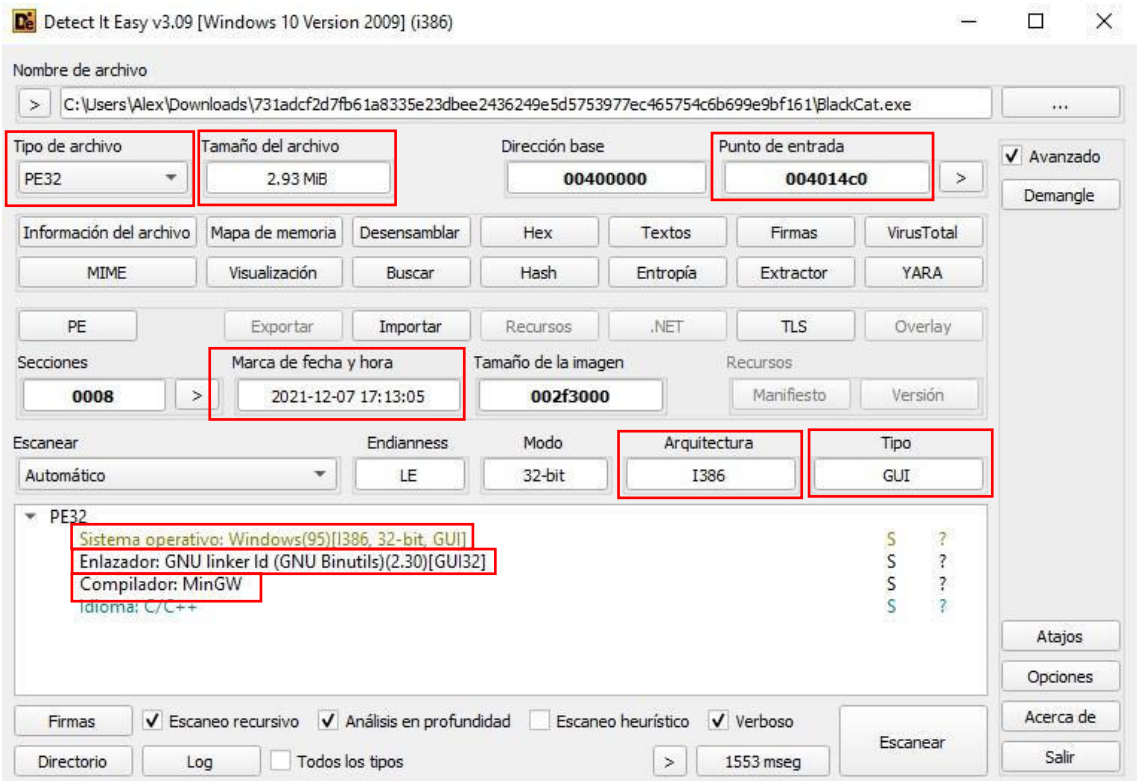


Figura 3 Información del ejecutable

Figura 4 Gráfico de visualización

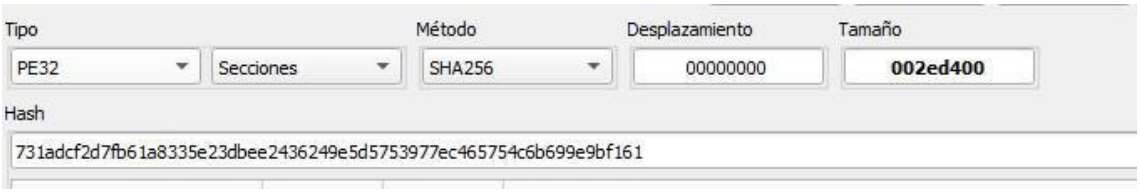


Figura 5 Hash SHA256

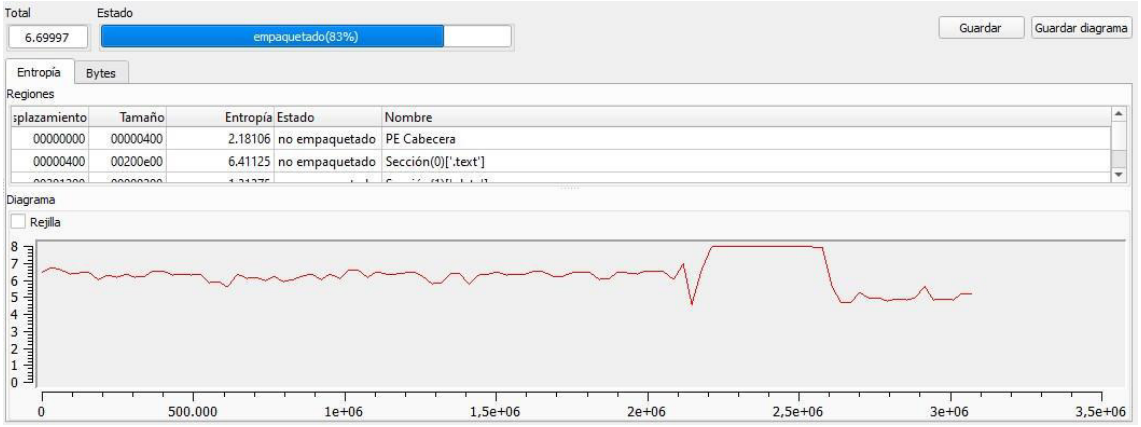


Figura 6 Porcentaje de entropía y su grafico

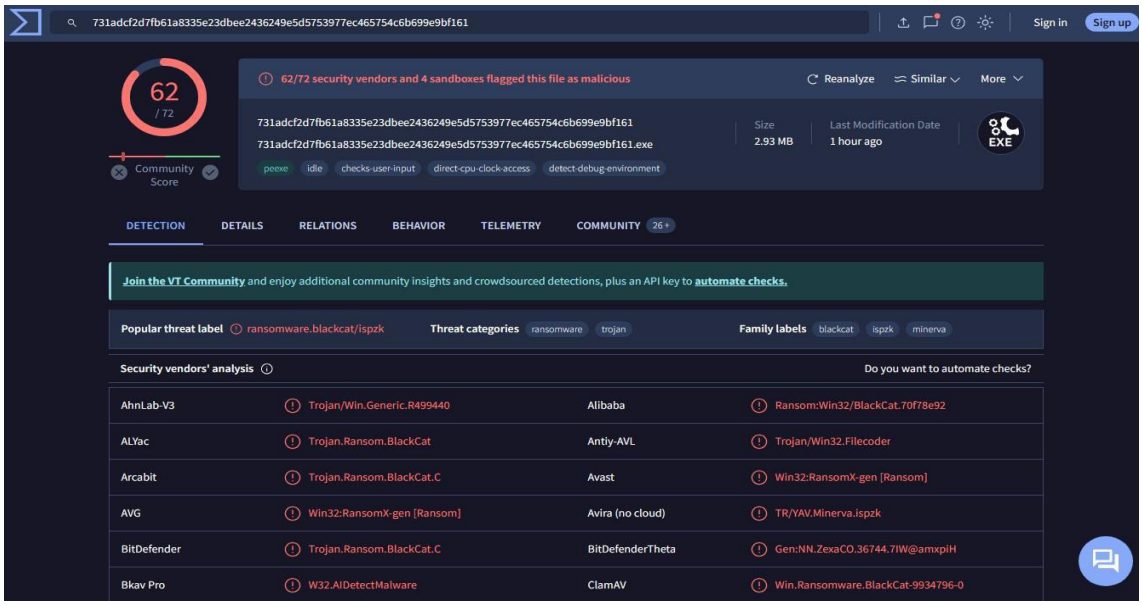


Figura 7 Virus Total

iii. Primera Prueba

Máquina de laboratorio Windows 10 desde cero en la que se procedió a descargar el archivo malicioso.

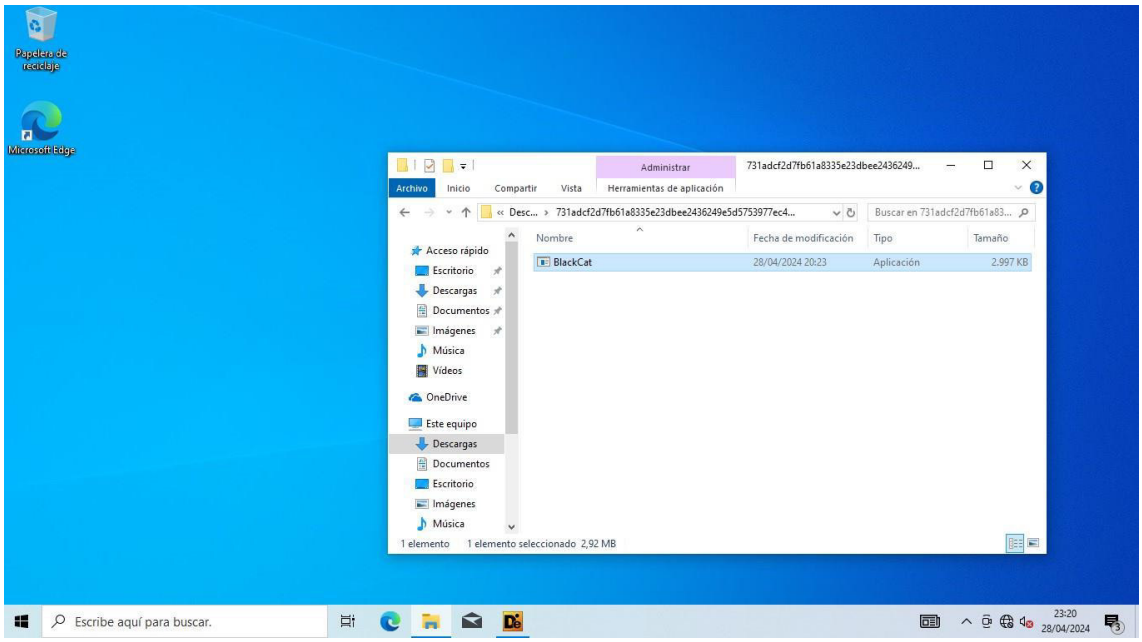


Figura 8 Descarga de ransomware en Windows 10

Se presenta la ruta del archivo, y preparación para ejecución vía Powershell:

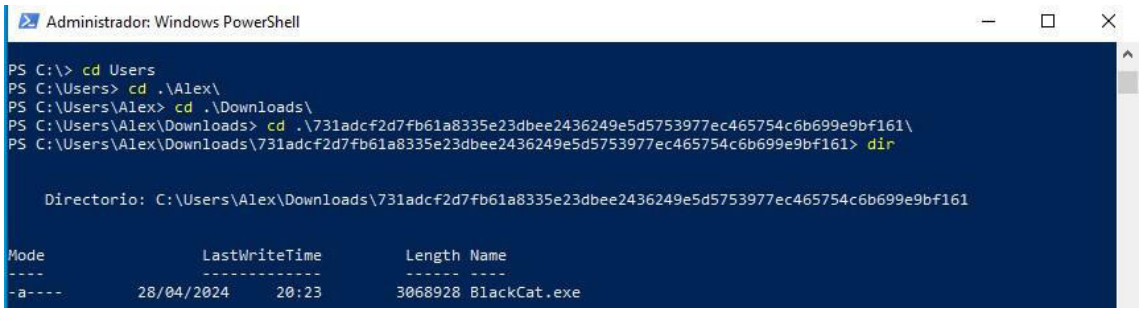


Figura 9 Ruta del Archivo

Adicional se utilizó un extractor de configuración estática “blackcatconf” de github para obtener más información antes de su ejecución:

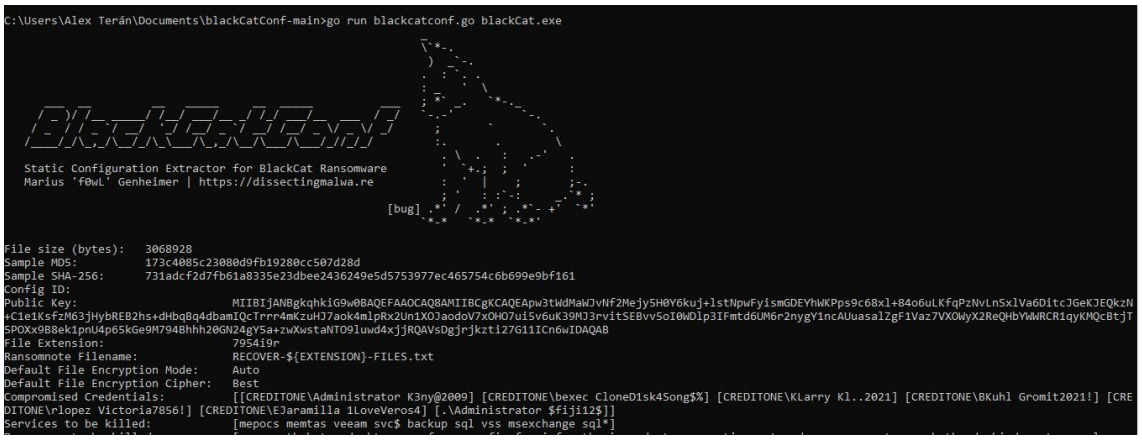


Figura 10 Análisis con extractor blackcatconf

En este caso como datos relevantes se puede evidenciar su hash, la llave pública, la extensión del archivo y el nombre del archivo de la nota de rescate, entre otros.

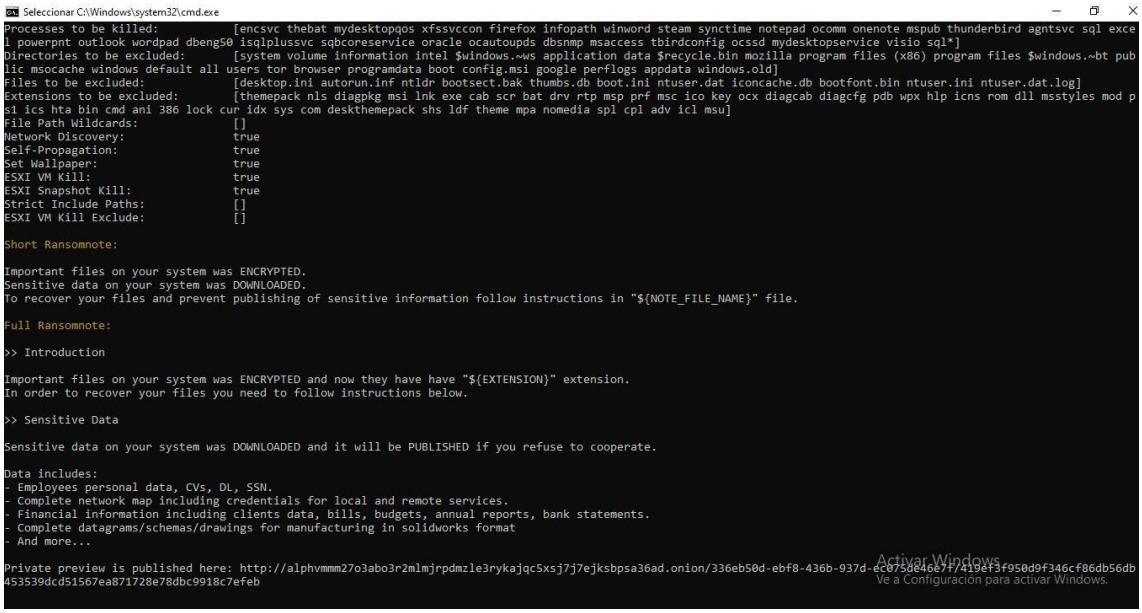


Figura 11 Información extraída

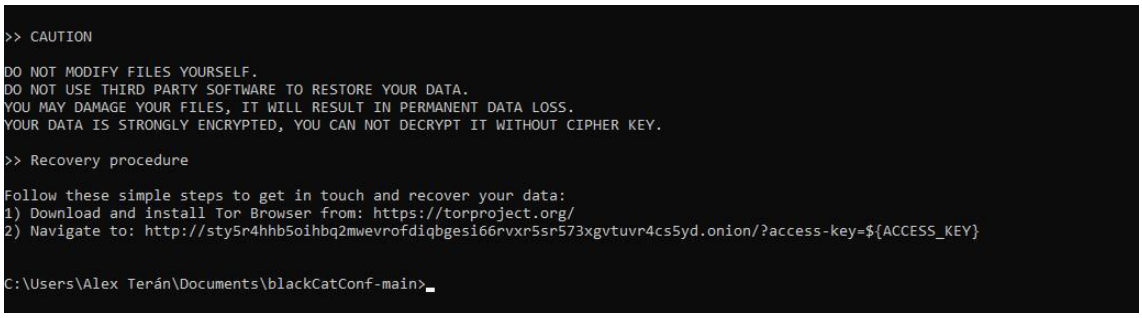


Figura 12 Nota de rescate

El ransomware está programado para ser ejecutado de forma manual y, una vez ejecutado, se comporta como una aplicación de escritorio en formato de consola de comandos que, incluso, muestra información de depuración durante su ejecución, según se ha podido observar en el código fuente:

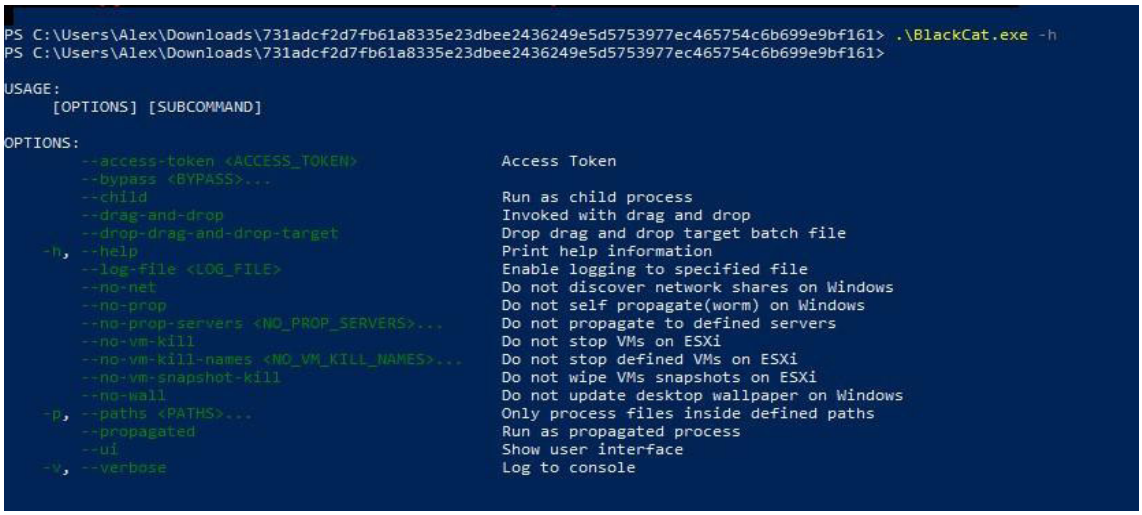


Figura 13 Información de Depuración

Para poder realizar la ejecución de BlackCat es necesario introducir el valor del parámetro:

"—access -token", sin este parámetro el binario no se puede ejecutar.

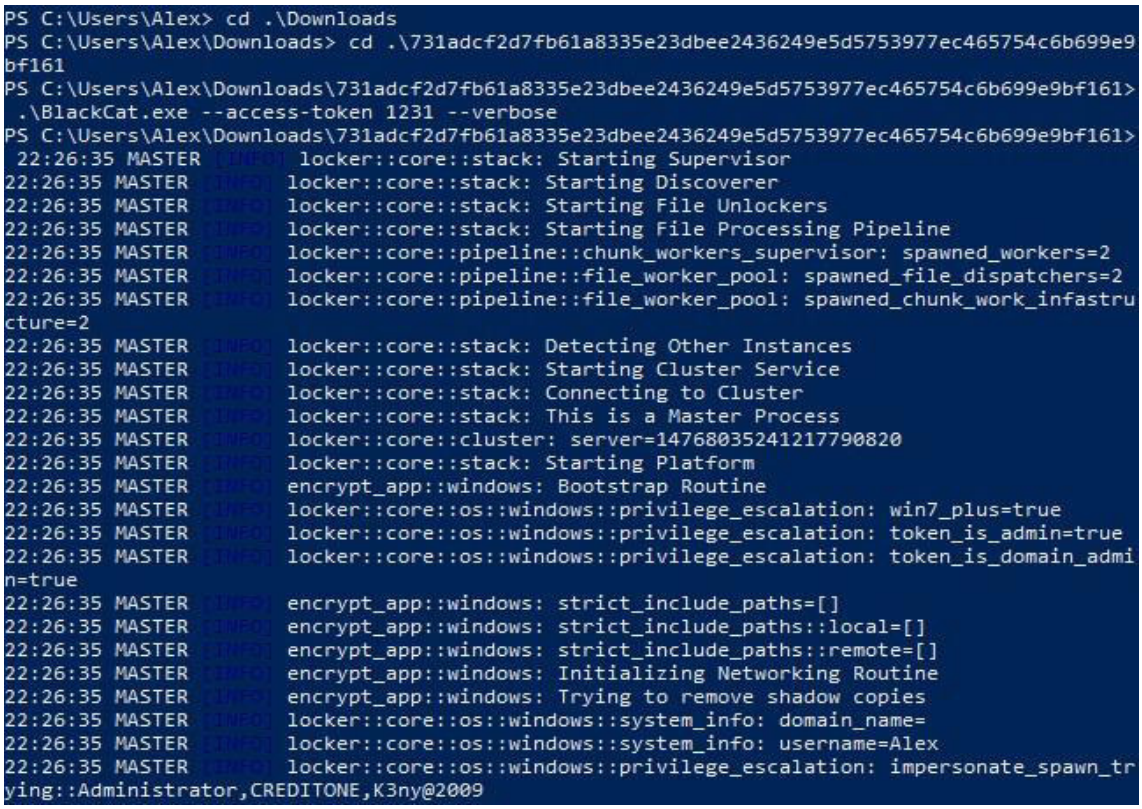


Figura 14 Ejecución por consola

1. **Parámetros “--log-file” o “--verbose”**

Durante las pruebas de ejecución se ha podido comprobar el funcionamiento del sistema encargado de indicar al operador el estado de la ejecución. Para ello se puede hacer uso de los parámetros ***“--log-file”*** o ***“--verbose”***: en el primer caso se mostrará directamente por la consola en el segundo caso se guardará la información en un fichero de texto.

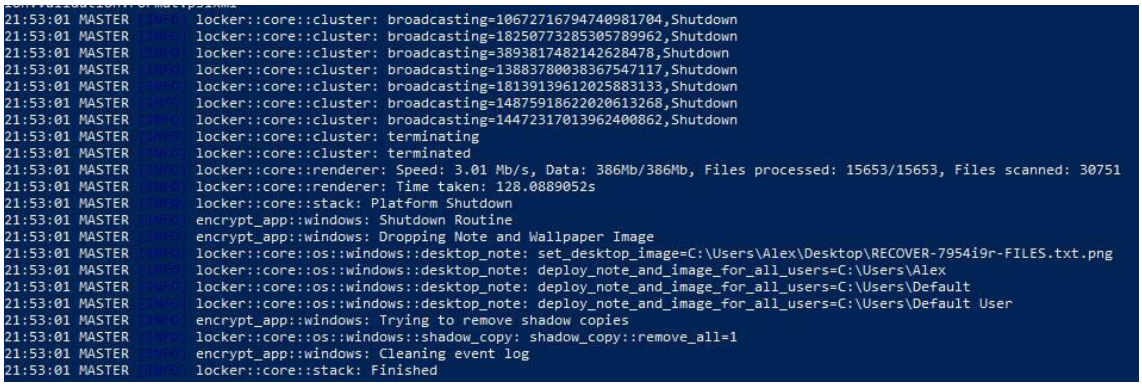


Figura 15 Procesos finalizados

Podemos observar los procesos finalizados donde nos indica el cambio de fondo de pantalla y la creación de un archivo de texto donde se almacena los pasos a seguir después de la ejecución del ransomware.

También guardamos todo en un archivo.log con el comando ***–log-file*** para observar la información recogida luego de la ejecución:

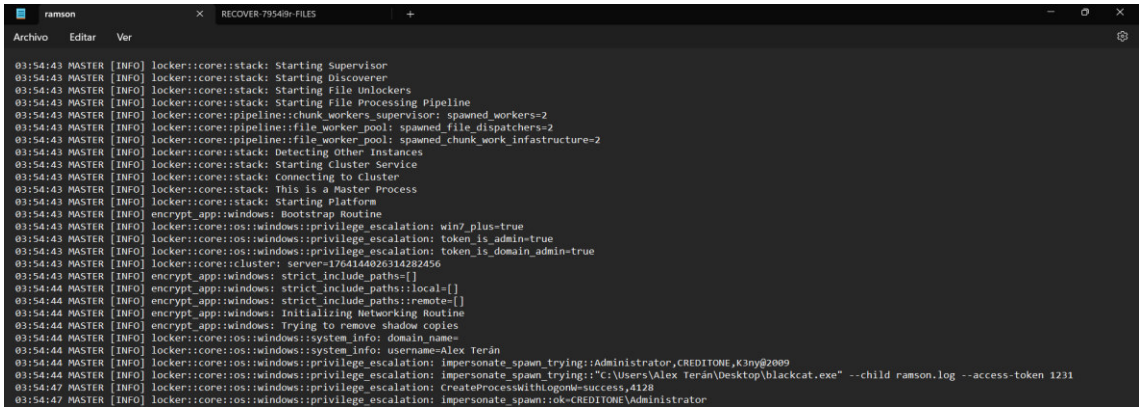


Figura 16 Ejecución por log

Una vez finalizado observamos que queda comprometido el equipo y sus archivos, el tiempo de ejecución y posterior el mensaje en pantalla fue de 5-10 minutos en múltiples ejecuciones

realizadas, tomando en cuenta que el sistema operativo no cuenta con varios archivos, más que principalmente que vienen por defecto:

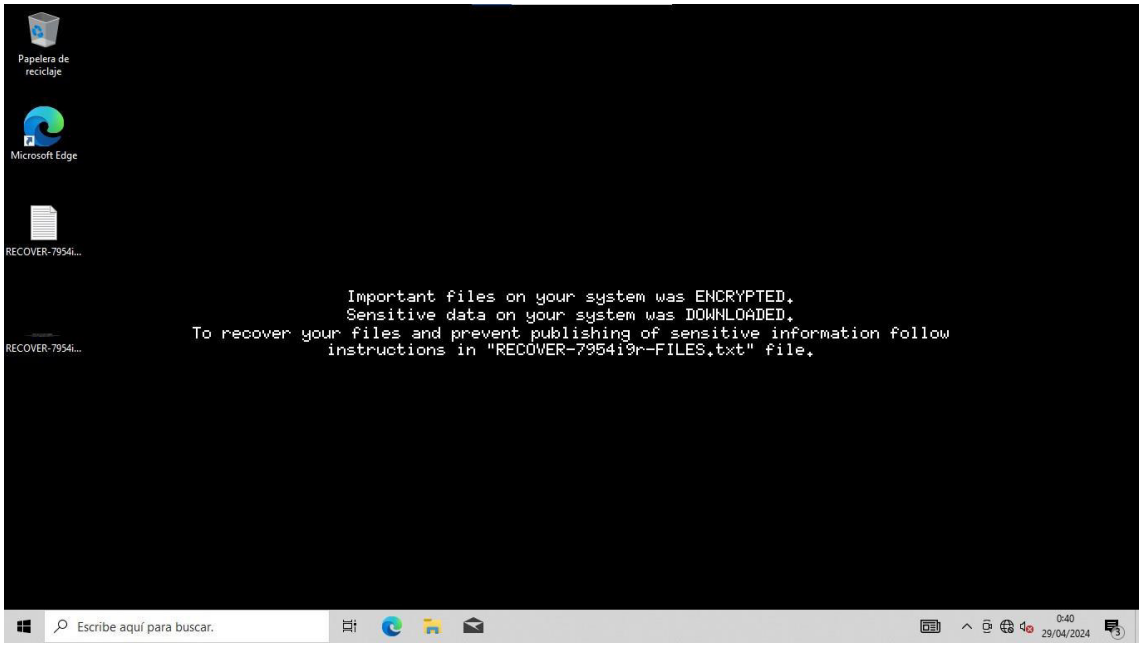


Figura 17 Inicio comprometido

Documentos encriptados con extensión .7954I9R

Screenshots	28/04/2024 23:50	Carpeta de archivos	
731adcf2d7fb61a8335e23dbee2436249e5...	28/04/2024 23:50	Archivo 7954I9R	1.611 KB
blackCatConf-main.zip.7954i9r	28/04/2024 23:50	Archivo 7954I9R	147 KB
checkpoints-die_win32_portable_3.09_x8...	28/04/2024 23:50	Archivo 7954I9R	1 KB
die_win32_portable_3.09_x86.zip.7954i9r	02/04/2024 15:03	Archivo 7954I9R	18.101 KB
ProcessMonitor.zip.7954i9r	28/04/2024 23:50	Archivo 7954I9R	3.380 KB
RECOVER-7954i9r-FILES	28/04/2024 23:50	Documento de te...	2 KB

Figura 18 Archivos encriptados

Creación de una partición donde se almacena la nota de rescate

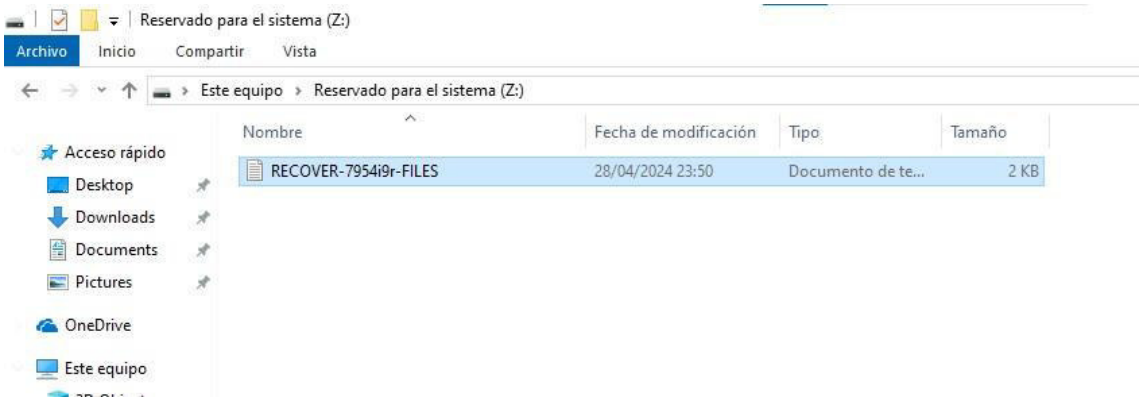


Figura 19 Creación de partición en el sistema

Por otro lado, la nota de rescate escrita en cada uno de los directorios por donde el proceso de cifrado ha pasado, es la siguiente:

>> Introduction

Important files on your system was ENCRYPTED and now they have have "7954i9r" extension.

In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate.

Data includes:

- Employees personal data, CVs, DL, SSN.

- Complete network map including credentials for local and remote services.

- Financial information including clients data, bills, budgets, annual reports, bank statements.

- Complete datagrams/schemas/drawings for manufacturing in solid works format

- And more...

Private preview is published here:
http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/336eb50d-ebf8-436b-937d-ec075de46e7f/419ef3f950d9f346cf86db56db453539dcd51567ea871728e78dbc9918c7efeb

>> CAUTION

DO NOT MODIFY FILES YOURSELF.

DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.

YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

>> Recovery procedure

Follow these simple steps to get in touch and recover your data:

1) Download and install Tor Browser from: https://torproject.org/

2)Navigate to: http://sty5r4hhb5oihbq2mwevrofdiqbgesi66rvxr5sr573xgvtuvr4cs5yd.onion/?access-key=GCTOsFhMMlTRq921Dkb8tDO0rbWeLm%2Fb%2Fd%2FlQEfEgHG7fxpSD%2Bu6%2BHgGAE%2Bt5b0XUYZdG%2FSM8oJcC9P1PnYohkWb5vn45w6%2FIQ7BMS5nXP%2FBPhLbAgrCaTcepgxdFwOahFTMEBszgBVcSdNaX9ovk1YVbYKdIY2%2B5LmUPCEpW%2Bw0JM2jlxPGoW8xiU3wxX5TKg7czMDPY5xCI6MiWdpdt0x8t1xF9CNZQZoiXeSutbTSx6xY9raNBRHjx6cVTkQgh7DJYVU7k5OG0dGgws8lCwsqCjKRuqd3Ro6ObaDKcjX0eZwABfxbbSCSuKwgn81X%2BqGe1Ph%2Bj2hRG0tIRNLq%2Bg%3D%3D

Tabla 4 Nota de Rescate

Adicional, en una máquina virtual Linux con la herramienta para capturar el tráfico de red (Wireshark) en la misma red observamos a que IP o URL realiza la conexión al momento de su ejecución.

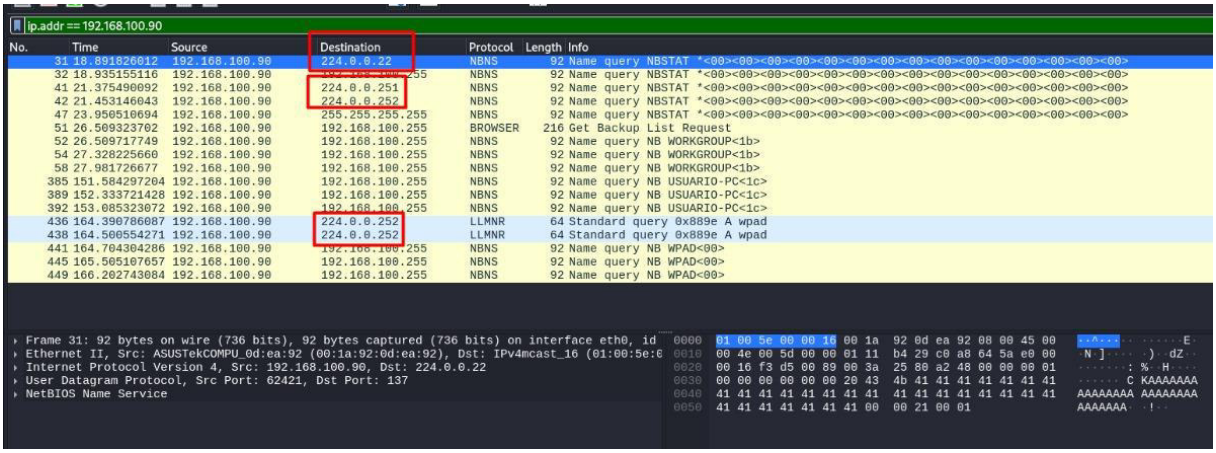


Figura 20 Análisis de tráfico de red

Se puede observar las siguientes IP's y protocolos a nivel de Wireshark:

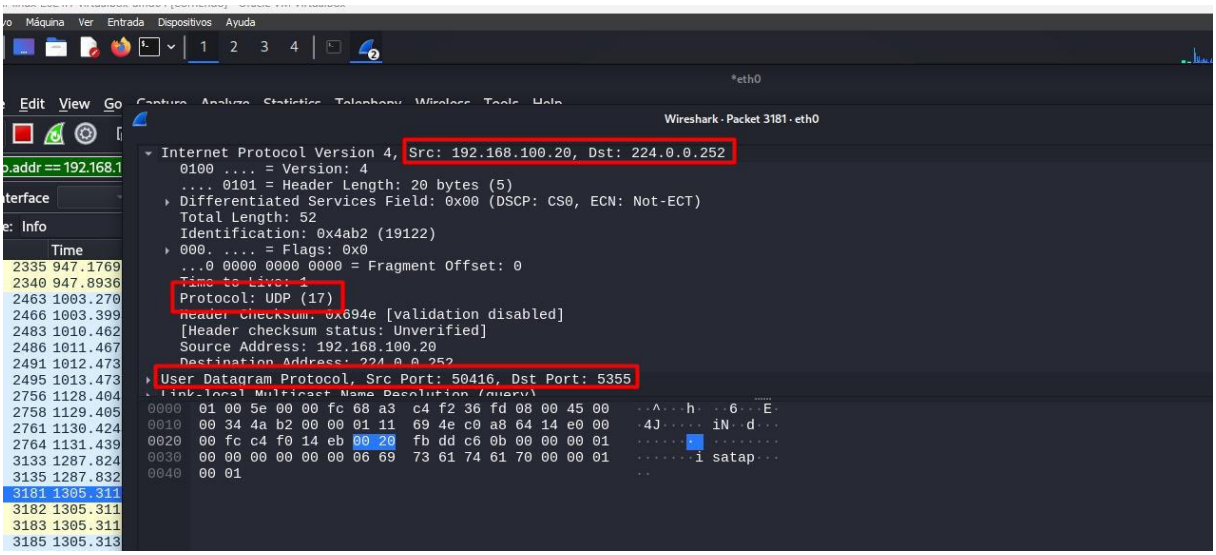


Figura 21 Protocolos y puertos

Basándonos en las direcciones IP y sus respectivos protocolos asociados observados durante el análisis del ransomware, podemos llegar a las siguientes conclusiones:

La dirección IP 224.0.0.22 utiliza el protocolo IGMP, indicando un intento potencial del ransomware de propagarse a través de la red mediante la suscripción a grupos de multidifusión.

Las direcciones IP 224.0.0.251 y 224.0.0.252 utilizan el protocolo LLMNR, lo que sugiere que el ransomware también podría intentar propagarse utilizando el servicio de resolución de nombres de multidifusión local de enlace.

En resumen, el análisis revela que el ransomware está intentando difundirse o propagarse a través de la red aprovechando los protocolos IGMP y LLMNR. Esta observación subraya la importancia de implementar medidas de seguridad robustas para prevenir la propagación del ransomware dentro de la red y mitigar sus efectos adversos.

iv. Análisis dinámico en la herramienta Open Source x32dbg

Para este análisis se ha utilizado la herramienta de código abierto X32dbg, la cual, es un depurador de aplicaciones y programas usado comúnmente para prácticas de reversing.

Iniciamos verificando las cadenas de texto que aparecen en la ejecución del ransomware.

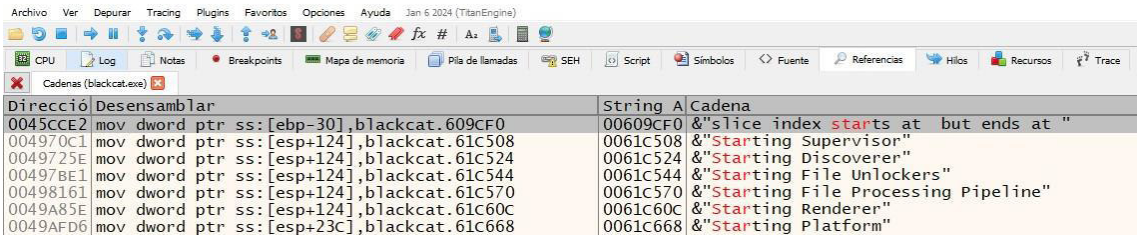


Figura 22 Cadenas de textos mostrados por BlackCat en su arranque.

Posteriormente se observa las funciones *"Killing Processes"* y *"Kill all"*, los cuales mata los procesos en ejecución del sistema.

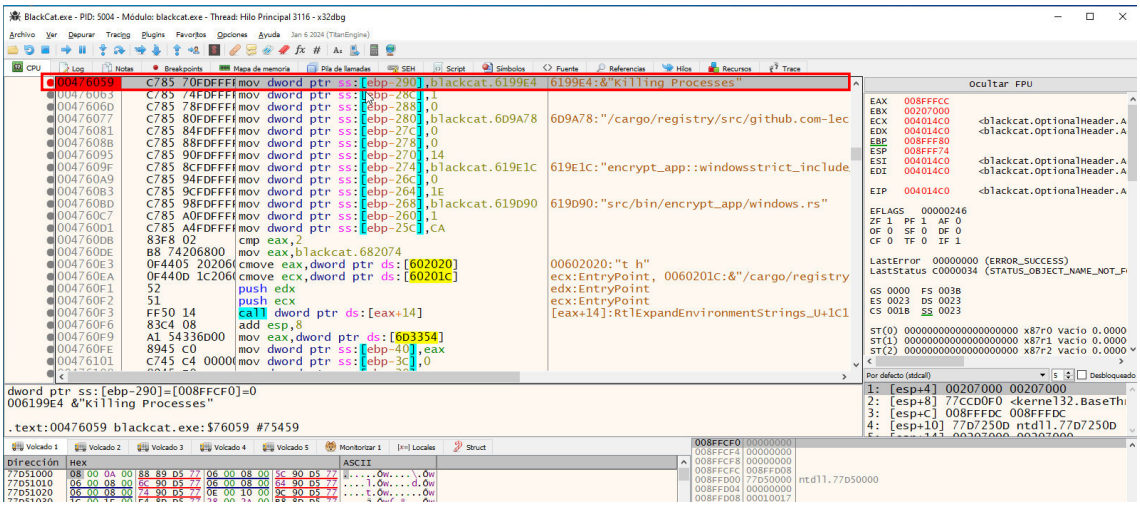


Figura 23 Función con la cadena de texto "Killing Processes".

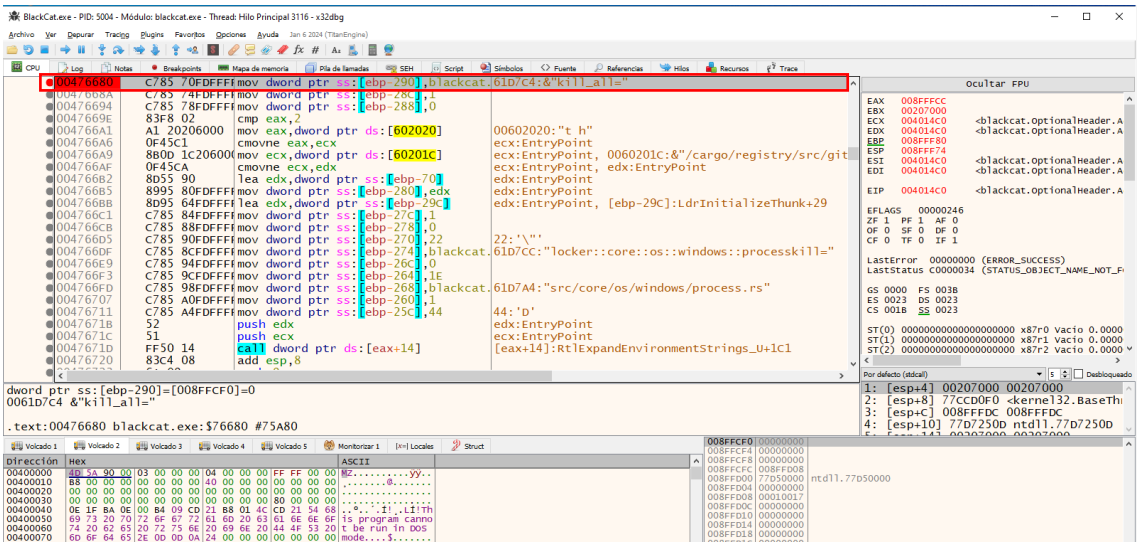


Figura 24 Función con la cadena de texto “Kill_all”.

Continuando, se puede apreciar en el código fuente, varias funciones con las cadenas de texto que hacen referencia al comando que elimina las copias de seguridad del sistema.

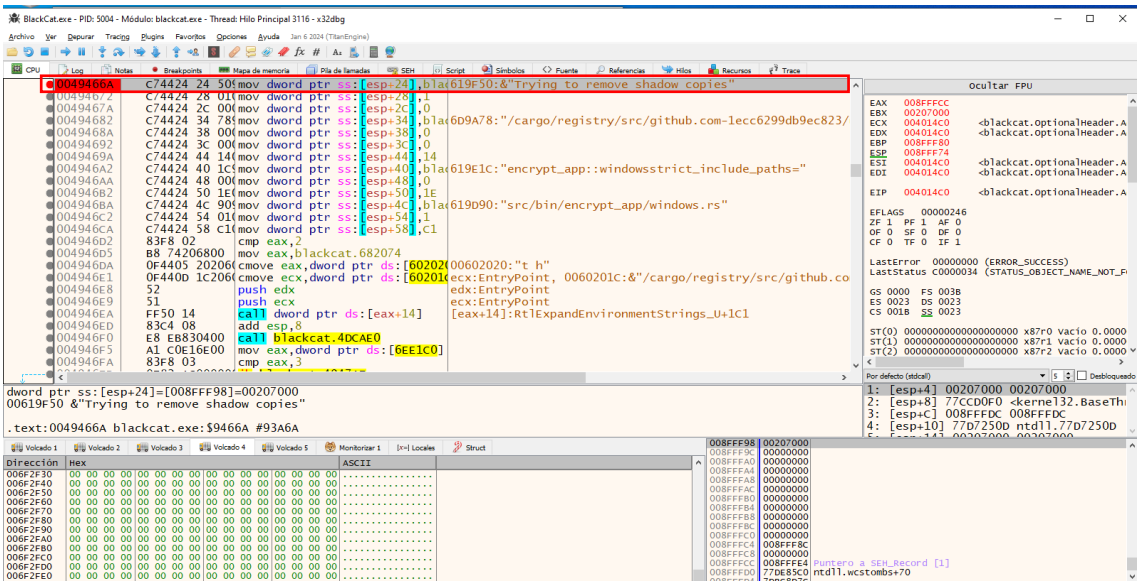


Figura 25 Función con la cadena de texto “Tryining to remove shadow copies”

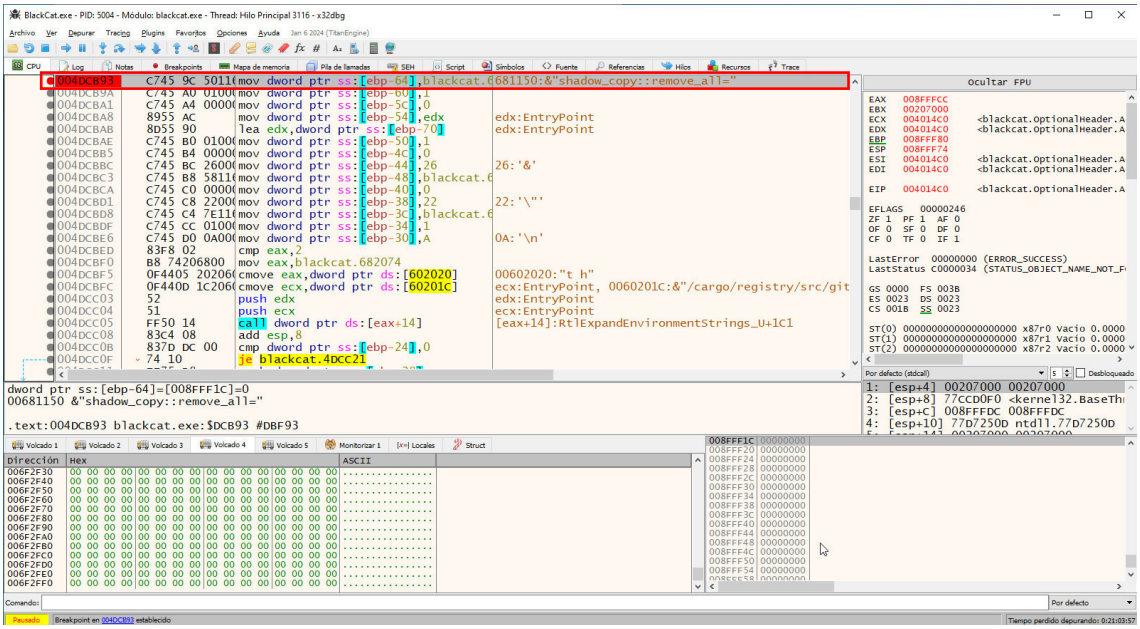


Figura 26 Función con la cadena de texto “shadow_copy::remove_all”.

Para finalmente eliminar las instantáneas de un volumen especifico.

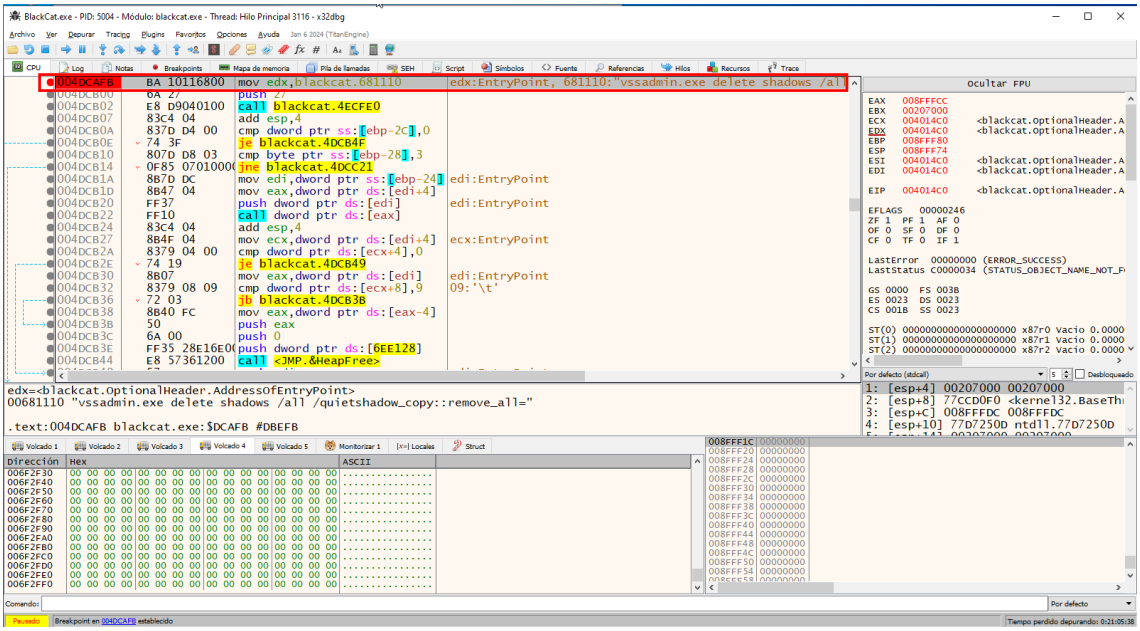


Figura 27 Función con la cadena de texto “delete_shadows /all”.

También se pudo apreciar la función que coloca la nota de rescate con el texto *"NOTE_FILE_NAME"*

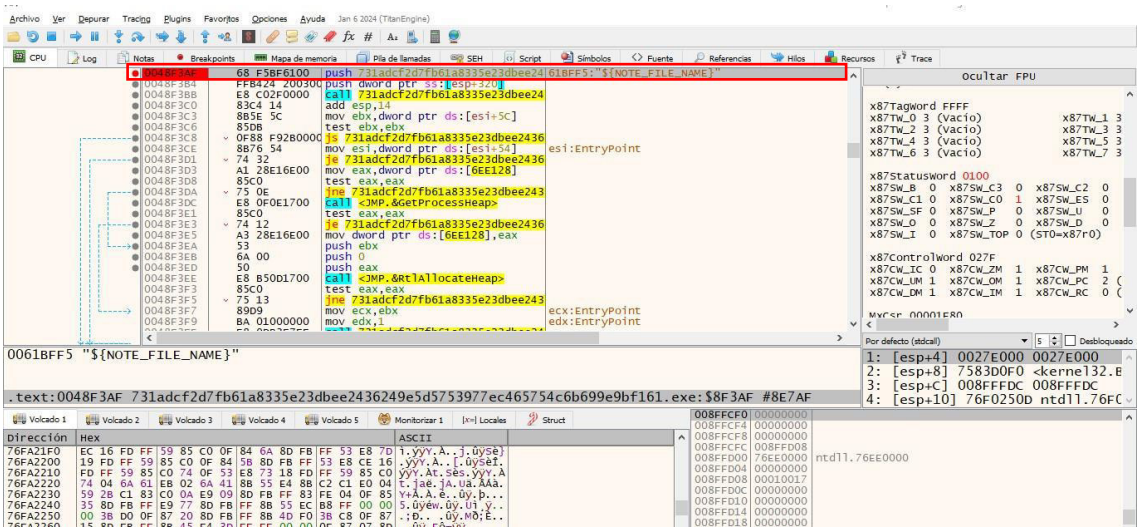


Figura 28 Función que coloca la nota de texto "NOTE_FILE_NAME".

El mensaje que contiene la nota de texto *"NOTE_FILE_NAME"*

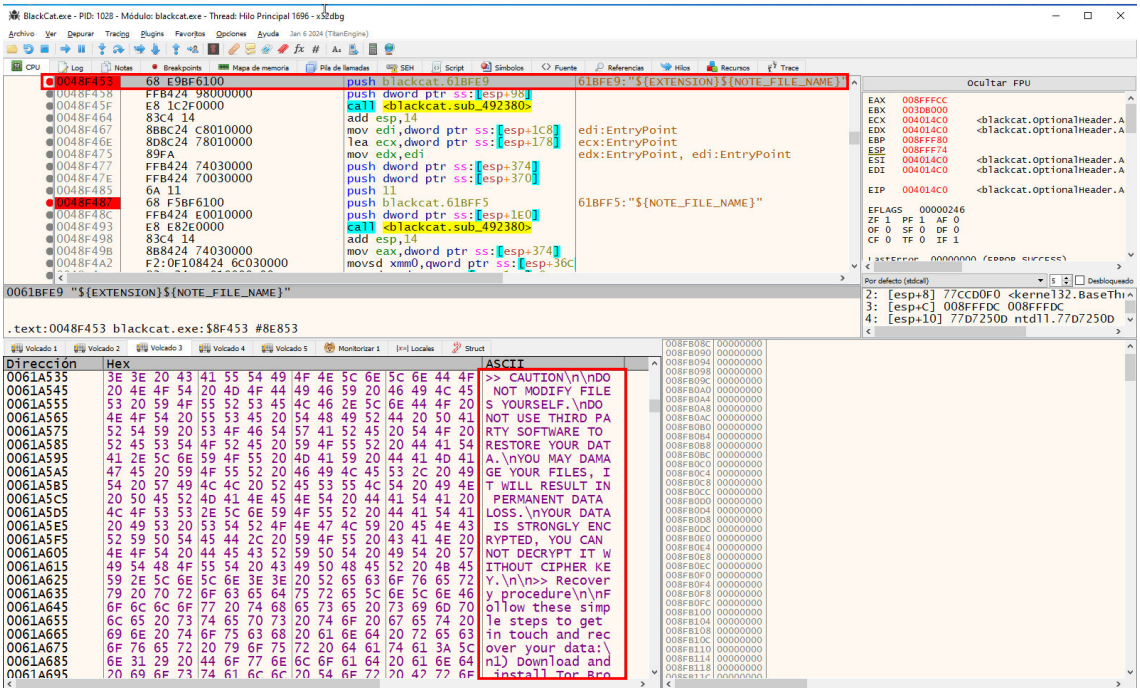


Figura 29 Mensaje de la nota de texto "NOTE_FILE_NAME".

Y el mensaje de rescate cifrado en el ransomware:

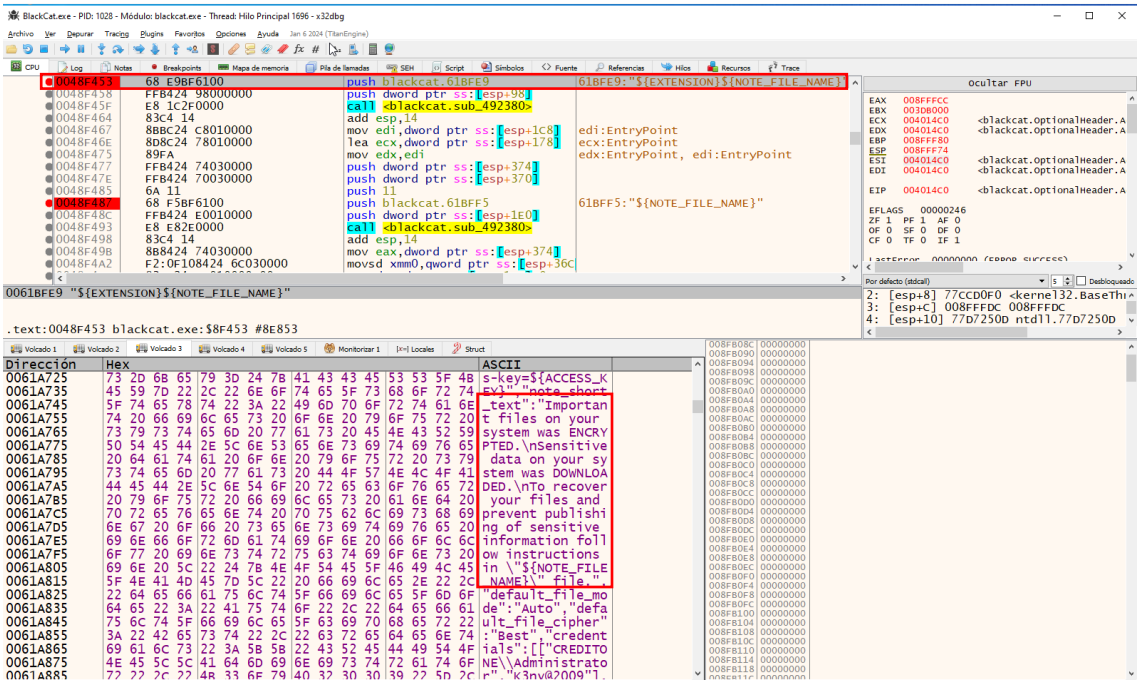


Figura 30 Mensaje de rescate cifrado en el ransomware

Finalmente, aparece la función con la que el ransomware cambia el fondo de pantalla y coloca la nota de rescate.

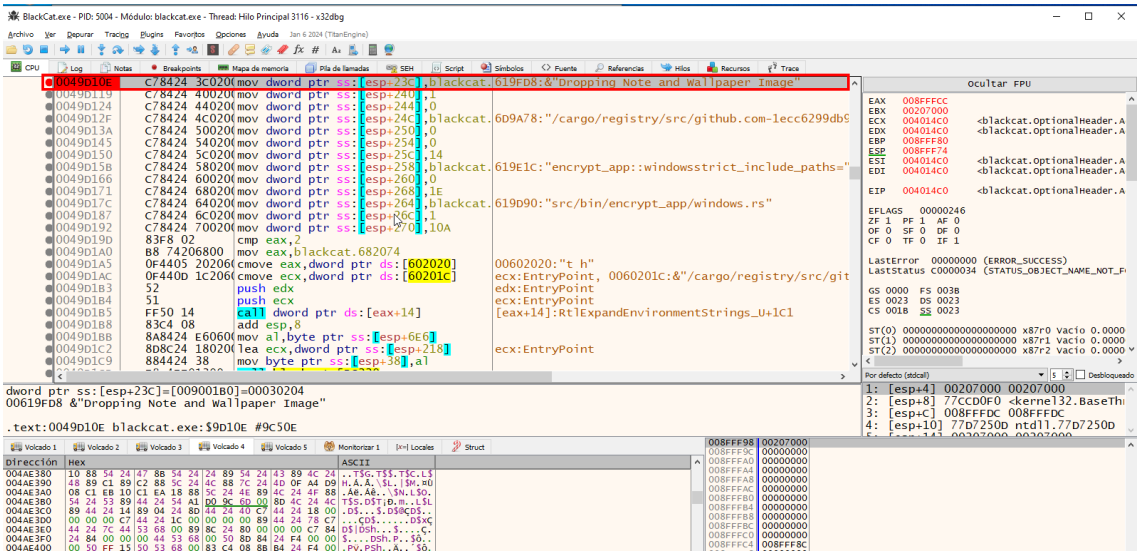


Figura 31 Función que coloca la nota de texto y cambia el fondo de pantalla.

Mensajes juntos:

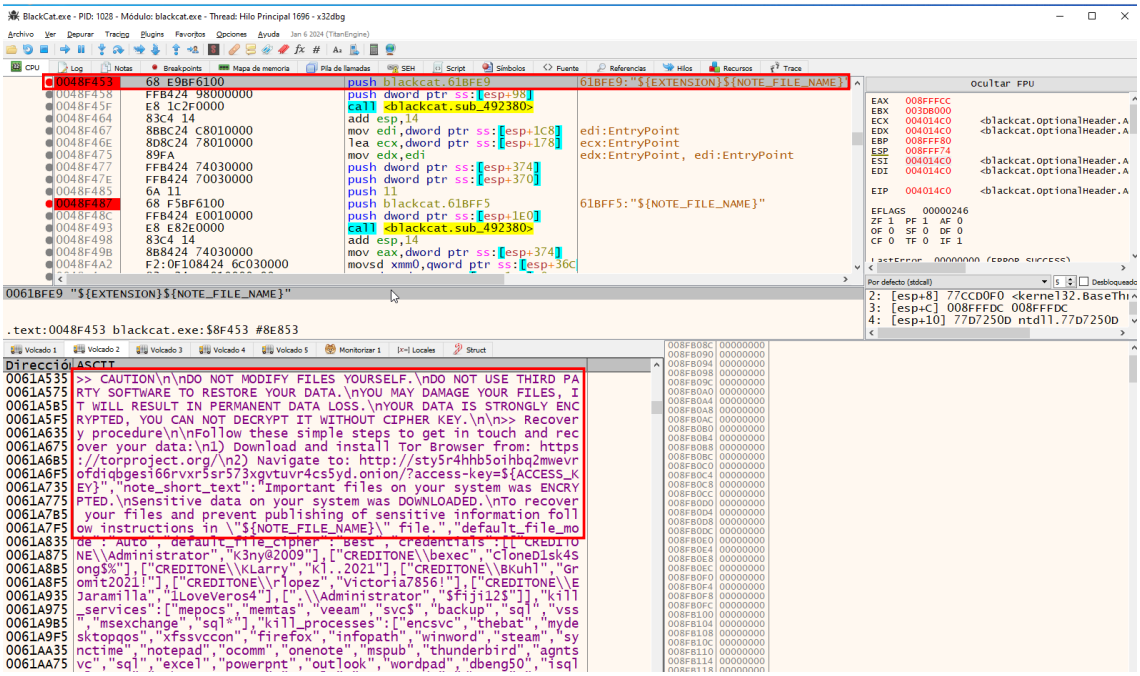


Figura 32 Mensaje final

v. Segunda Prueba

En este caso se realizó pruebas de la muestra en ambientes como una máquina Windows 7:

Como primer dato la máquina Windows 7 contaba con varios archivos en su disco duro.

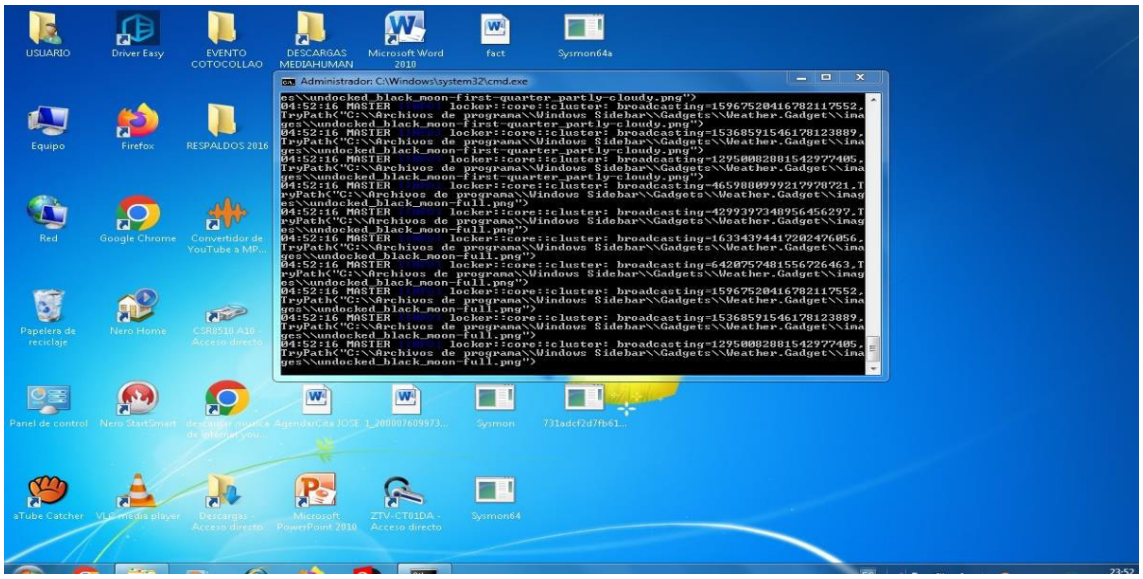


Figura 33 Máquina Windows 7

Y como se evidencia en esta ejecución de la máquina Windows 7 al contar con tantos archivos, tarda mucho más en encriptar cada uno. En este caso tardó alrededor de 1 hora.

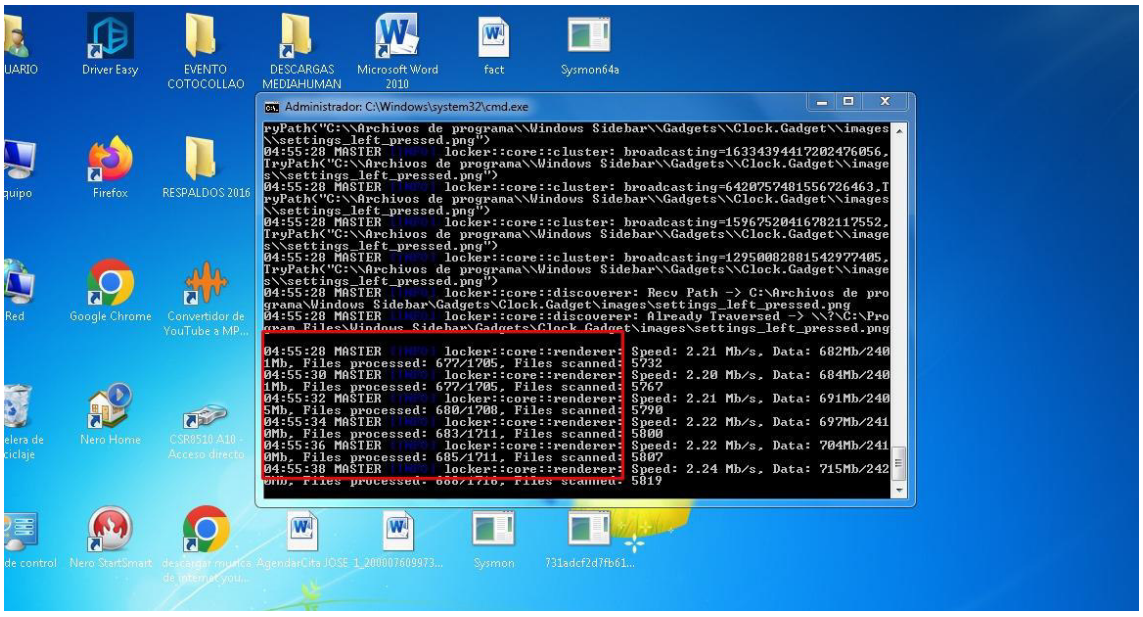


Figura 34 Ejecución de la muestra

vi. IMPLEMENTACIÓN DE LA TECNOLOGÍA SIEM (WAZUH):

Como se mencionó anteriormente se utilizará el SIEM – Wazuh ya que se trata de una plataforma open source. Desde el cual desplegaremos en el ambiente de pruebas, para montar el servidor/máquina virtual desde el que se generará la consola de administración y gestión.

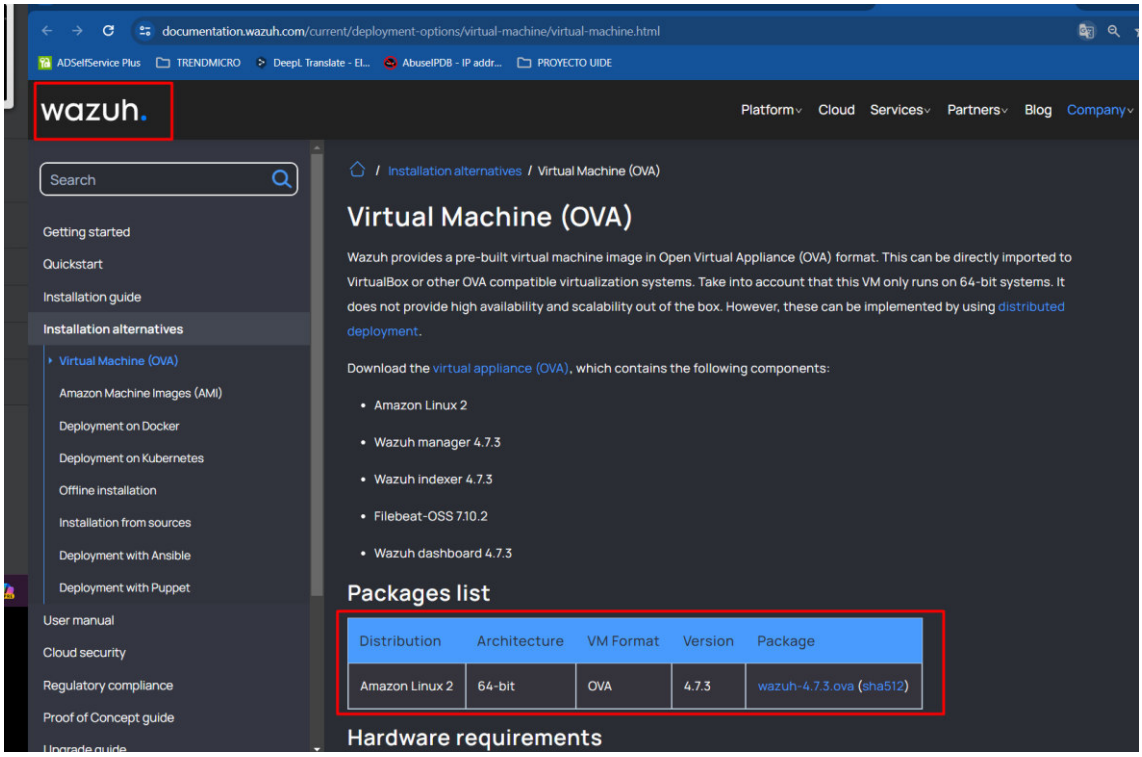


Figura 35 Requisitos para el servidor SIEM

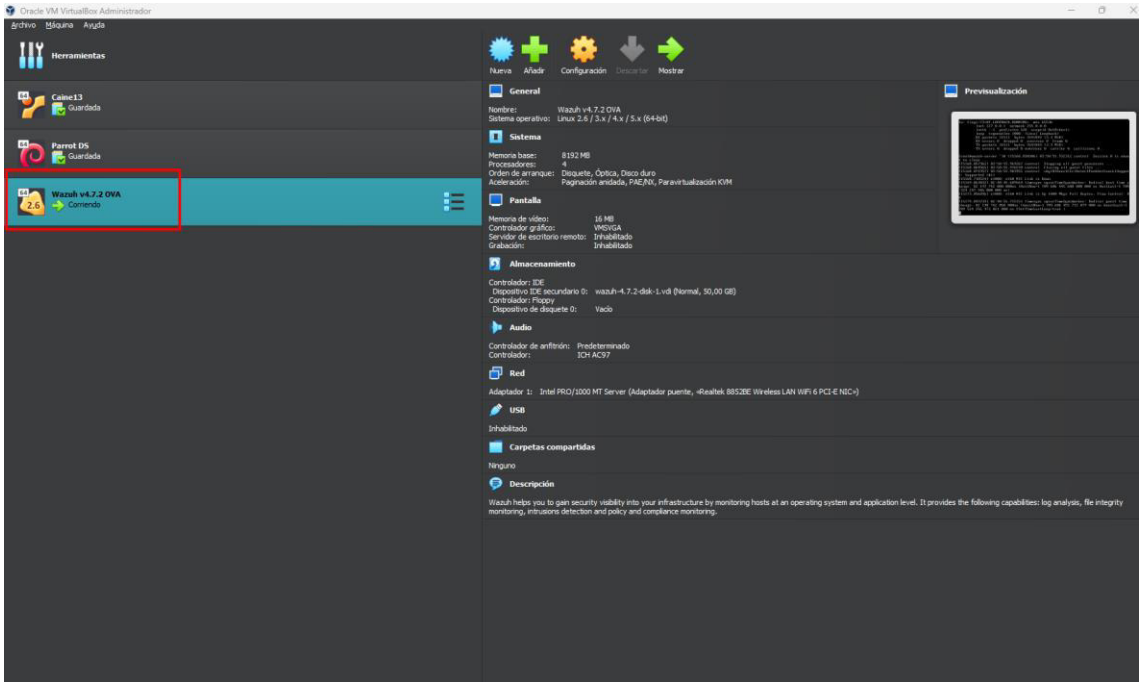


Figura 36 Máquina Virtual para despliegue

Luego de montar el archivo .ova en nuestro ambiente gracias a VirtualBox, procedemos a evidenciar con que IP podremos acceder a la consola:

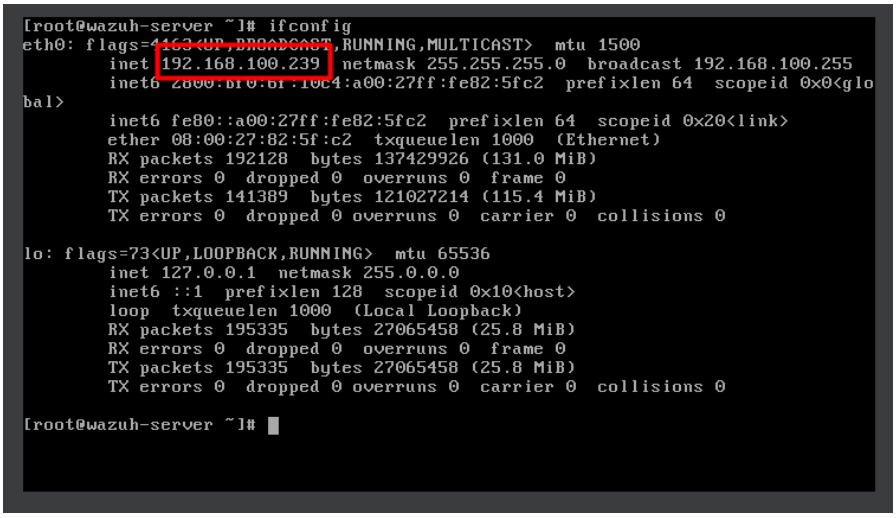


Figura 37 Servidor desplegado - IP de su interfaz

En el navegador, ya podremos evidenciar el login para acceder a la consola:

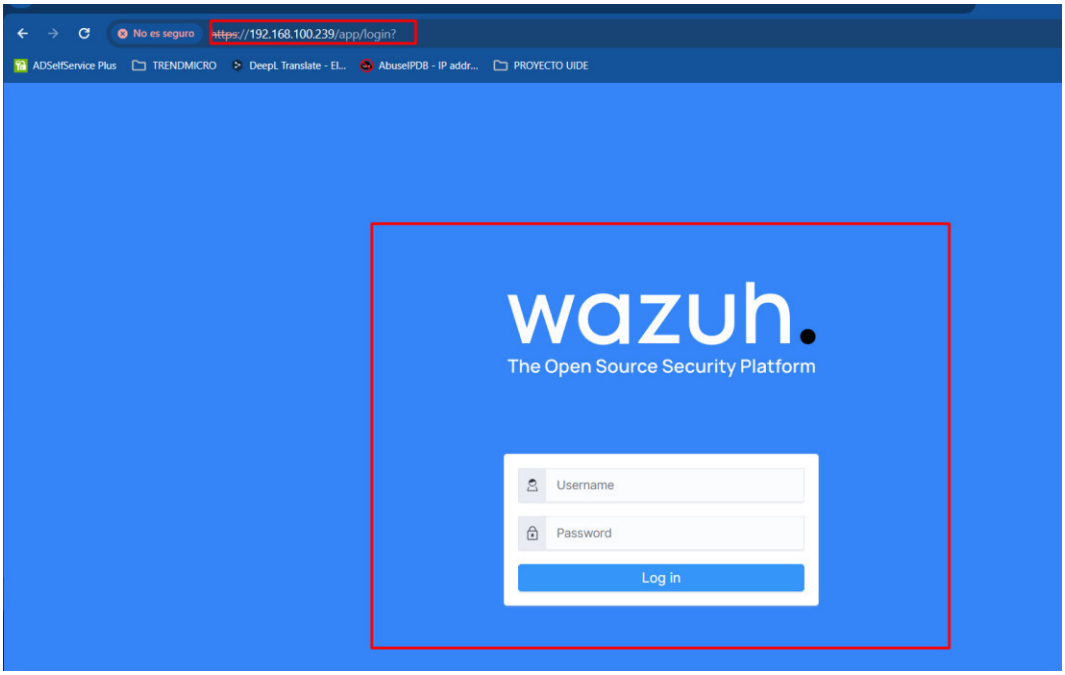


Figura 38 Consola Web Wazuh - Login

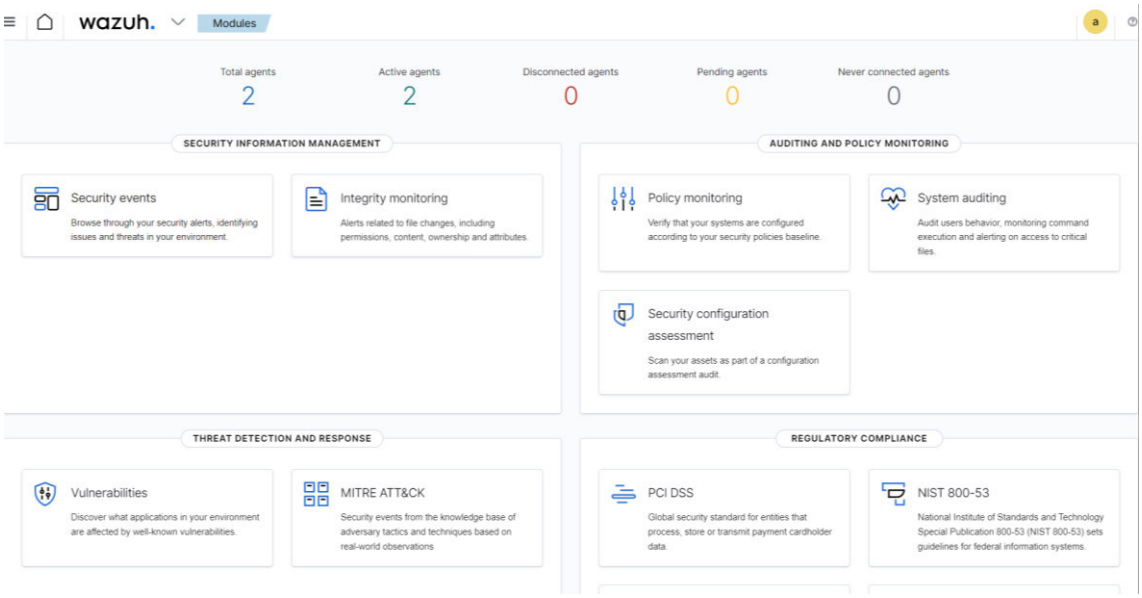


Figura 39 Dashboard - Página Principal de Wazuh

Posterior al logeo lo siguiente es instalar el agente de Wazuh en nuestros equipos de prueba, para ello podemos igualmente descargarlo de la página oficial:

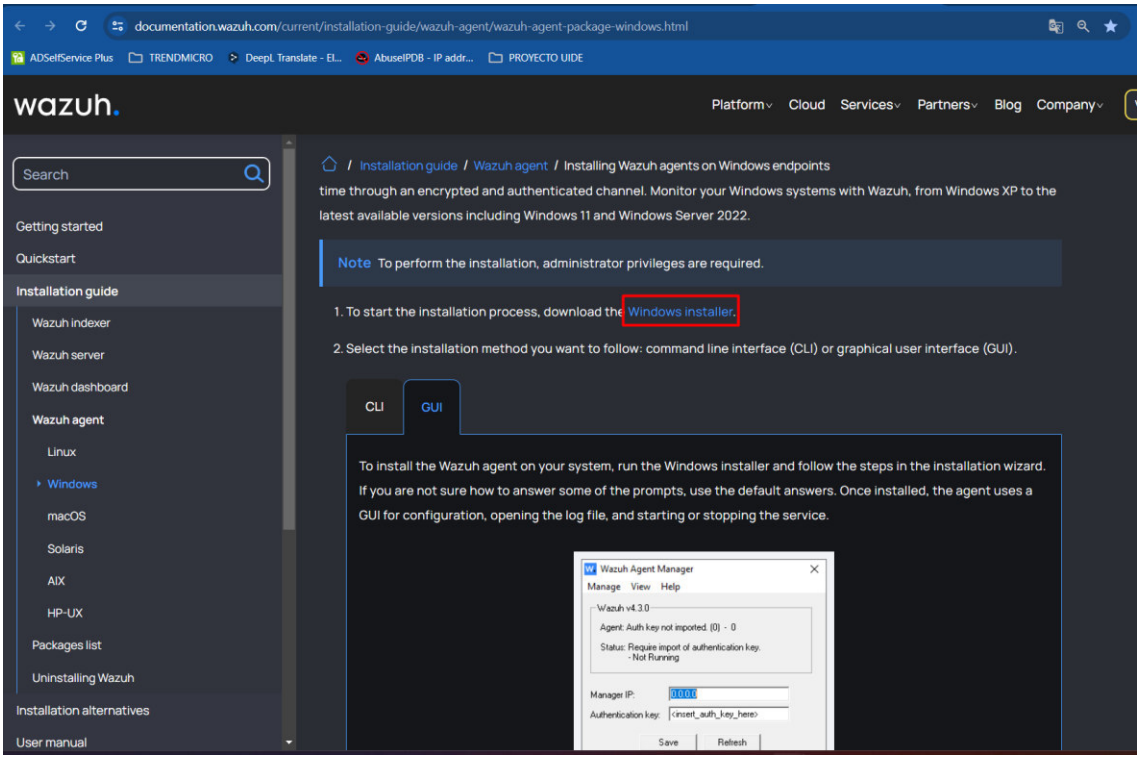


Figura 40 Descarga para instalación de los agentes

En estos endpoints luego de su instalación por defecto, se debe colocar la IP del servidor en cuestión y se nos mostrará dentro de la consola:

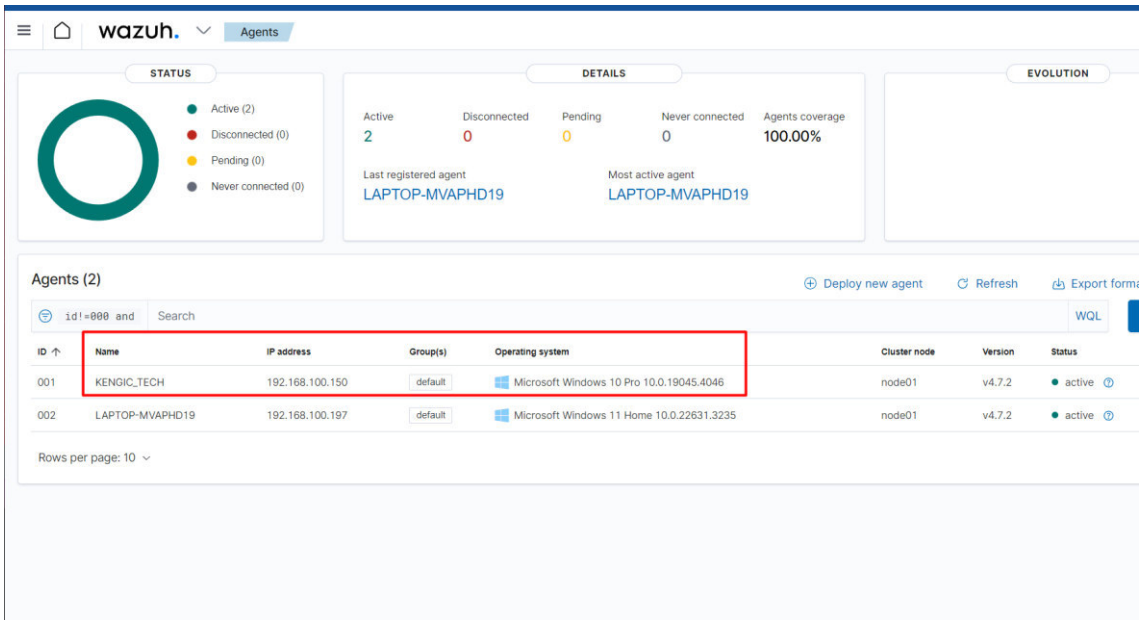


Figura 41 Endpoints con Agente Wazuh en Consola

Luego de esto, ya podremos ver en consola a nuestro equipo además de varios parámetros importantes del mismo como su hostname, IP, sistema operativo, entre otros.

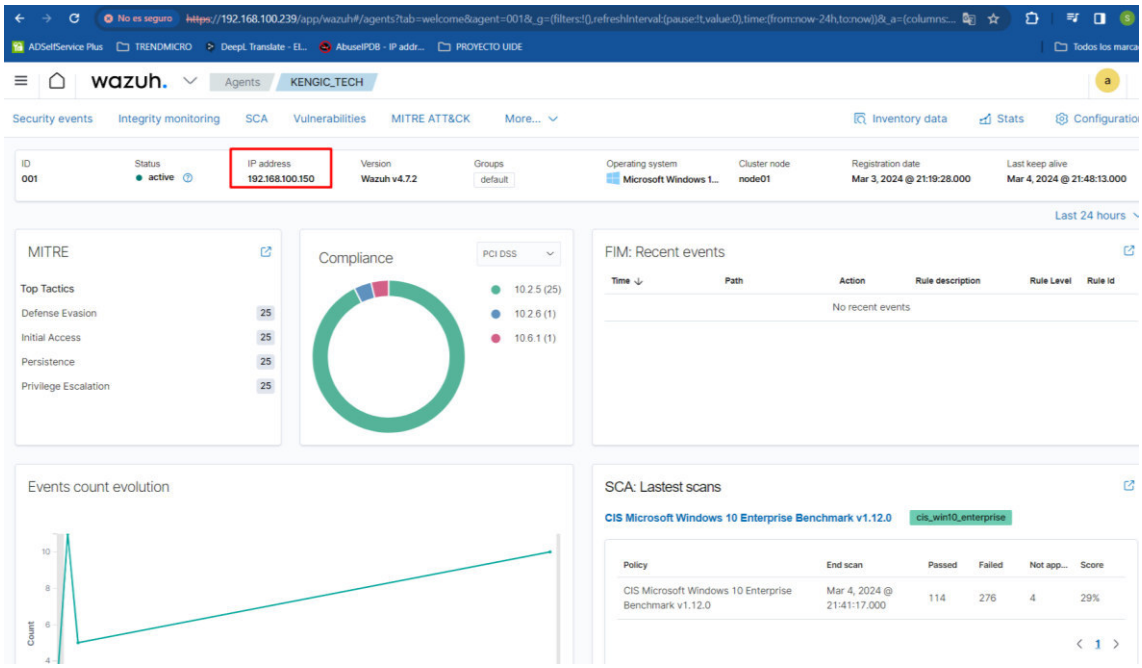


Figura 42 Características del Endpoint

vii. Tercera prueba

Configuración de Wazuh para detección de comportamiento del Ransomware Blackcat, posteriormente en una máquina con sistema operativo Windows 8, se planteó realizar la ejecución del ransomware, pero ya con la implementación del Agente SIEM Wazuh:

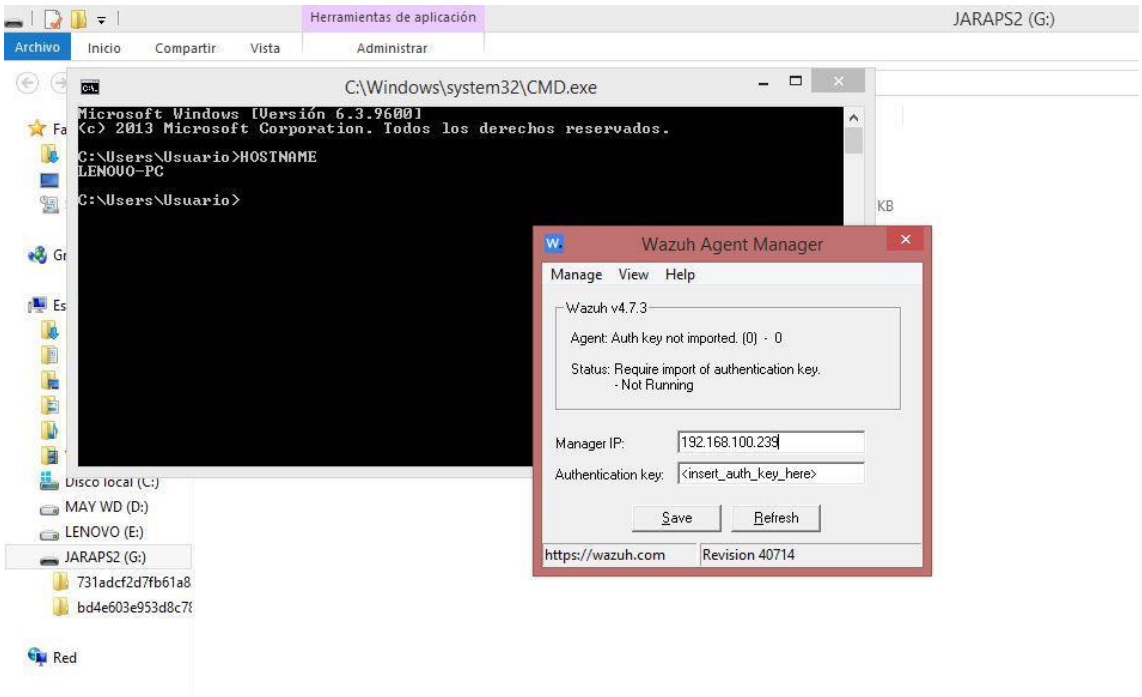


Figura 43 Máquina Windows 8 con Agente Wazuh instalado

Como objetivo de comenzar a realizar configuraciones a nivel de Wazuh e evidenciar los eventos de seguridad, se instaló la herramienta Sysmon de Windows, correspondiente a System Activity Monitor:

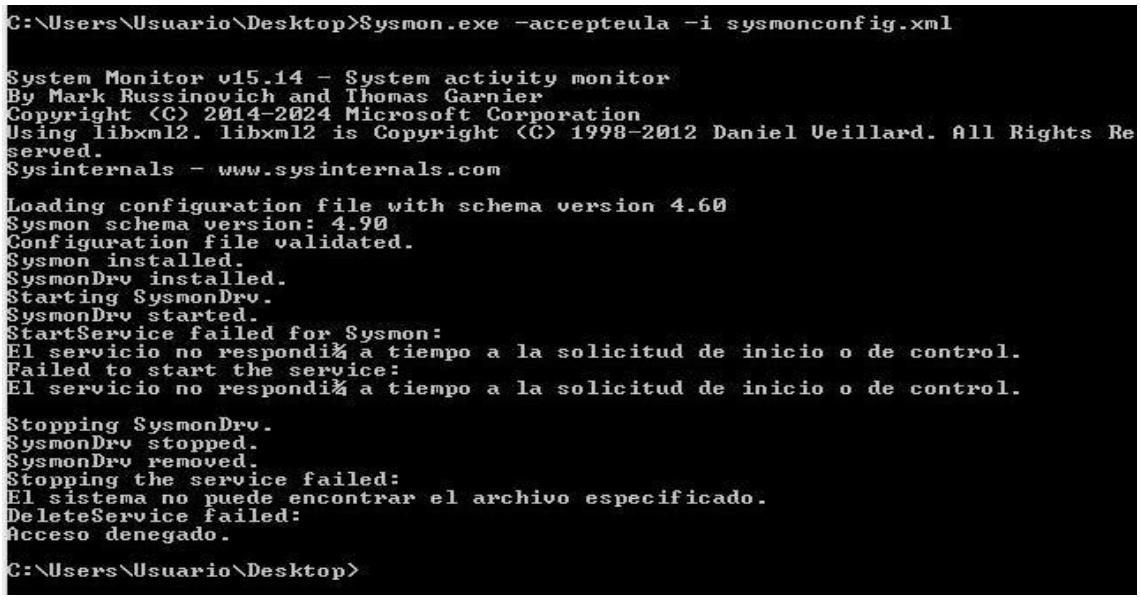


Figura 44 Instalación de Sysmon

Despues procedemos a configurar de tal manera que el agente de Wazuh reciba y envíe los eventos referentes al System Activity Monitor de la máquina. Esto se logra editando el archivo .conf del agente ossec:

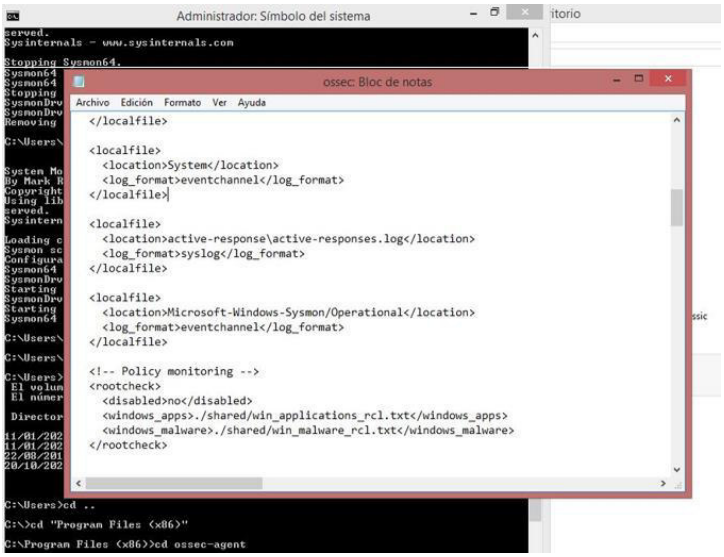


Figura 45 Edición de archivo .conf para eventos Sysmon en Wazuh

Se debe reinicar el agente:

Figura 46 Reinicio del servicio del agente

Como se evidencia a nivel de la consola de Wazuh (SIEM) ya se registran los eventos referentes a "Sysmon"

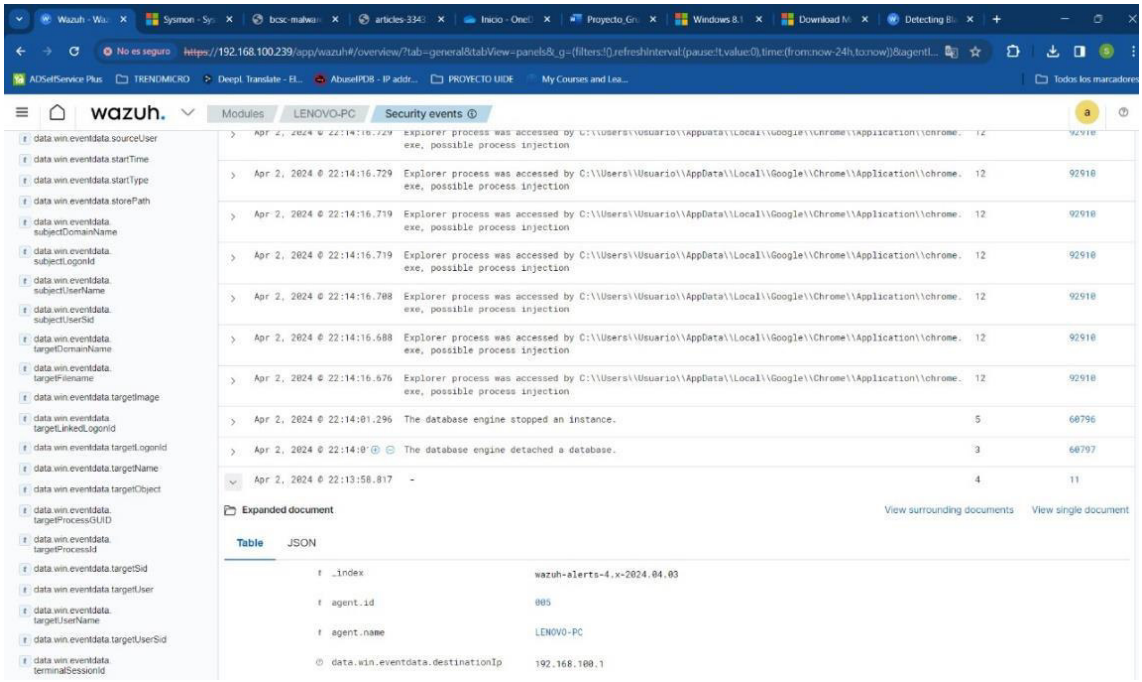


Figura 47 Eventos de Seguridad del Endpoint en Consola

Adicional a esto, se configuró las reglas correspondientes en el servidor de Wazuh para la detección del Ransomware, lo cual, al momento de su ejecución, se puede observar que lo detecta correctamente:

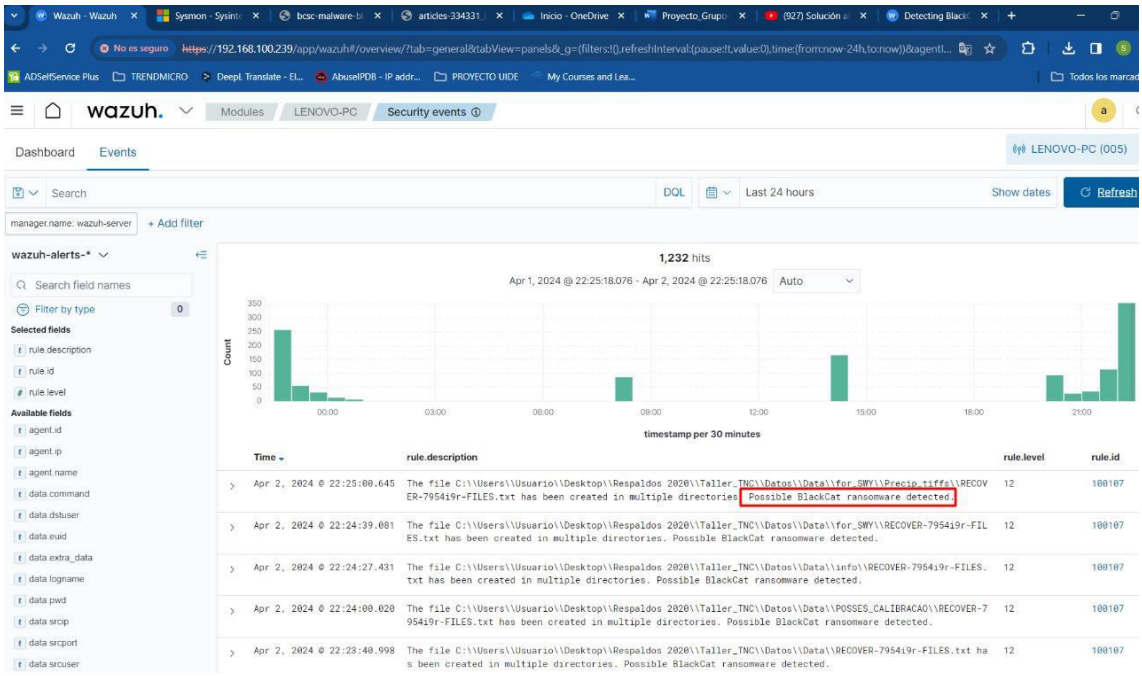


Figura 48 Detección de evento de seguridad – Ransomware

Como principal y segundo método de detección tendremos la lista CDB de hashes de malware que contendrá hashes en formato SHA-256 de ransomware BlackCat conocidos, además del hash de nuestra muestra principalmente. Estas se guardarán en el directorio */var/ossec/etc/lists* del servidor Wazuh:

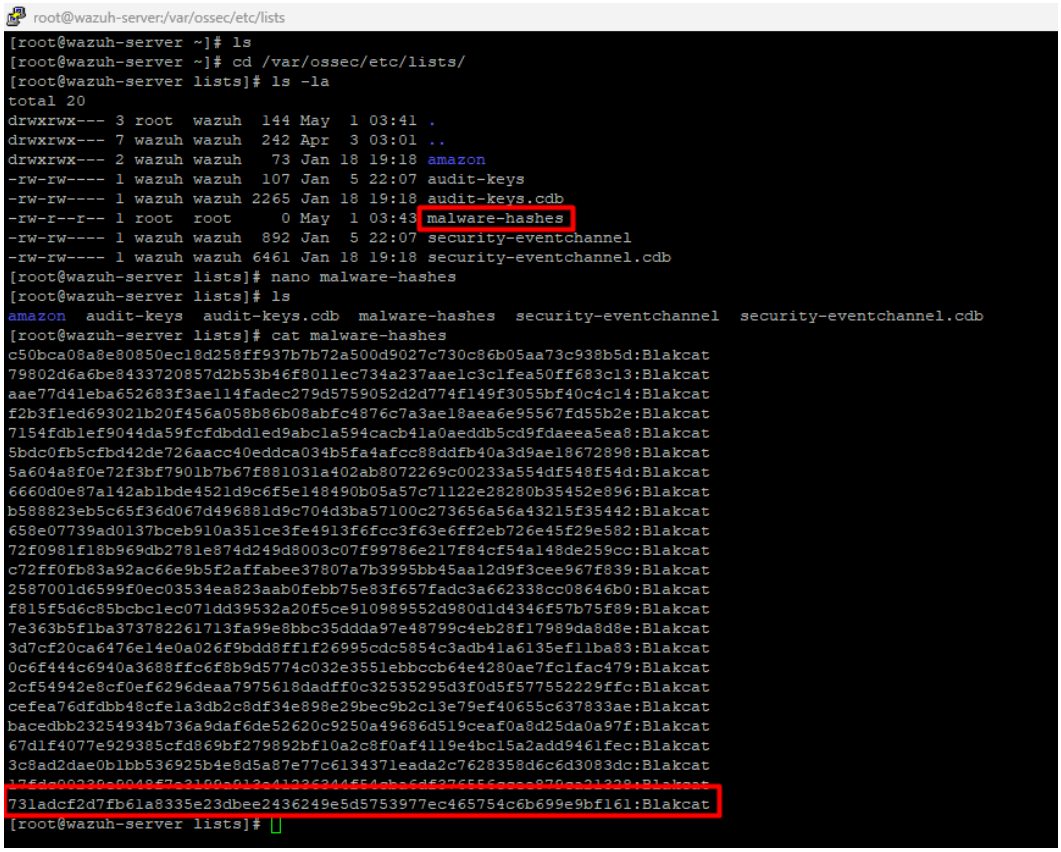


Figura 49 Lista CDB creada en servidor Wazuh

Para esto se agrega la lista a la sección ***<ruleset>*** del archivo ossec.conf como se muestra a continuación:

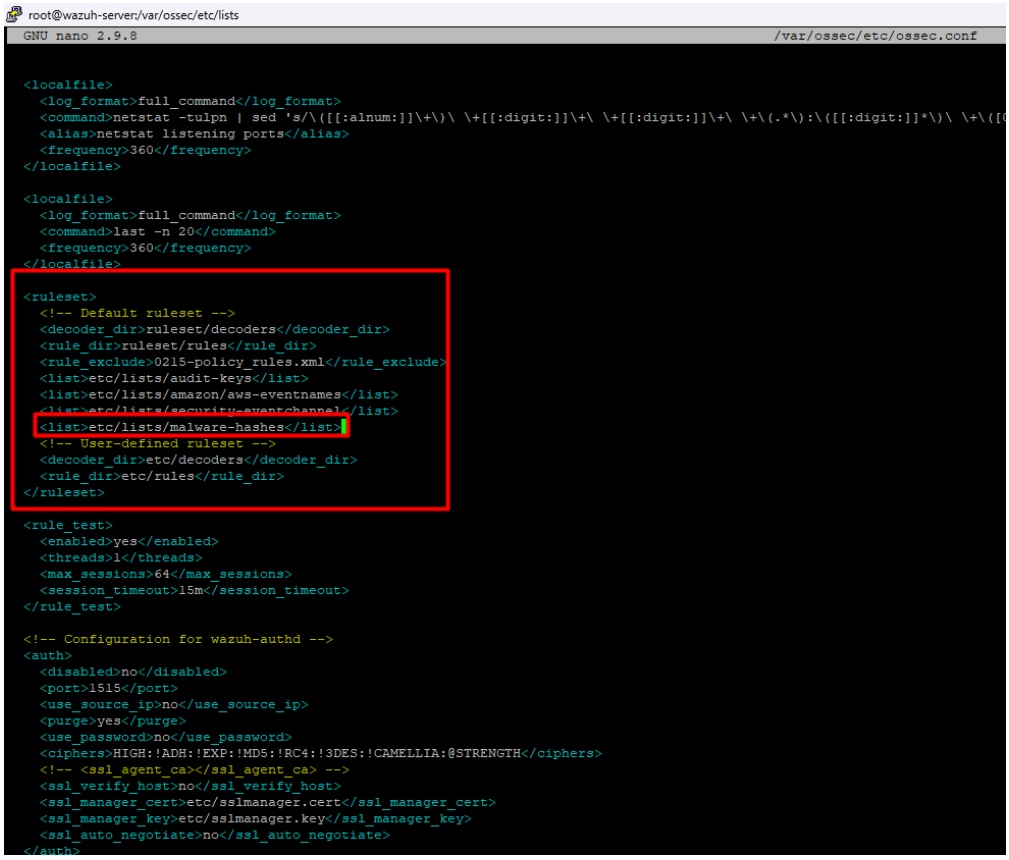


Figura 50 Archivo ossec.conf + la nueva regla con la ruta de la lista CDB

La regla genera alertas en el panel de Wazuh cuando se detecta cualquiera de los hashes SHA256 en la lista CDB:

```
<group name="blackcat,">
  <rule id="110002" level="13">
    <if_sid>554, 550</if_sid>
    <list field="sha256" lookup="match_key">etc/lists/malware-hashes</list>
    <description>File with known BlackCat malware hash detected: $(file)</description>
    <mitre>
      <id>T1204.002</id>
    </mitre>
```

```
  </rule>
</group>
```

Tabla 5 Regla de detección en base a lista CDB

Wazuh activa la regla 554 cuando un usuario o proceso agrega un nuevo archivo a un directorio monitoreado y la regla 550 cuando un usuario o proceso modifica un archivo.

Endpoint de prueba con Agente Wazuh

Se agregó la siguiente configuración dentro del bloque ***<syscheck>*** del archivo de configuración del agente Wazuh. Esto configura el módulo Wazuh FIM para monitorear el directorio de **Descargas (Downloads)** de todos los usuarios.

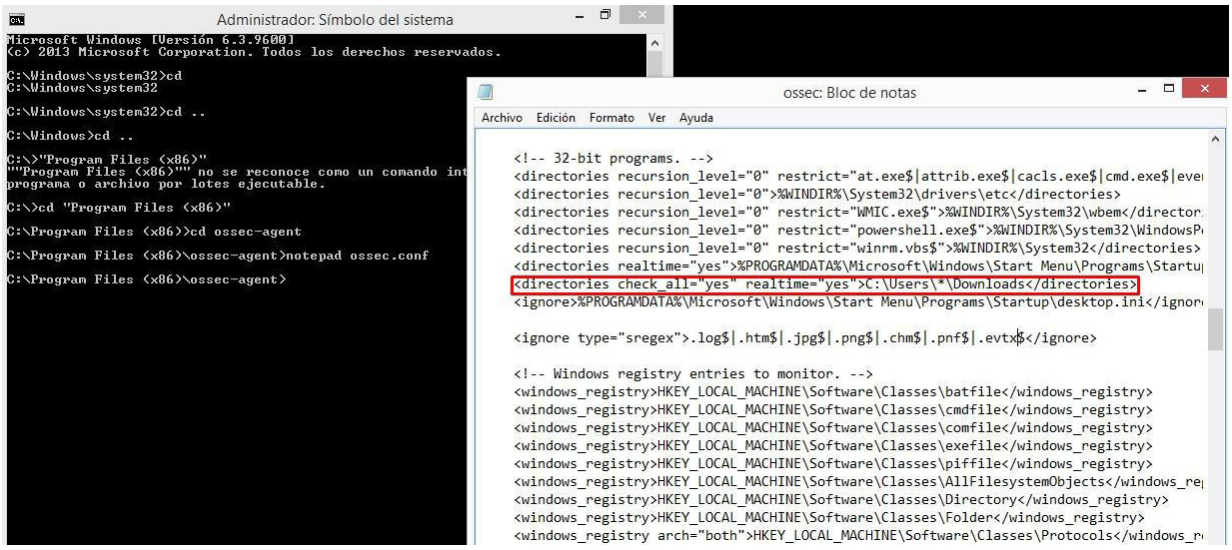


Figura 51 Archivo de configuración systemcheck + Directorio Downloads

La opción ***check_all*** garantiza que Wazuh verifique todos los atributos del archivo, incluido el tamaño del archivo, los permisos, el propietario, la fecha de la última modificación, el inodo y el hash.

Para probar la regla de detección, se descargó la muestra del ransomware BlackCat en el directorio monitoreado. La siguiente alerta muestra que el hash del archivo descargado está en la lista CDB.

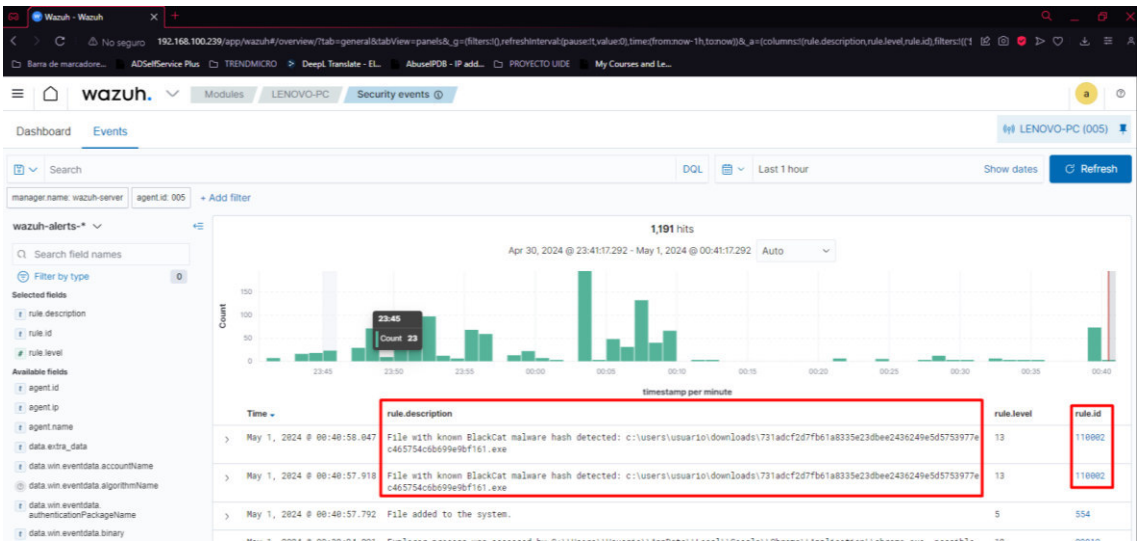


Figura 52 Eventos de seguridad + Log de la regla de la lista CDB y su ID

Con esto hemos mostrado cómo se detecta el ransomware BlackCat utilizando una lista CDB haciendo coincidir las sumas de comprobación (SHA256) de los archivos con una lista CDB de hashes maliciosos conocidos. Se puede llevar esto más allá configurando el módulo de **respuesta activa** para eliminar cualquier archivo con los hashes en nuestra lista CDB.

Configuración de la respuesta activa para eliminar archivos del ransomware BlackCat

El módulo de respuesta activa de Wazuh realiza varias contramedidas para hacer frente a las amenazas detectadas. Las **respuestas activas** ejecutan un script en un endpoint en respuesta a ciertos disparadores. Por ejemplo, si una regla específica se activa y genera una alerta, un script de respuesta activa se ejecutará en el endpoint que generó esa alerta. En este caso, mostramos cómo se puede configurar un script de Python en el endpoint de Windows para eliminar los archivos del ransomware BlackCat en cuanto Wazuh los detecte. Para lograr esto, se requiere Python y Pyinstaller en el endpoint de Windows para convertir el script de Python en un archivo ejecutable.

Creación del script con el nombre remove-threat.py, el cual cómo funciones principales se tomarán en cuenta las siguientes:

Eliminación de archivos basada en el registro de Wazuh:

```
try:
    os.remove(msg.alert["parameters"]["alert"]["syscheck"]["path"])
    write_debug_file(argv[0], json.dumps(msg.alert) + " Successfully removed threat")
except OSError as error:
    write_debug_file(argv[0], json.dumps(msg.alert) + "Error removing threat")
```

Tabla 6 Función que elimina los archivos y muestra un mensaje de registro

- Esta sección del script utiliza la función **os.remove** para eliminar archivos del sistema de archivos, basándose en la información obtenida de las alertas de Wazuh.
- La ruta del archivo a eliminar se extrae de la alerta de Wazuh y se proporciona como argumento a la función **os.remove**.
- Si la eliminación tiene éxito, se registra un mensaje indicando que la amenaza se ha eliminado correctamente. En caso de error, se registra un mensaje de error.
- **msg.alert:** Este es el objeto JSON que contiene la alerta generada por Wazuh.
- **["parameters"]["alert"]["syscheck"]["path"]:** Estos son los diferentes niveles de anidación en la estructura JSON que llevan a la ruta del archivo a eliminar. Por ejemplo:
    - "parameters": Este es un campo dentro de la alerta que contiene varios parámetros asociados con la alerta.
    - "alert": Dentro de los parámetros, este campo contiene información específica sobre la alerta.
    - "syscheck": Dentro de la información de la alerta, este campo puede contener detalles relacionados con el sistema de archivos o la integridad del sistema.
    - "path": Finalmente, este campo específico contiene la ruta del archivo que se desea eliminar.

2. **Registro de mensajes de depuración**:

```
def write_debug_file(ar_name, msg):
    with open(LOG_FILE, mode="a") as log_file:
        log_file.write(str(datetime.datetime.now().strftime('%Y/%m/%d %H:%M:%S')) + " " + ar_name + ": " + msg +"\n")
```

Tabla 7 Código con registro de mensaje de depuración

- La función ***write_debug_file*** se encarga de registrar mensajes de depuración en un archivo de registro.
- Toma dos argumentos: el nombre del archivo de registro y el mensaje que se va a registrar.
- El mensaje se concatena con la fecha y hora actuales antes de escribirse en el archivo de registro.

Este script utiliza la función ***os.remove*** para eliminar archivos como parte de su respuesta a amenazas de seguridad detectadas por Wazuh. Además, registra información relevante sobre sus acciones utilizando la función ***write_debug_file***, lo que facilita el seguimiento y la depuración del comportamiento del script.

Finalmente convertimos este script de Python remove-threat.py en un archivo ejecutable gracias a pyinstaller y lo copiamos de la carpeta ***\dist*** a la ruta *C:\Archivos de programa (x86)\ossec-agent\active-response\bin* para la respuesta activa y registro en la consola del SIEM.

En el servidor de Wazuh se añadió el siguiente bloque en ossec.conf para que el servidor Wazuh inicie una respuesta activa una vez que un evento active la **regla 110002:**

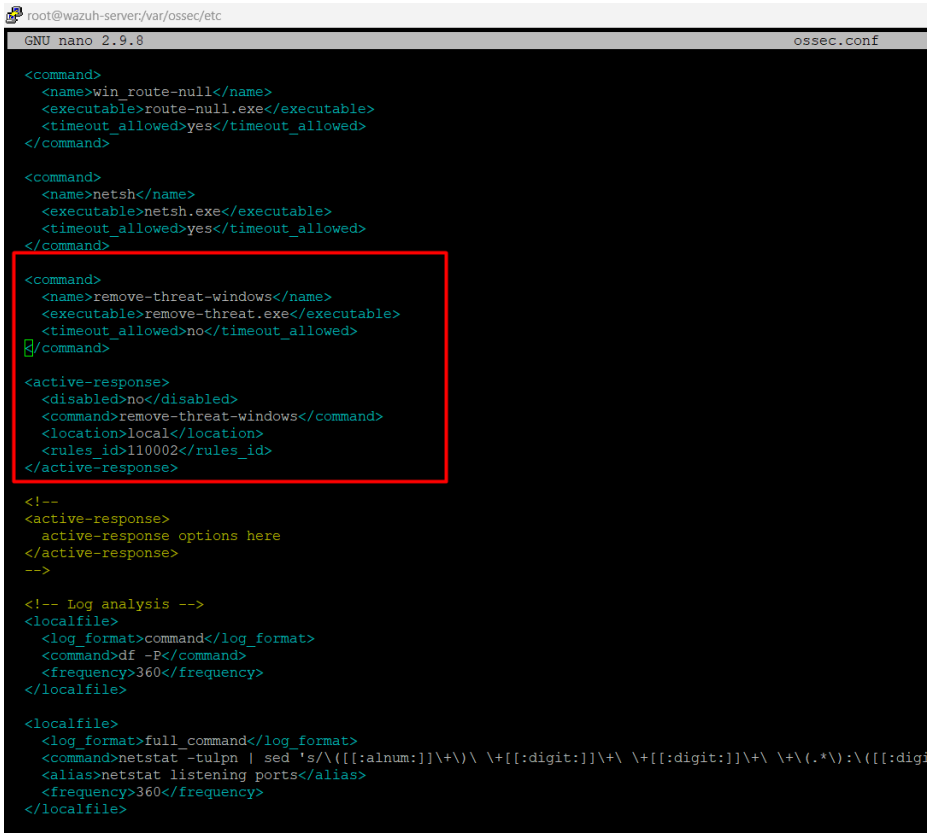


Figura 53 Respuesta activa + ID de la regla

Donde:

- La etiqueta <***name***> especifica el nombre del comando en la sección de respuesta activa.

- La etiqueta <***executable***> especifica el archivo ejecutable a ejecutar. En este caso, el ejecutable remove-threats.exe que construyó anteriormente.
- El bloque de etiquetas <***active response***> llama al bloque de comandos cuando el ID de regla especificado activa una alerta. En este caso, especifica el ID de **regla 110002**, que es la regla que detecta archivos con hashes maliciosos que especificamos en la lista CDB.

También se crearon reglas para alertar cuando la eliminación de archivos de respuesta activa tenga éxito o falle añadiendo las siguientes reglas a al archivo ***/local_rules.xml*:**

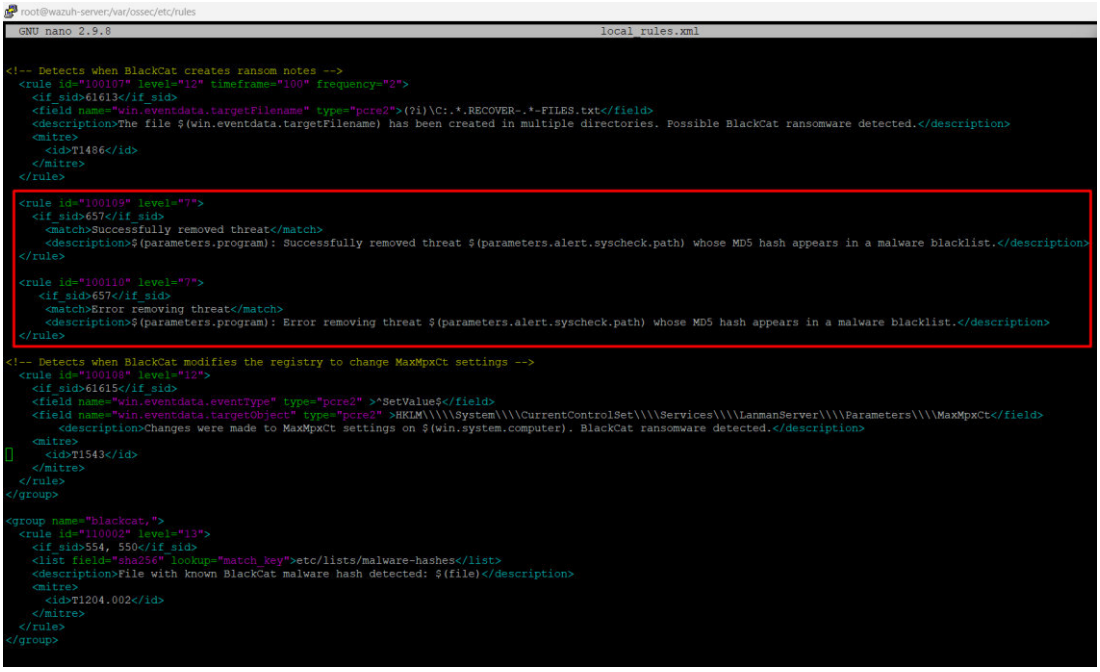


Figura 54 Reglas para registro de éxito o falla de la respuesta activa

Para probar la configuración realizada, intentamos descargar nuevamente la muestra de nuestro ransomware BlackCat en el endpoint de Windows.

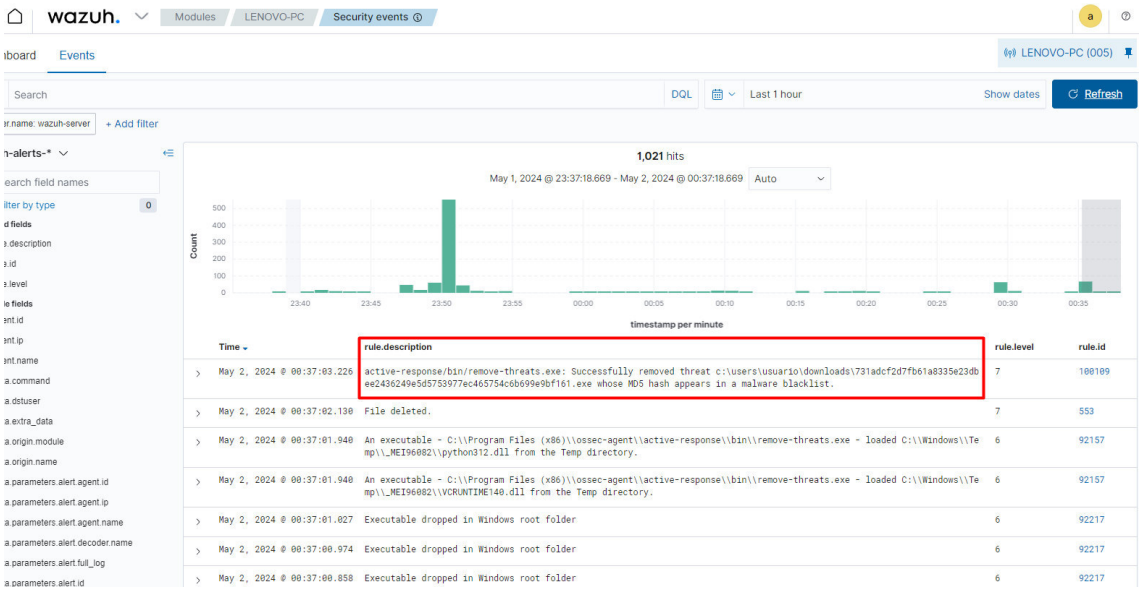


Figura 55 Registro del evento en base a la regla creada + la respuesta activa realizada

En la siguiente captura de pantalla se puede observar que el módulo de respuesta activa elimina el archivo y genera una alerta de este evento.

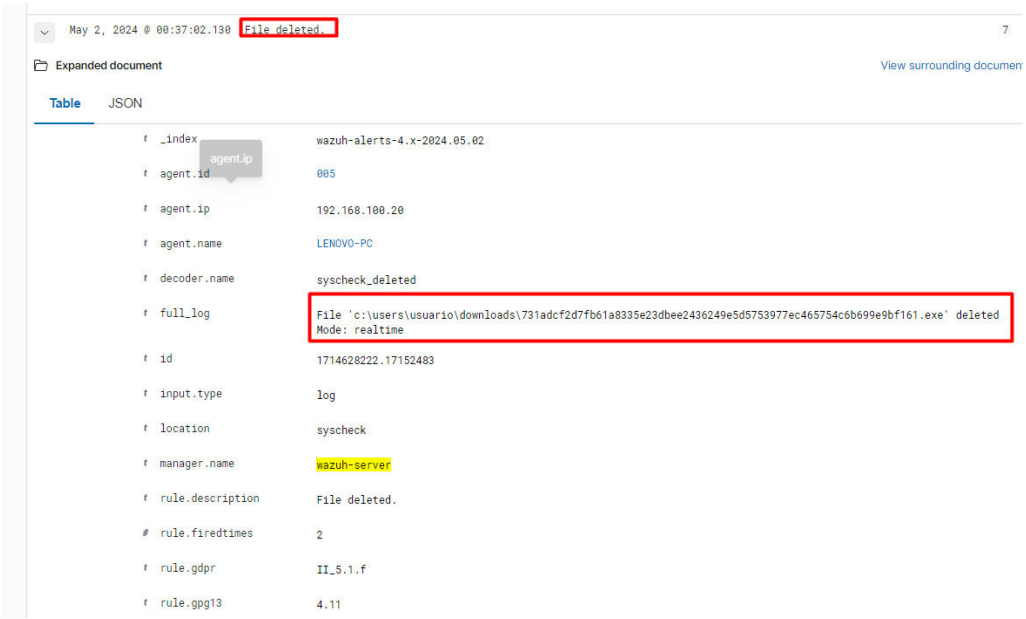
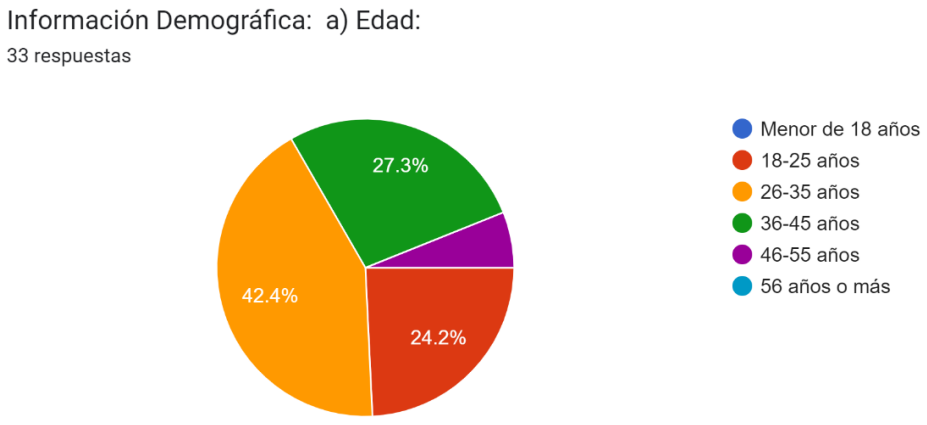


Figura 56 Evidencia del archivo descargado eliminado gracias a la respuesta activa con Wazuh.

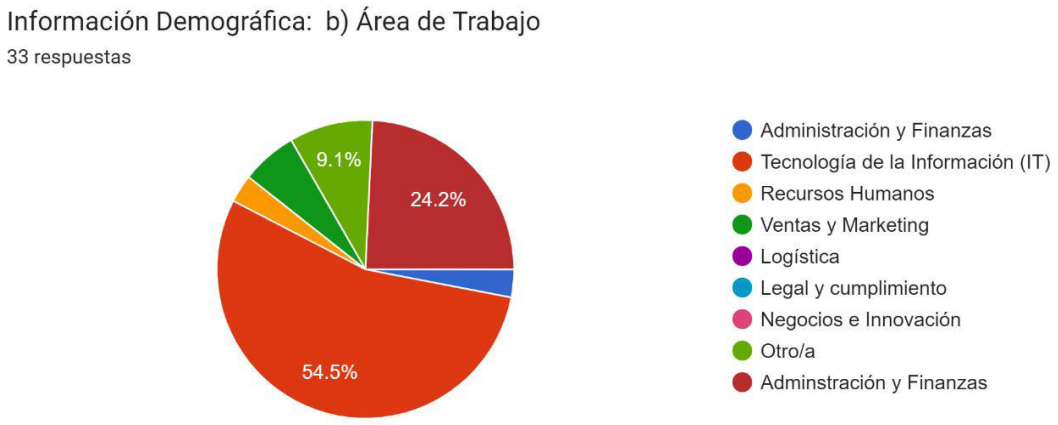
Un medidor utilizado para recopilar información en el desarrollo de este proyecto fue la realización de una encuesta en diferentes ambientes laborales, todos estos datos obtenidos mediante el uso de los formularios de Google permitieron entender cómo los diferentes usuarios, tanto expertos como no expertos, perciben la amenaza del ransomware y cuánto conocen sobre las soluciones SIEM. Esto incluye evaluar el nivel de conciencia y conocimiento sobre estos temas en distintos sectores y niveles de experiencia.

También, se pudo obtener una idea en base opiniones y experiencias sobre la efectividad de las soluciones SIEM en la detección y prevención de ataques de ransomware. Esto ayudará a identificar si estas herramientas están cumpliendo su propósito y dónde podrían necesitar mejoras. Los datos recopilados revelan brechas en el conocimiento y en la implementación de soluciones de ciberseguridad. Esto puede ayudar a organizaciones, profesionales y proveedores de SIEM a entender mejor qué áreas necesitan más atención o recursos. A continuación, se presenta los datos obtenidos:



Pregunta 1

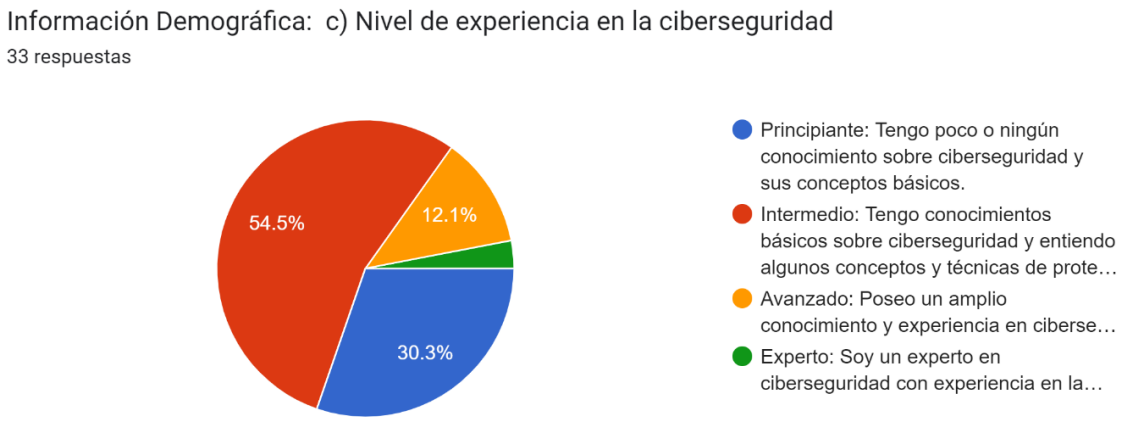
La mayoría de los encuestados (69.7%) están en el rango de edad de 26 a 45 años, lo que podría indicar que la encuesta ha captado la atención de profesionales en una etapa productiva de su carrera. La ausencia de respuestas en los grupos de edad menores de 18 años y mayores de 46 años podría sugerir una baja participación de estudiantes menores de edad y profesionales de mayor edad o jubilados. Esto puede influir en los resultados, ya que las percepciones y conocimientos sobre ciberseguridad y ransomware podrían variar significativamente entre diferentes grupos etarios. La fuerte representación del grupo de 26-35 años puede reflejar un interés particular de los jóvenes profesionales en temas de ciberseguridad, quizás debido a su relevancia en el mercado laboral actual.



Pregunta 2

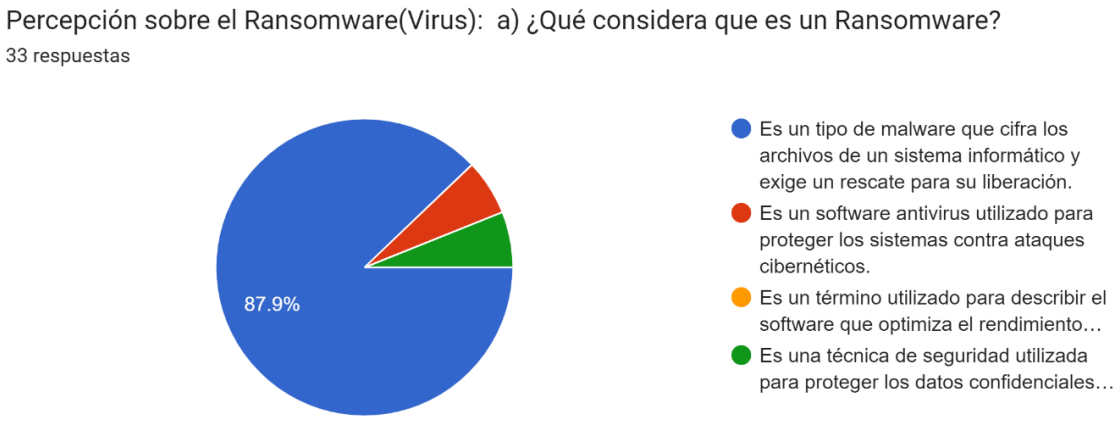
Con un 54.5% de los participantes trabajando en el sector de Tecnología de la Información, es claro que esta encuesta ha atraído principalmente a profesionales con un enfoque en tecnología. Esto es relevante porque estos individuos probablemente tengan una comprensión más profunda de los temas de ciberseguridad y SIEM. Aunque el sector IT es predominante, hay una

representación notable de otras áreas, particularmente "Otro/a" con un 24.2%. Esto sugiere que, aunque la mayoría de los encuestados son de IT, la encuesta también ha captado la atención de profesionales de otros campos. Sectores como Administración y Finanzas, Ventas y Marketing, Legal y Cumplimiento, y Negocios e Innovación no tienen representación en esta encuesta. Esto puede limitar la perspectiva sobre cómo estos sectores perciben las amenazas de ransomware y las soluciones SIEM.



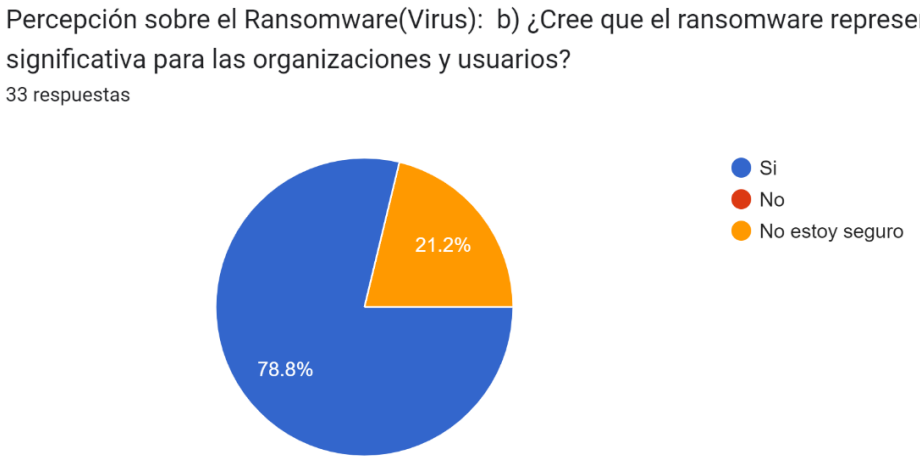
Pregunta 3

La encuesta muestra que una gran parte de los encuestados (54.5%) está en un nivel intermedio, lo que es positivo, pero también resalta la oportunidad de avanzar más en la formación y el desarrollo de habilidades. El 12.1% de nivel avanzado proporciona una base de expertos para liderar y guiar, aunque su número es limitado. El 30.3% de principiantes sugiere una necesidad significativa de programas educativos básicos para aumentar la conciencia y las habilidades en ciberseguridad.



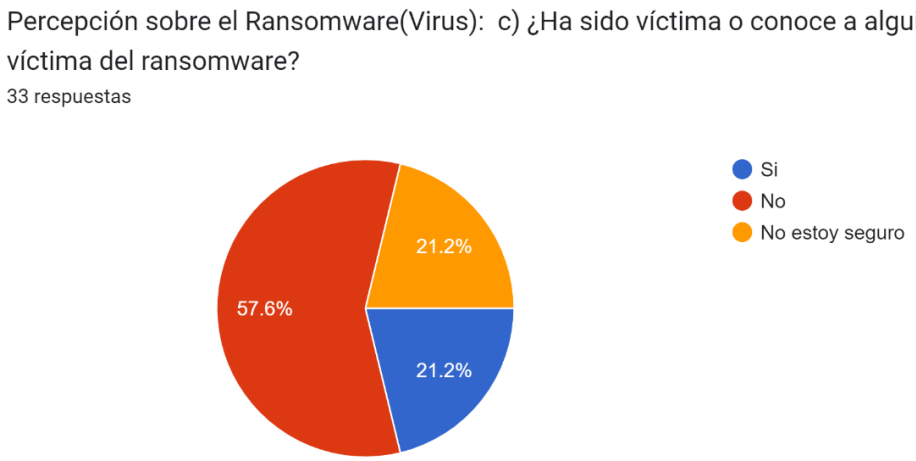
Pregunta 4

La mayoría de los encuestados tiene una percepción correcta del ransomware, lo cual es alentador y sugiere una buena base de conocimiento en la comunidad o entre los empleados. Sin embargo, hay un pequeño porcentaje que muestra confusión sobre el término, lo cual puede ser preocupante.



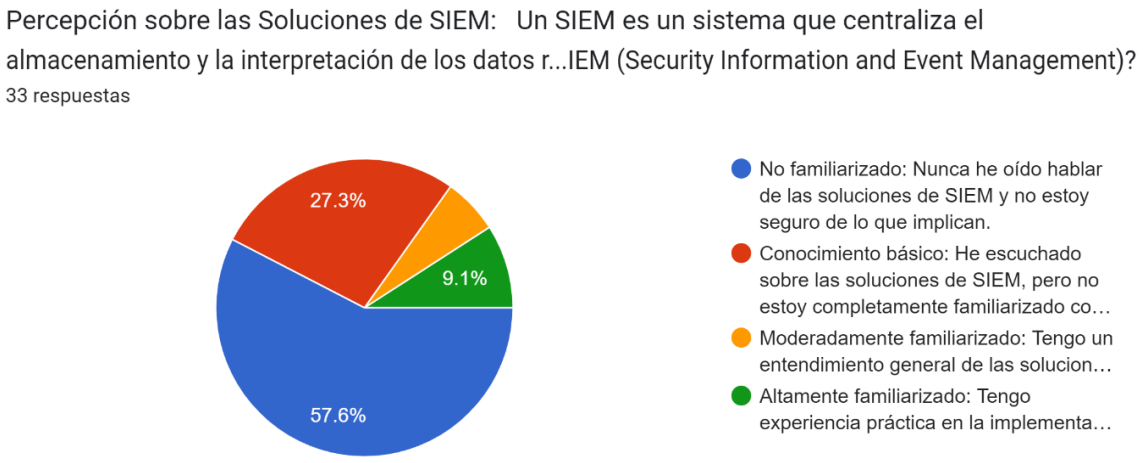
Pregunta 5

La mayoría de los participantes reconoce la seriedad del ransomware como una amenaza, lo cual es alentador y sugiere que una parte significativa de la población encuestada está consciente de los riesgos y posiblemente preparada para enfrentarlos. No obstante, hay una minoría significativa que no está segura de la magnitud de la amenaza, lo que indica la necesidad de mejorar la educación y la concienciación sobre el ransomware.



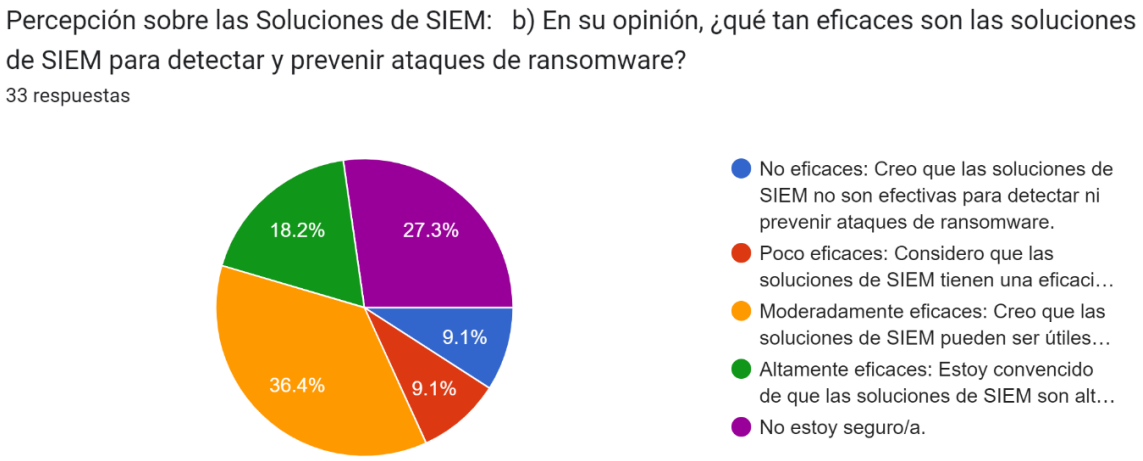
Pregunta 6

Los resultados sugieren que si bien una mayoría no ha experimentado el ransomware personalmente ni conoce a alguien que lo haya hecho, una parte significativa de la población encuestada tiene experiencia directa o indirecta con este tipo de ataque. Esto subraya la importancia de la concienciación y la preparación en materia de ciberseguridad, ya que el ransomware sigue siendo una amenaza relevante para muchas personas y organizaciones.



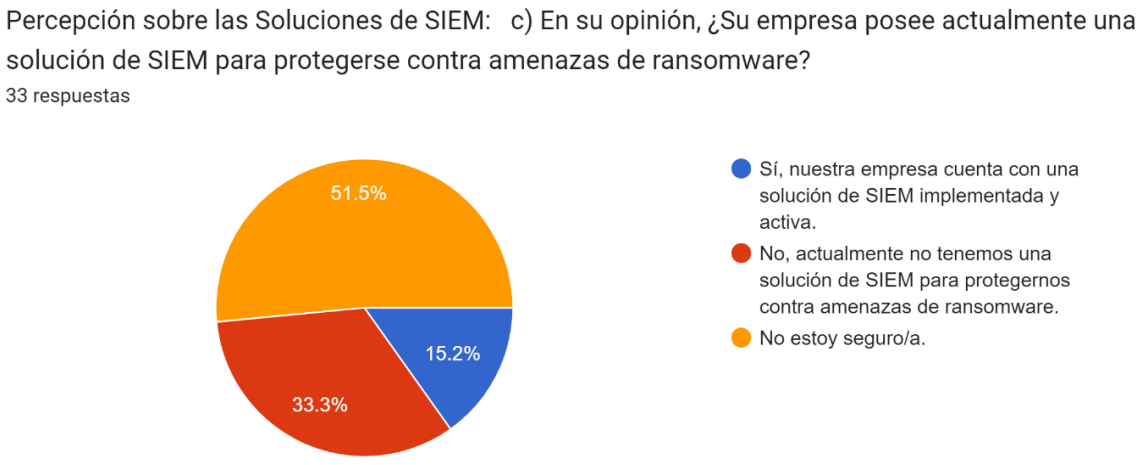
Pregunta 7

Los resultados muestran una amplia gama de niveles de familiaridad con las soluciones de SIEM entre los encuestados. La mayoría reporta estar no familiarizado o tener solo un conocimiento básico sobre estas herramientas, lo que destaca la necesidad de mayor educación y concienciación sobre la importancia y el funcionamiento de las soluciones de SIEM en el ámbito de la ciberseguridad. Aquellos que están moderadamente o altamente familiarizados pueden desempeñar un papel importante en la educación y capacitación de otros sobre este tema.



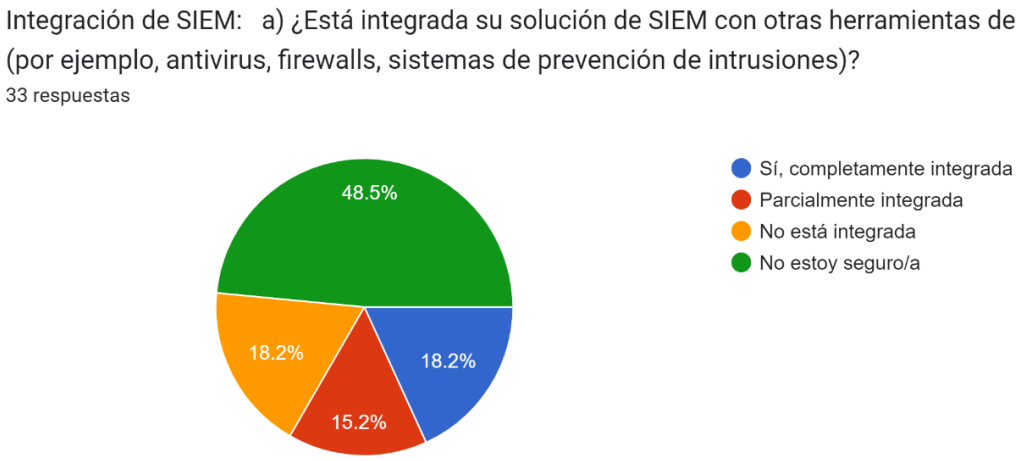
Pregunta 8

La percepción sobre la eficacia de las soluciones de SIEM para detectar y prevenir ataques de ransomware varía entre los encuestados. Mientras que algunos tienen una percepción positiva de su eficacia, otros expresan dudas o desconfianza en su capacidad para abordar eficazmente esta amenaza. Es importante abordar estas percepciones y trabajar para mejorar la efectividad de las soluciones de SIEM en la detección y prevención de ataques de ransomware mediante la mejora de la configuración, la integración con otras herramientas de seguridad, y la educación sobre su funcionamiento y capacidades.



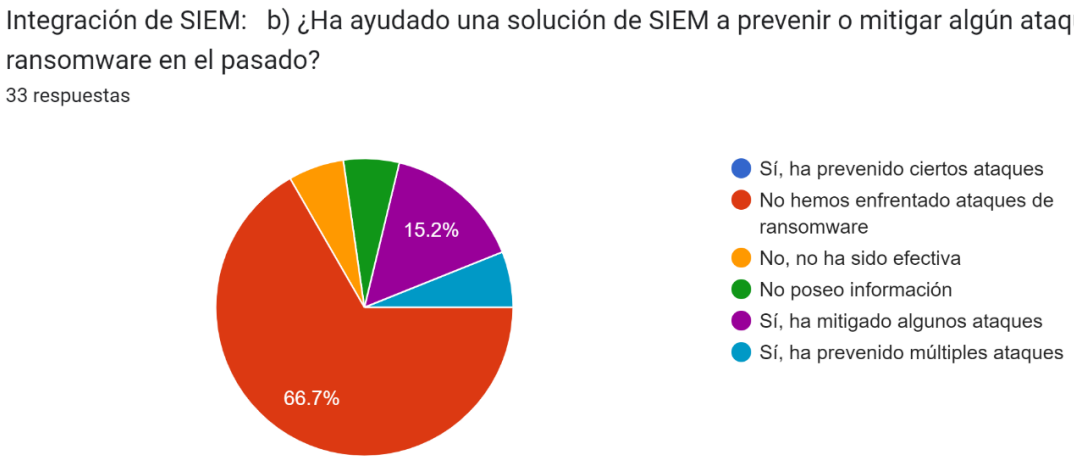
Pregunta 9

Los resultados muestran una diversidad de percepciones sobre si las empresas poseen actualmente una solución de SIEM para protegerse contra amenazas de ransomware. Mientras que una minoría afirma tener una solución de SIEM, una proporción significativa no está segura o cree que su empresa no tiene una solución de SIEM en su lugar. Esto destaca la importancia de una evaluación exhaustiva de la postura de seguridad de las empresas y la implementación de soluciones de SIEM donde sea necesario para protegerse contra amenazas de ransomware y otros ataques cibernéticos.



Pregunta 10

Los resultados muestran una diversidad de percepciones sobre el nivel de integración de las soluciones de SIEM con otras herramientas de seguridad. Mientras que algunos informan una integración completa o parcial, otros indican una falta de integración o no están seguros sobre el estado de la integración en sus organizaciones. Esto subraya la importancia de una evaluación exhaustiva de la arquitectura de seguridad y la implementación de estrategias de integración efectivas para mejorar la eficacia de la seguridad cibernética en general.



Pregunta 11

Los resultados muestran una variedad de experiencias con respecto a si una solución de SIEM ha ayudado a prevenir o mitigar ataques de ransomware en el pasado. Mientras que la mayoría no ha enfrentado tales ataques, una minoría informa que su solución de SIEM ha sido efectiva en la mitigación o prevención de ataques de ransomware. Esto resalta la importancia de implementar y gestionar adecuadamente soluciones de SIEM como parte integral de la estrategia de seguridad cibernética de una organización para protegerse contra las amenazas emergentes, como el ransomware.

viii. Análisis y Discusión Crítica:

En el proyecto "Análisis de Ransomware BlackCat para Detección y Mitigación con Tecnología SIEM Wazuh", se han analizado diversos aspectos del ransomware BlackCat para comprender su funcionamiento y determinar soluciones efectivas para su mitigación mediante tecnología SIEM.

El ransomware BlackCat opera mediante un token de acceso específico, en este caso, el token de acceso utilizado fue el 1231. Durante la ejecución y el análisis del ransomware, se observó que, una vez ingresado el token, el ransomware toma privilegios de administrador, lo que le permite eliminar cualquier copia de respaldo disponible en el sistema. Esta acción crítica prepara el terreno para que el ransomware pueda cifrar archivos sin ser interrumpido.

En pruebas realizadas en equipos con diferentes niveles de contenido de información, se encontró que el tiempo de cifrado varía significativamente. En una máquina con pocos archivos, el cifrado fue prácticamente inmediato, mientras que, en un sistema con un volumen de datos considerable, el proceso tomó aproximadamente 15 minutos. En ambos casos, el ransomware finalizó su actividad colocando un archivo de texto con el mensaje de rescate en el escritorio de las computadoras, todas operando bajo Windows 10.

Sin embargo, una prueba en un equipo con Windows 8 reveló una anomalía: el mensaje de rescate no apareció, lo que sugiere posibles diferencias en la efectividad del ransomware dependiendo del sistema operativo. Este hallazgo subraya la importancia de adaptar las medidas de detección y mitigación a diferentes entornos tecnológicos.

Adicionalmente, el análisis del tráfico de red con Wireshark mostró intentos de conexión a direcciones IP del rango multicast (224.0.0.22, 224.0.0.251 y 224.0.0.252). Estas conexiones sugieren que el ransomware intenta propagarse a otros dispositivos en la red, utilizando la comunicación multicast para expandir su alcance.

Los resultados obtenidos de estos análisis revelan patrones significativos en el comportamiento del ransomware BlackCat en un entorno controlado. Estos patrones son esenciales para la creación de reglas específicas en el SIEM Wazuh, lo que permite una detección y mitigación efectivas. Wazuh demostró ser altamente eficiente en la detección temprana de actividades sospechosas, y su capacidad de personalización permite ajustar las reglas según las necesidades específicas de cada escenario.

En cuanto a limitaciones, se debe considerar que los resultados obtenidos en un entorno controlado pueden no representar completamente situaciones reales en varias organizaciones. Sin embargo, este estudio proporciona una guía valiosa para el análisis de otras variantes de ransomware y resalta la importancia de la adaptabilidad de las soluciones SIEM.

La metodología empleada, que combinó análisis técnico y pruebas prácticas, ofrece una visión integral de la amenaza que representa el ransomware BlackCat y destaca la eficacia de Wazuh como herramienta de mitigación. Este proyecto no solo refuerza la ciberseguridad en Ecuador, sino que también contribuye al conocimiento global en la lucha contra el ransomware, proponiendo estrategias de defensa proactivas y efectivas.

En base a los datos obtenidos de la encuesta se puede decir que, en un panorama digital cada vez más complejo y en constante evolución, la ciberseguridad se ha convertido en una prioridad crucial para organizaciones y usuarios por igual. En este contexto, las soluciones de SIEM (Security Information and Event Management) desempeñan un papel fundamental al proporcionar una plataforma centralizada para la recopilación, el almacenamiento y la interpretación de datos

relevantes de seguridad. Sin embargo, la percepción y la experiencia con respecto a estas soluciones, así como la amenaza del ransomware, reflejan una serie de desafíos y oportunidades en el ámbito de la ciberseguridad. Desde el punto de vista de la familiaridad y la percepción sobre la eficacia de las soluciones de SIEM, es evidente que existe una variedad de niveles de conocimiento y opiniones. Mientras que algunos tienen un entendimiento básico y perciben estas soluciones como efectivas para abordar las amenazas, otros muestran escepticismo o desconocimiento sobre su funcionalidad y eficacia. Esto subraya la necesidad de una mayor educación y concienciación sobre las soluciones de SIEM y su papel en la protección contra amenazas cibernéticas, como el ransomware. La integración de las soluciones de SIEM con otras herramientas de seguridad es otro aspecto crítico que influye en su efectividad. Si bien algunos informan sobre una integración completa o parcial, muchos muestran incertidumbre sobre el estado de la integración en sus organizaciones. Esto destaca la importancia de mejorar la transparencia y la colaboración en la implementación y gestión de soluciones de seguridad, así como de promover las mejores prácticas de integración entre las diferentes herramientas de seguridad. En cuanto a la experiencia con la prevención o mitigación de ataques de ransomware mediante soluciones de SIEM, si bien la mayoría de las organizaciones no han enfrentado tales ataques, hay casos en los que las soluciones de SIEM han demostrado ser efectivas en la detección temprana o la prevención de ataques de ransomware. Esto resalta la importancia de implementar y gestionar adecuadamente estas soluciones como parte integral de la estrategia de seguridad cibernética de una organización. La percepción general sobre la amenaza del ransomware refleja una comprensión generalizada de su gravedad y su impacto potencial en las organizaciones y los

usuarios. Sin embargo, aún existe una minoría que muestra incertidumbre sobre la magnitud de esta amenaza, lo que destaca la necesidad de mejorar la educación y la concienciación sobre el ransomware y otras amenazas cibernéticas emergentes.

d. CAPITULO 4

i. Conclusiones

El análisis exhaustivo realizado en este estudio sobre el ransomware BlackCat y su mitigación utilizando la tecnología SIEM Wazuh revela hallazgos fundamentales que requieren una acción inmediata. Es evidente que fortalecer las defensas contra el ransomware, especialmente frente a la amenaza persistente de BlackCat, es imperativo en el panorama actual de ciberseguridad.

Las recomendaciones derivadas de este estudio no solo abogan por mejoras en la implementación de SIEM Wazuh, sino que también resaltan la necesidad de adoptar enfoques adaptativos para enfrentar amenazas cibernéticas en constante evolución. La flexibilidad y capacidad de adaptación son elementos clave en la defensa contra ataques de ransomware, y es crucial que las organizaciones estén preparadas para ajustar sus estrategias y medidas de seguridad según sea necesario.

Además, este estudio ofrece una plataforma sólida para futuras investigaciones en el campo de la ciberseguridad. Identificar y abordar las limitaciones identificadas en este estudio es esencial para avanzar en la protección contra amenazas cibernéticas. La adaptabilidad de las estrategias de prevención es esencial, y la investigación continua es fundamental para mantenerse a la vanguardia de las tecnologías y prácticas de seguridad.

En resumen, este estudio resalta la relevancia crítica de la ciberseguridad en entornos gubernamentales y más allá. Solo al estar alerta y comprometidos con la mejora continua de

nuestras defensas cibernéticas podremos mitigar eficazmente las amenazas emergentes y proteger nuestros activos más valiosos contra futuros ataques de ransomware.

ii. Recomendaciones

Realizar capacitaciones especializadas para los equipos de TI sobre la configuración avanzada y el uso efectivo de SIEM Wazuh. Esto asegurará que el personal esté bien preparado para maximizar las capacidades de esta herramienta en la detección y mitigación de amenazas como BlackCat en entornos gubernamentales del Ecuador.

Implementar programas de concientización y formación continua sobre ciberseguridad para todos los empleados. Esto debe incluir capacitación específica sobre cómo identificar y evitar ataques de ransomware, así como la importancia de seguir las mejores prácticas de seguridad en sus actividades diarias, esto cambiara totalmente la perspectiva de los empleados a la hora de abrir y confiar en archivos externos a la institución, promoviendo un entorno de trabajo más seguro.

Hay que asegurar que todos los sistemas operativos, aplicaciones y dispositivos estén actualizados con los últimos parches y actualizaciones de seguridad. Establecer procedimientos automatizados para el despliegue de parches y actualizaciones, reduciendo la ventana de oportunidad para los atacantes que explotan vulnerabilidades conocidas.

Establecer políticas de seguridad claras y comprensibles que todos los empleados deben seguir. Esto incluye la gestión segura de contraseñas, el uso de autenticación multifactor, y la limitación de privilegios de acceso basado en el principio de mínimo privilegio.

Crear y entrenar equipos dedicados de respuesta a incidentes de seguridad cibernética. Estos equipos deben estar preparados para actuar rápidamente ante cualquier indicio de ataque, con protocolos claros para la identificación, contención, erradicación y recuperación de incidentes.

Referencias/Bibliografía:

Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encinas, L. (2020). Ciberseguridad. Editorial CSIC Consejo Superior de Investigaciones Científicas. https://www.mdconsult.internacional.edu.ec:2057/es/lc/uide/titulos/172144

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

Algar Díaz, M. J., & Fernández de Sevilla Vellón, M. (2019). Introducción práctica a la programación con Python. Editorial Universidad de Alcalá. https://www.mdconsult.internacional.edu.ec:2057/es/lc/uide/titulos/124259?as_all=python&as_all_op=unaccent__icontains&prev=as

Cen, M., Jiang, F., Qin, X., Jiang, Q., & Doss, R. (2024). Ransomware early detection: A survey. Computer Networks, 239, 110138. https://doi.org/10.1016/j.comnet.2023.110138

Görmez, Y., Arslan, H., Işık, Y. E., & Dadaş, İ. E. (2023). A User and Entity Behavior Analysis for SIEM Systems: Preprocessing of The Computer Emergency and Response Team Dataset. Journal of Soft Computing and Artificial Intelligence, 4(1), Article 1. https://doi.org/10.55195/jscai.1213782

Pereira, T., & Huey, C. (2022, marzo 17). From BlackMatter to BlackCat: Analyzing two attacks from one affiliate. Cisco Talos Blog. https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/

Raja, M. S. N., & Vasudevan, A. R. (2017). Rule Generation for TCP SYN Flood attack in SIEM Environment. Procedia Computer Science, 115, 580-587. https://doi.org/10.1016/j.procs.2017.09.117

Santos, A. T., Alex Hinchliffe, Doel. (2022, enero 27). Threat Assessment: BlackCat Ransomware. Unit 42. https://unit42.paloaltonetworks.com/blackcat-ransomware/

Smiliotopoulos, C., Barmpatsalou, K., & Kambourakis, G. (2022). Revisiting the Detection of Lateral Movement through Sysmon. Applied Sciences, 12(15), Article 15. https://doi.org/10.3390/app12157746

Tomás Guerra, J. (2019). Repositori Institucional (O2): Monitorización de seguridad con Wazuh. 63.

Torres, J. (2020). Python Deep Learning: Introducción práctica con Keras y TensorFlow 2. Alpha Editorial.

Wazuh. (2022). Deploying Wazuh agents on Linux systems. Recuperado de https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html

Wazuh. (2022). Enhancing with MITRE. Recuperado de https://documentation.wazuh.com/current/user-manual/ruleset/mitre.html

Wazuh. (2022). File integrity monitoring. Recuperado de https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/index.html

Kevin Beaver, C. (2018). Hacking for dummies 6ta Edición. New Jersey: John Wiley & Sons, Inc.

Singh, N., & Tripathy, S. (2024). It's too late if exfiltrate: Early stage Android ransomware detection. Computers & Security, 141, 103819. https://doi.org/10.1016/j.cose.2024.103819

Tiago Pereira, C. H. (17 de marzo de 2022). Cisco Talos. Obtenido de https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/

Görmez, Y., Arslan, H., Işık, Y. E., & Dadaş, İ. E. (2023). A User and Entity Behavior Analysis for SIEM Systems: Preprocessing of The Computer Emergency and Response Team Dataset. Journal of Soft Computing and Artificial Intelligence, 4(1), Article 1. https://doi.org/10.55195/jscai.1213782

Santos, A. T., Alex Hinchliffe, Doel. (2022, enero 27). Threat Assessment: BlackCat Ransomware. Unit 42. https://unit42.paloaltonetworks.com/blackcat-ransomware/

Smiliotopoulos, C., Barmpatsalou, K., & Kambourakis, G. (2022). Revisiting the Detection of Lateral Movement through Sysmon. Applied Sciences, 12(15), Article 15. https://doi.org/10.3390/app12157746

Wazuh. (2024). Custom database lists (CDB). https://documentation.wazuh.com/current/user-manual/ruleset/cdb-list.html

Apéndices/Anexos:

Script completo en Python para eliminación del archivo en base a la detección del SIEM:

```
        #!/usr/bin/python3
        # Copyright (C) 2015-2022, Wazuh Inc.
        # All rights reserved.

        import os
        import sys
        import json
        import datetime

        if os.name == 'nt':
            LOG_FILE = "C:\\Program Files (x86)\\ossec-agent\\active-response\\active-responses.log"
        else:
            LOG_FILE = "/var/ossec/logs/active-responses.log"

        ADD_COMMAND = 0
        DELETE_COMMAND = 1
        CONTINUE_COMMAND = 2
        ABORT_COMMAND = 3

        OS_SUCCESS = 0
        OS_INVALID = -1

        class message:
            def __init__(self):
                self.alert = ""
                self.command = 0

        def write_debug_file(ar_name, msg):
            with open(LOG_FILE, mode="a") as log_file:
                log_file.write(str(datetime.datetime.now().strftime('%Y/%m/%d %H:%M:%S')) + " " + ar_name
+ ": " + msg +"\n")

        def setup_and_check_message(argv):

            # get alert from stdin
            input_str = ""
            for line in sys.stdin:
                input_str = line
                break
            try:
                data = json.loads(input_str)
            except ValueError:
                write_debug_file(argv[0], 'Decoding JSON has failed, invalid input format')
                message.command = OS_INVALID
                return message

            message.alert = data

            command = data.get("command")

            if command == "add":
                message.command = ADD_COMMAND
            elif command == "delete":
                message.command = DELETE_COMMAND
            else:
                message.command = OS_INVALID
```

```
            write_debug_file(argv[0], 'Not valid command: ' + command)

        return message


    def send_keys_and_check_message(argv, keys):

        # build and send message with keys
        keys_msg     =     json.dumps({"version":     1,"origin":{"name":     argv[0],"module":"active-
response"},"command":"check_keys","parameters":{"keys":keys}})

        write_debug_file(argv[0], keys_msg)

        print(keys_msg)
        sys.stdout.flush()

        # read the response of previous message
        input_str = ""
        while True:
            line = sys.stdin.readline()
            if line:
                input_str = line
                break

        # write_debug_file(argv[0], input_str)

        try:
            data = json.loads(input_str)
        except ValueError:
            write_debug_file(argv[0], 'Decoding JSON has failed, invalid input format')
            return message

        action = data.get("command")

        if "continue" == action:
            ret = CONTINUE_COMMAND
        elif "abort" == action:
            ret = ABORT_COMMAND
        else:
            ret = OS_INVALID
            write_debug_file(argv[0], "Invalid value of 'command'")

        return ret

    def main(argv):

        write_debug_file(argv[0], "Started")

        # validate json and get command
        msg = setup_and_check_message(argv)

        if msg.command < 0:
            sys.exit(OS_INVALID)

        if msg.command == ADD_COMMAND:
            alert = msg.alert["parameters"]["alert"]
            keys = [alert["rule"]["id"]]
            action = send_keys_and_check_message(argv, keys)

            # if necessary, abort execution
            if action != CONTINUE_COMMAND:

                if action == ABORT_COMMAND:
```

```
                write_debug_file(argv[0], "Aborted")
                sys.exit(OS_SUCCESS)
            else:
                write_debug_file(argv[0], "Invalid command")
                sys.exit(OS_INVALID)

        try:
            os.remove(msg.alert["parameters"]["alert"]["syscheck"]["path"])
            write_debug_file(argv[0], json.dumps(msg.alert) + " Successfully removed threat")
        except OSError as error:
            write_debug_file(argv[0], json.dumps(msg.alert) + "Error removing threat")


    else:
        write_debug_file(argv[0], "Invalid command")

    write_debug_file(argv[0], "Ended")

    sys.exit(OS_SUCCESS)

if __name__ == "__main__":
    main(sys.argv)
```

Encuesta sobre la amenaza Ransomware y Solución SIEM - Ciberseguridad

Estimado participante,

Gracias por participar en esta encuesta. Su opinión es fundamental para comprender mejor la percepción de los usuarios y expertos sobre la amenaza del ransomware BlackCat y la eficacia percibida de las soluciones de SIEM

Por favor, responda las siguientes preguntas de manera sincera y completa. Sus respuestas serán tratadas de forma confidencial y se utilizarán únicamente con propósitos de investigación.

Opción Múltiple:

Información Demográfica.

Edad:

- Menor de 18 años
- 18-25 años
- 26-35 años
- 36-45 años
- 46-55 años
- 56 años o más

Área de Trabajo:

- Administración y Finanzas
- Tecnología de la Información (IT)
- Recursos Humanos
- Ventas y Marketing
- Logística
- Legal y cumplimento
- Negocios e Innovación O Otro/a

Nivel de experiencia en la ciberseguridad:

- Principiante: Tengo poco o ningún conocimiento sobre ciberseguridad y sus conceptos básicos.
- Intermedio: Tengo conocimientos básicos sobre ciberseguridad y entiendo algunos conceptos y técnicas de protección.
- Avanzado: Poseo un amplio conocimiento y experiencia en ciberseguridad,

- incluyendo la implementación de medidas de seguridad avanzadas y la gestión de incidentes.
- Experto: Soy un experto en ciberseguridad con experiencia en la protección de sistemas complejos y la mitigación de amenazas avanzadas.

Percepción sobre el Ransomware (Virus):

¿Qué considera que es un Ransomware?

- Es un tipo de malware que cifra los archivos de un sistema informático y exige un rescate para su liberación.
- Es un software antivirus utilizado para proteger los sistemas contra ataques cibernéticos.
- Es un término utilizado para describir el software que optimiza el rendimiento de un dispositivo.
- Es una técnica de seguridad utilizada para proteger los datos confidenciales de una empresa.

¿Cree que el ransomware representa una amenaza significativa para las organizaciones y usuarios?

- Si
- No
- No estoy seguro.

Un SIEM es un sistema que centraliza el almacenamiento y la interpretación de los datos relevantes de seguridad.

¿Qué tan familiarizado está con las soluciones de SIEM (Security Information and Event Management)?

- No familiarizado: Nunca he oído hablar de las soluciones de SIEM y no estoy seguro de lo que implican.
- Conocimiento básico: He escuchado sobre las soluciones de SIEM, pero no estoy completamente familiarizado con su funcionamiento y utilidad.
- Moderadamente familiarizado: Tengo un entendimiento general de las soluciones de
- SIEM y su capacidad para monitorear, detectar y responder a amenazas de seguridad.

- Altamente familiarizado: Tengo experiencia práctica en la implementación y
- utilización de soluciones de SIEM, y comprendo completamente su importancia en la gestión de la seguridad de la información.

En su opinión, ¿qué tan eficaces son las soluciones de SIEM para detectar y prevenir ataques de ransomware?

- No eficaces: Creo que las soluciones de SIEM no son efectivas para detectar ni prevenir ataques de ransomware.
- Poco eficaces: Considero que las soluciones de SIEM tienen una eficacia limitada en la detección y prevención de ataques de ransomware.
- Moderadamente eficaces: Creo que las soluciones de SIEM pueden ser útiles para detectar y prevenir algunos ataques de ransomware, pero no son infalibles.
- Altamente eficaces: Estoy convencido de que las soluciones de SIEM son altamente
- eficaces para detectar y prevenir ataques de ransomware, y representan una parte crucial de la estrategia de seguridad cibernética de una organización.
- No estoy seguro/a.

En su opinión, ¿Su empresa posee actualmente una solución de SIEM para protegerse contra amenazas de ransomware?

- Sí, nuestra empresa cuenta con una solución de SIEM implementada y activa.
- No, actualmente no tenemos una solución de SIEM para protegernos contra amenazas de ransomware.
- No estoy seguro/a.

Integración de SIEM:

¿Está integrada su solución de SIEM con otras herramientas de seguridad (por ejemplo, antivirus, firewalls, sistemas de prevención de intrusiones)?

- Sí, completamente integrada
- Parcialmente integrada
- No está integrada
- No estoy seguro/a

¿Ha ayudado una solución de SIEM a prevenir o mitigar algún ataque de ransomware en el pasado?

- Sí, ha prevenido ciertos ataques

- No hemos enfrentado ataques de ransomware
- No, no ha sido efectiva
- No poseo información