**Pre Entrega de Proyecto Final**

**Datos de las fuentes de la información**

Para la elaboración del presente informe, se han analizado las siguientes fuentes

de información:

* Informe sobre el estado actual de la empresa.
* Archivo digital de muestra del malware entregado por el equipo de soporte técnico de LexCorp.

**Análisis de Malware**

Este informe responde a la necesidad de analizar y conocer el alcance del incidente de seguridad provocada por el malware que realizo el cifrado masivo de archivos (ransomware) en la infraestructura de LexCorp afectando a equipos servidores Windows Server 2003/2012 y equipos clientes Windows 7/10, identificado del 20 al 23 de junio de 2021. Este análisis servirá para emitir las recomendaciones y mejorar la postura de ciberseguridad en la infraestructura informática y de red de LexCorp.  
Con base en las actuaciones de respuesta, los técnicos de la Corporación LexCorp tomaron las siguientes medidas de contención:

* Guardaron muestra del malware para el análisis.
* Identificaron los equipos afectados sobre el incidente y les realizaron el apagado el 23 de junio para evitar la propagación vía red del malware.
* Indagación al 90% de los empleados sobre algún correo abierto que decía tener en el asunto alguna información y posterior a la apertura esta información no estaba, o bien de algún software que se haya descargado y ejecutado (fuera de lo instalado por el área de soporte) previo al día 20 de junio 2023. **Contestación**: Ninguno descargo, ni abrió ningún correo o aplicación fuera de lo permitido.
* Confirmaron que luego del apagado de esos equipos no hay dispersión del malware por red.
* Se realizó la restauración del respaldo (a la fecha 19 de junio 2021) en algunos equipos (Solo 10% del parque informático), que contaban con procesos de copias de seguridad y que en ese momento estaban fuera de la red.
* Realizaron el relevamiento en todo el parque informático para verificar software o sistema operativo desactualizado y aplicaron todas las actualizaciones críticas y de seguridad a la fecha.
* Realizaron el clonado de equipo con las actualizaciones de software a la fecha para poner operativo la empresa al 100%.

En el resultado del análisis de malware, se ha identificado lo siguiente:

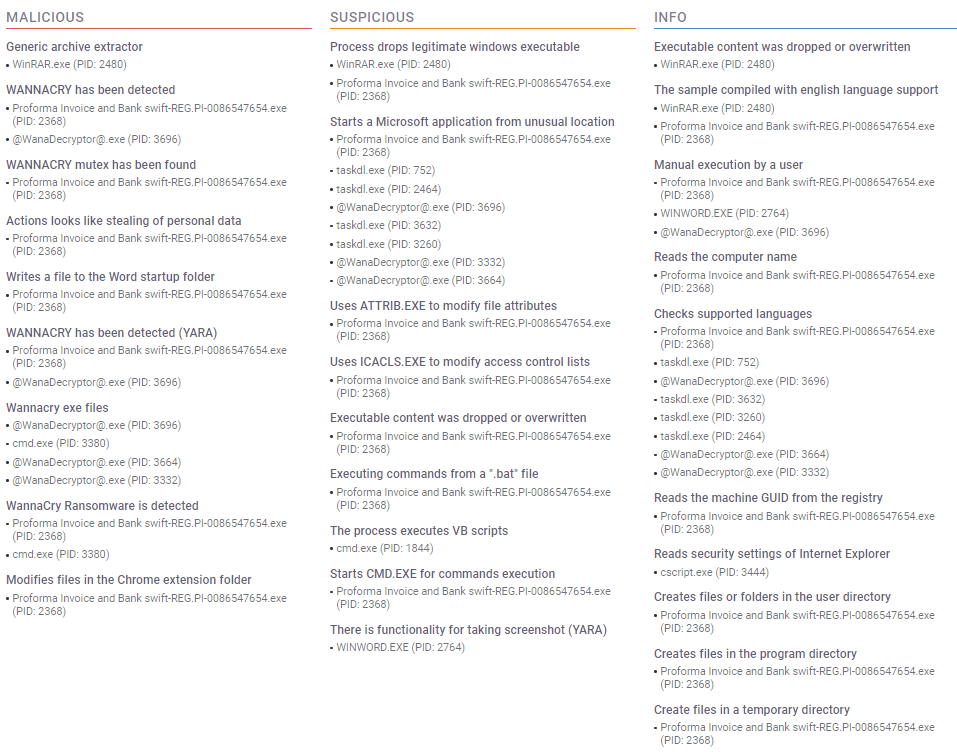
**Adicionales:**

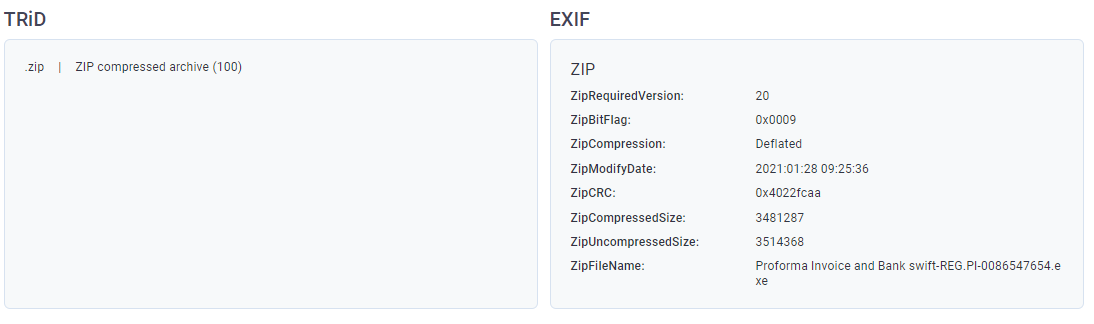
* Hasta el momento no se ha podido determinar inequívocamente la vía de entrada del ataque debido a la ausencia de fuentes de datos clave que permitan conocer el alcance completo del incidente.
* No obstante, planteo las siguientes hipótesis en base a las fuentes de información analizadas y los medios de propagación que se han realizado en estos últimos tiempos y responder “¿Por qué ocurrió lo sucedido?”:
* Un usuario abrió un correo e hizo clic a un mail con link malicioso que descargo la muestra del malware (En este caso el ransomware WannaCry).
* Descargado el archivo, ejecutó el .zip extrayendo un ejecutable que de inmediato inició procesos que permiten tener permisos para el acceso total a archivos dentro del discoel proceso de encriptación del archivo en el o los discos del equipo.
* Realizó posible movimiento lateral (escaneo de red para su propagación por red mediante protocolo SMB en su versión 1, que usa el puerto 445) a otros servidores (Servidor de archivos compartidos) ya que se comparte carpetas de toda la red.
* Ransomware ejecutó algunos mecanismos de persistencia, utilizables por el atacante, para acceder al sistema tras la consecución de su objetivo.
* Las acciones del atacante se centraron en la distribución de software malicioso en el mayor número de máquinas posibles, la recopilación de información y la desactivación de servicios de protección para facilitar la detonación final del ransomware de tipo Hive que causó el cifrado masivo de archivos.

**Analisis de Muestra analizada con Any.run y VirusTotal**

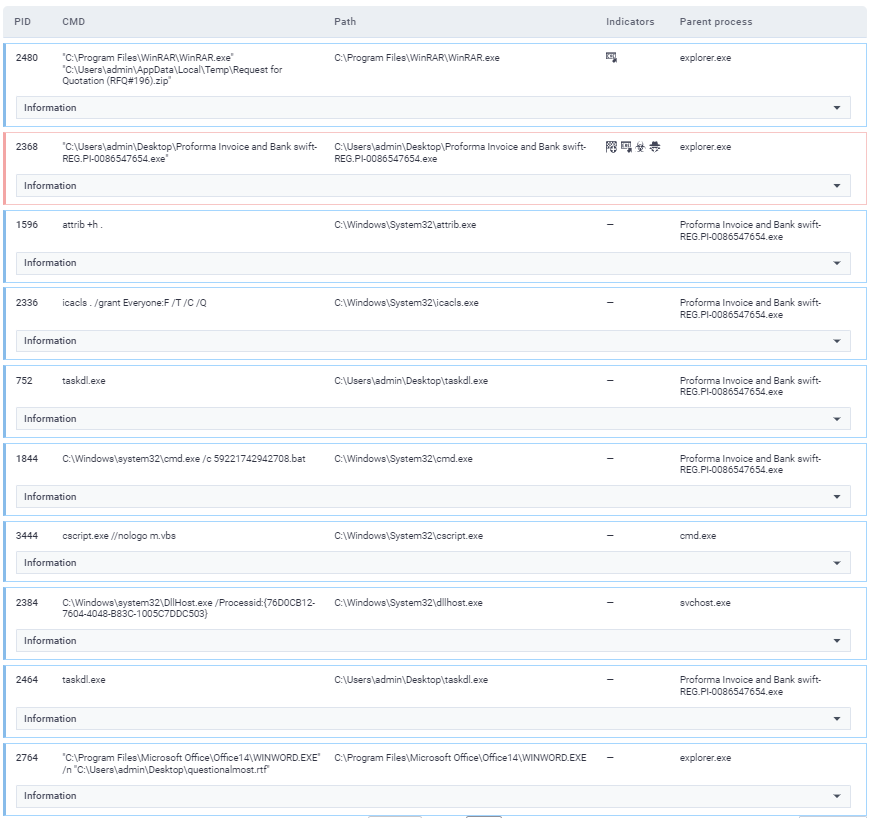
|  |  |
| --- | --- |
| Nombre del Contenedor de la Muestra | Request for Quotation (RFQ#196).zip |
| Tipo de Archivo (MIME) | Comprimido .zip (application/zip) |
| **Fecha de Análisis** | 24/06/2021 14:00hs |
| **Nombre de la Muestra** | Proforma Invoice and Bank swift-REG.PI-0086547654.exe |
| Tipo de Archivo | .EXE (PE: Portable Ejecution) |
| Tamaño | 3.32 MB (3481559 bytes) |
| **Hash MD5** | d69dc6569b385c0467185d002e252d89 |
| Hash SHA-1 | 25938a66cce0078c76a15f351cbd19c8fcc2b081 |
| Hash SHA-256 | 80239619c4ca44380c6269873a5b6b695585ccfcf278e0f2c72698658a3a6fd8 |
| **Sist. Op. Utilizado** | Windows 7 Professional Service Pack 1 (build: 7601, 32 bit) |

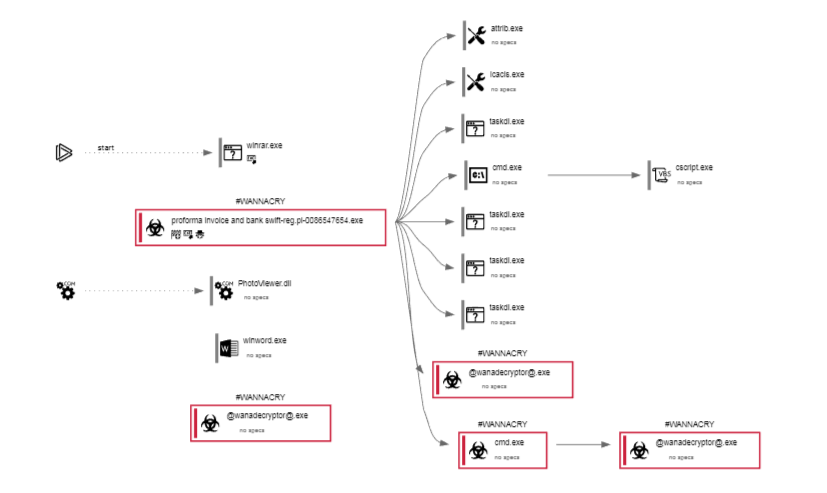
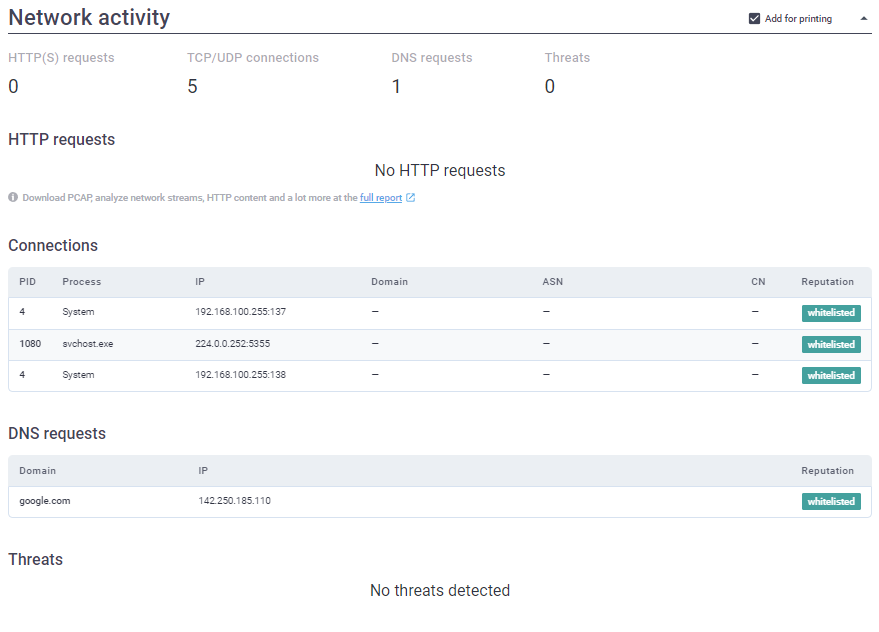
**Comportamiento:**



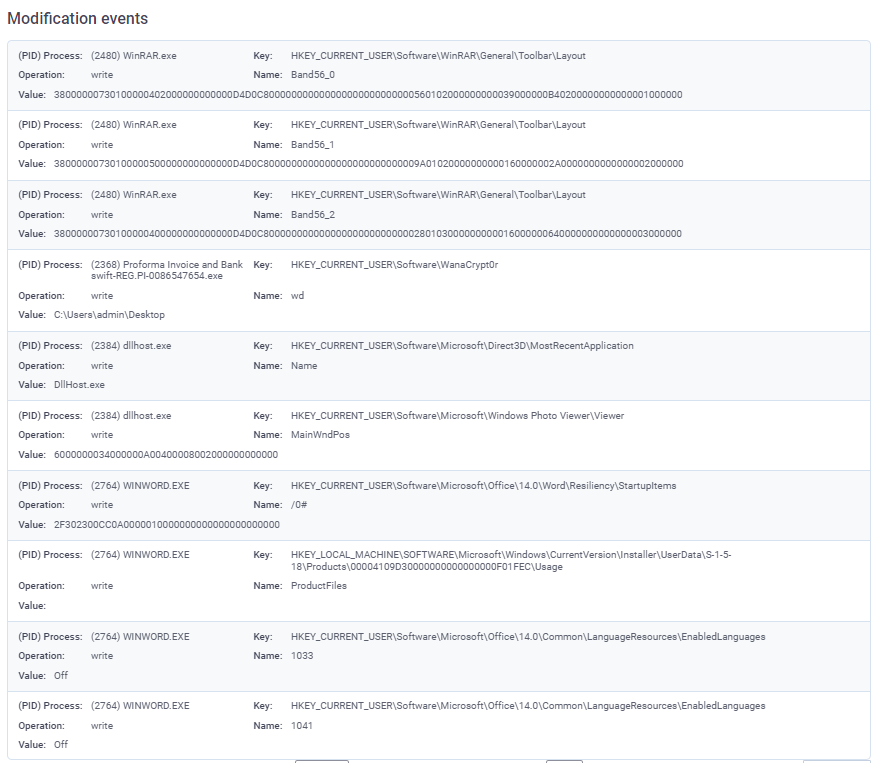
**Informacion Estatica:**

**Seguimiento del Comportamiento:**

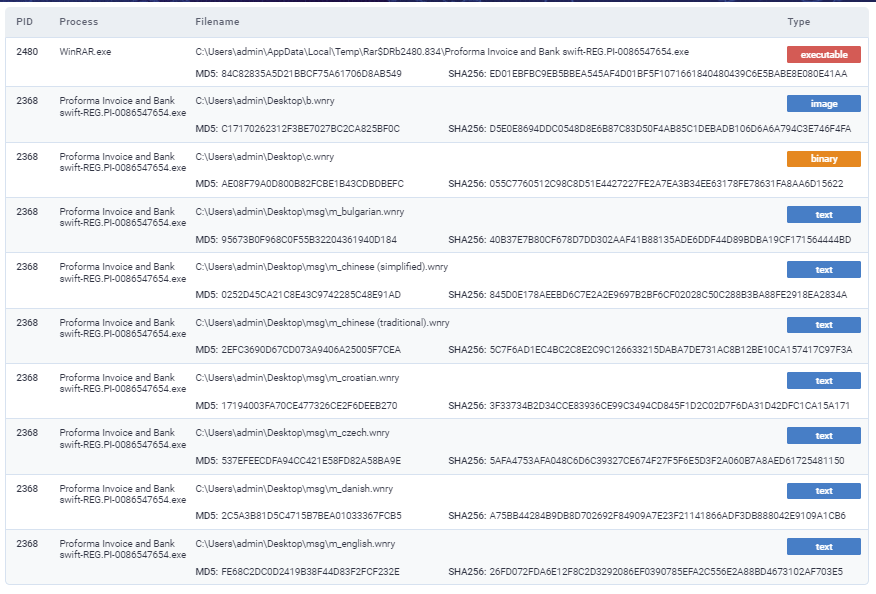


 **Actividad en la red:**

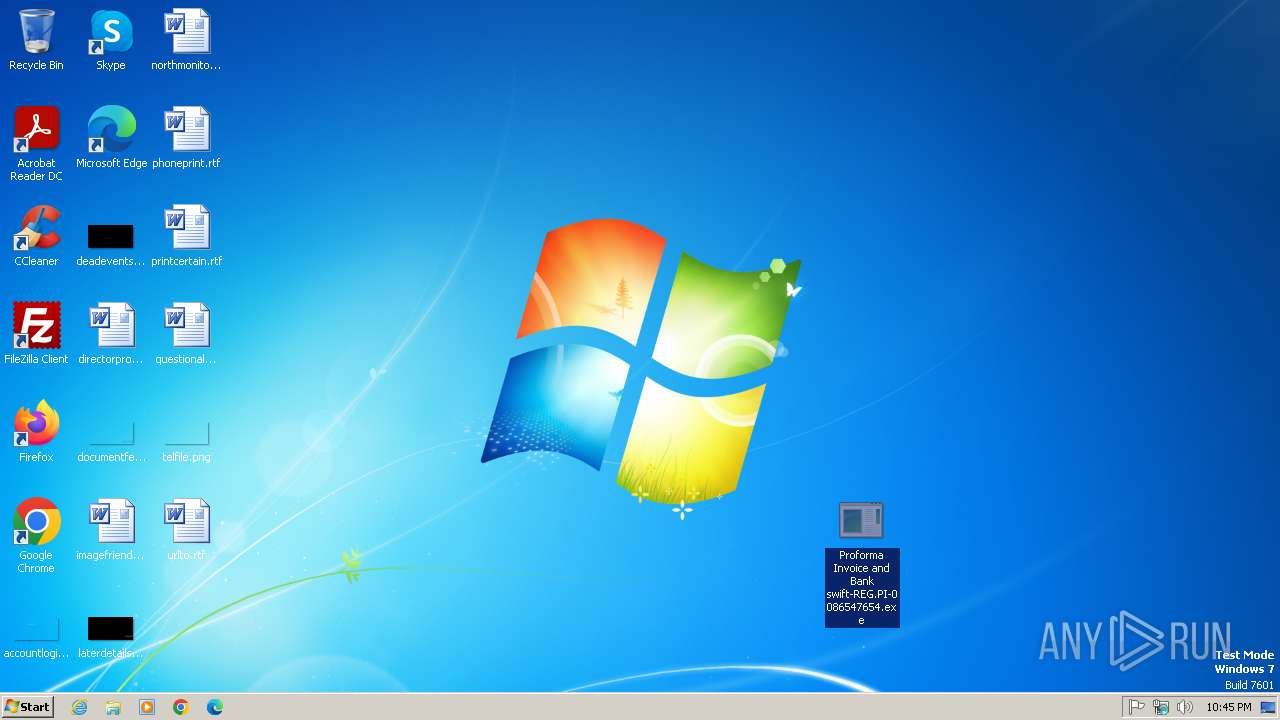
**Actividad en el Registro:**

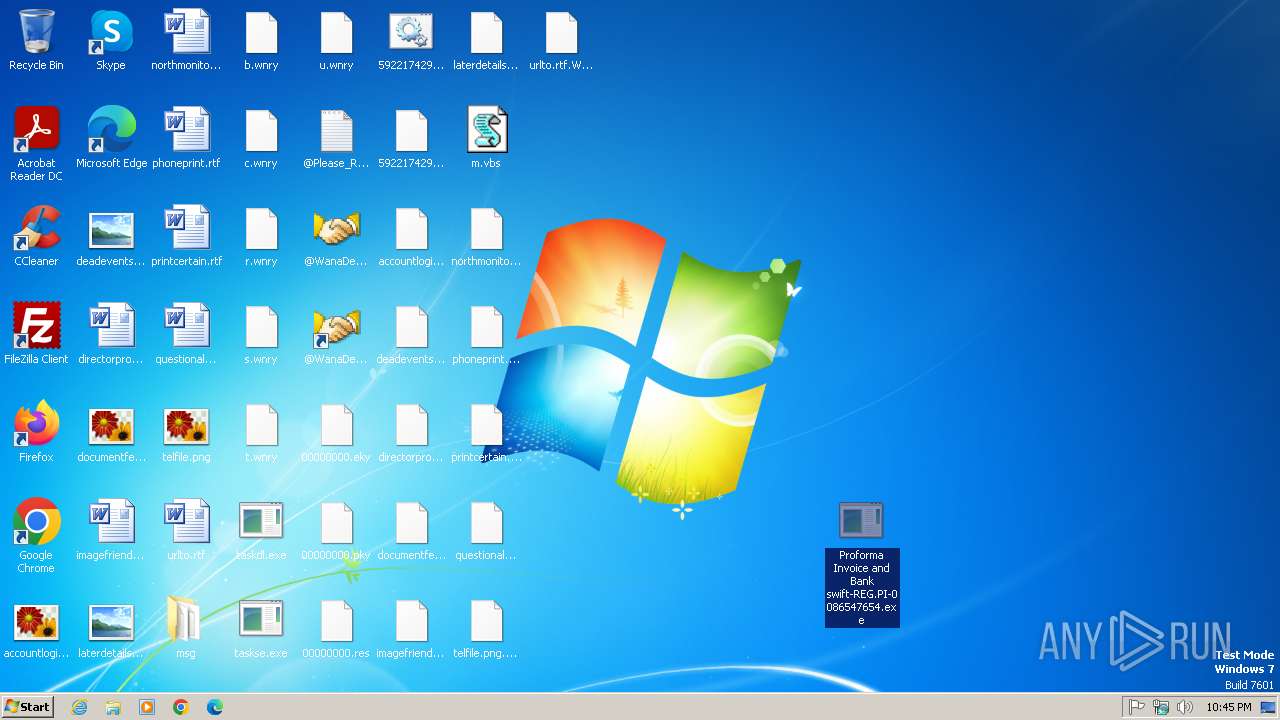


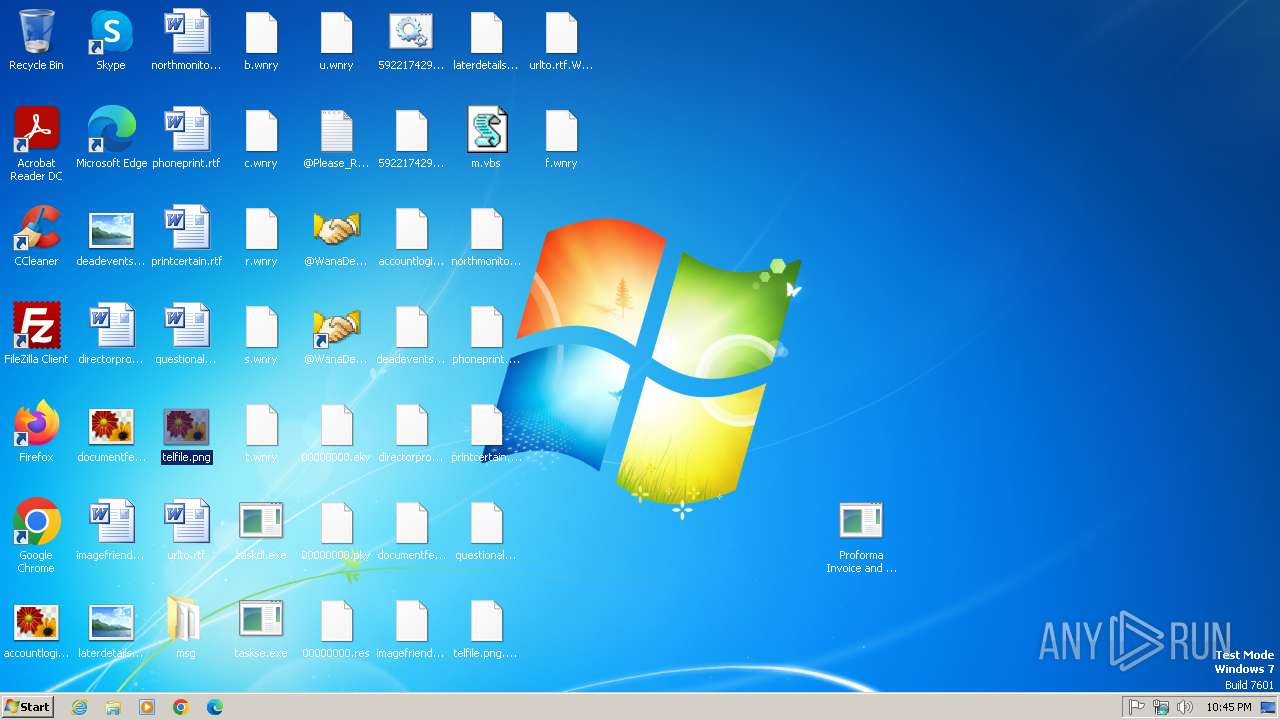
**Actividad en Sistema de Archivos:**

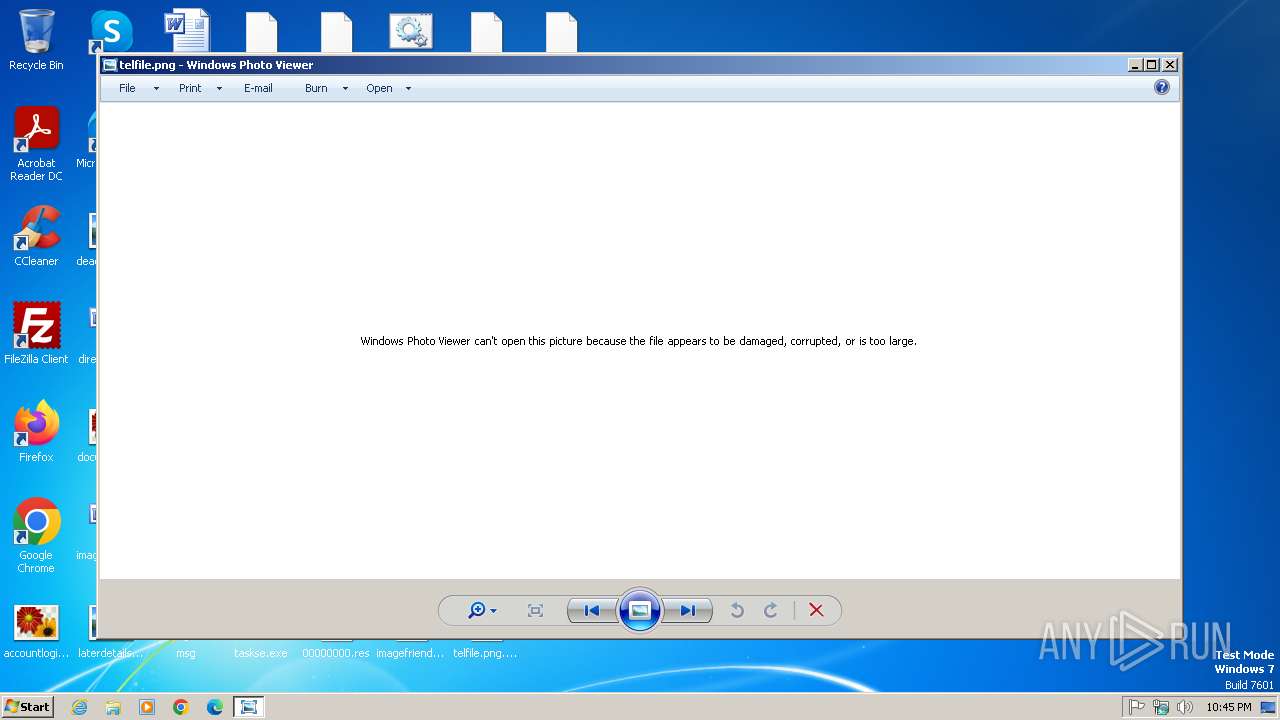


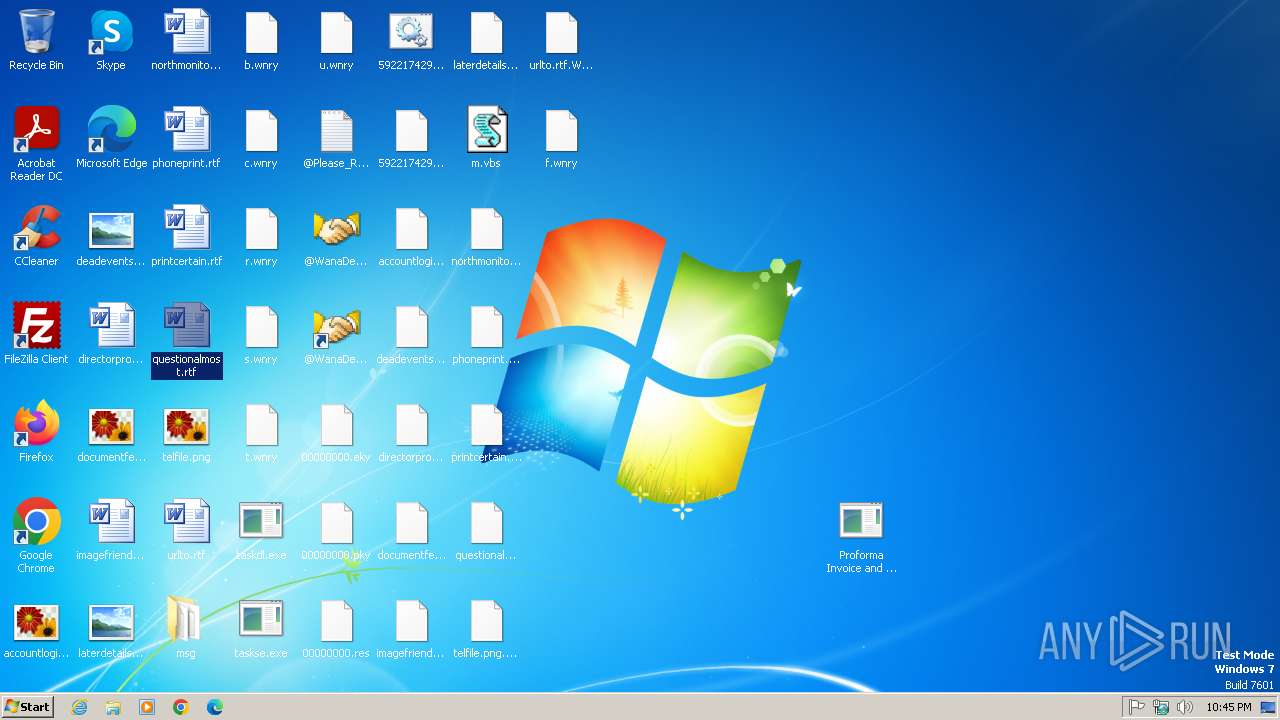
**Imágenes de Analisis:**

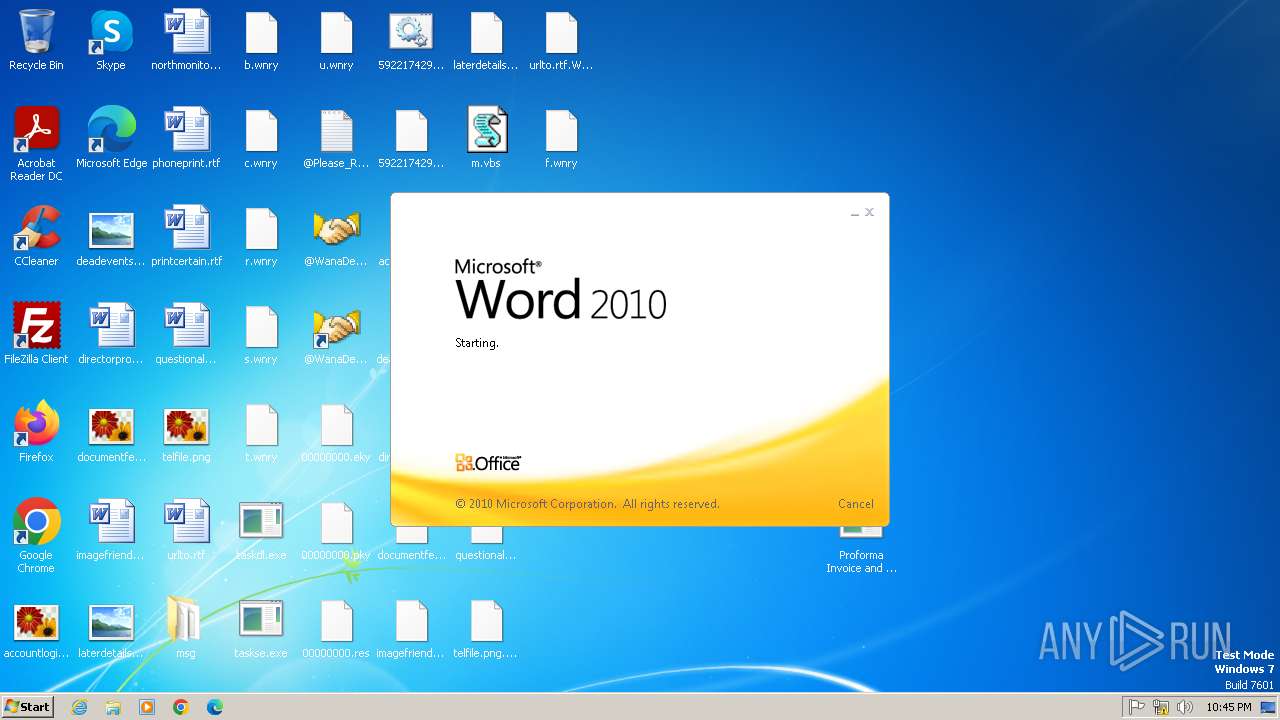


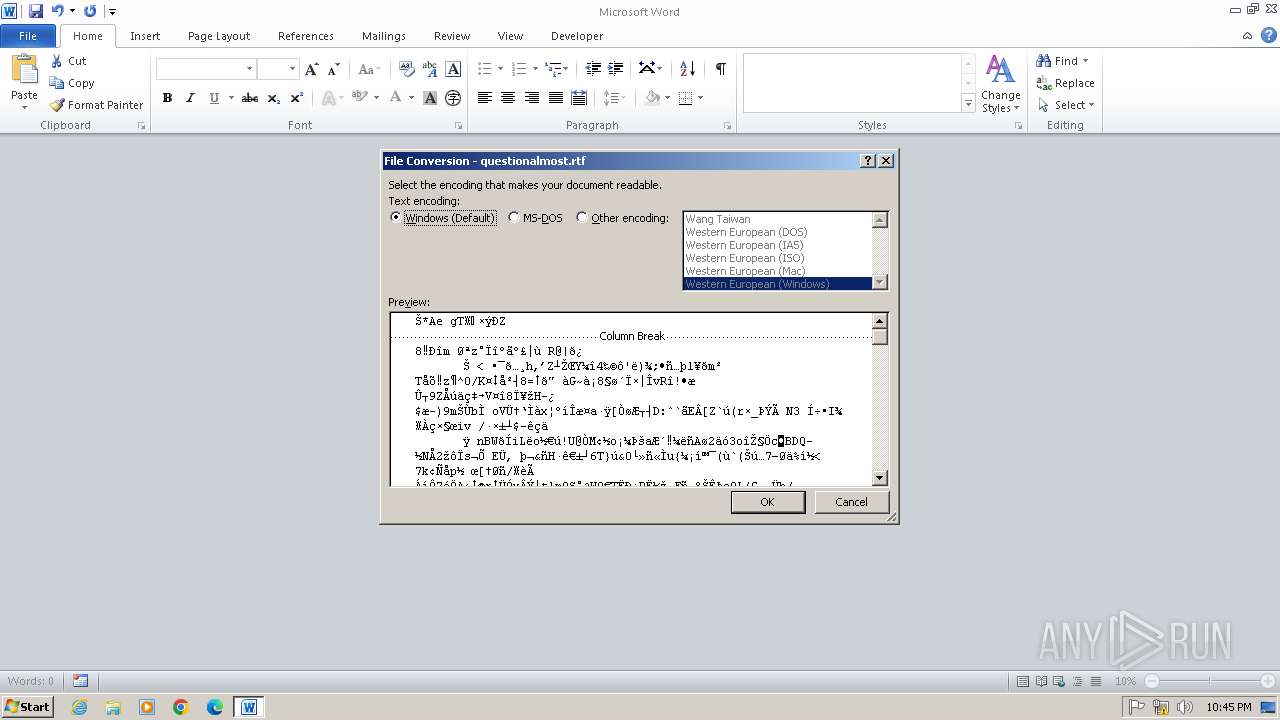














**Conclusiones**

Comportamiento del Malware: Evasion / Loader

Nombre general: WannaCry

Investigación del malware: Ransomware WannaCry

Tipo de malware: Ransomware

Información sobre WannaCry:

El ransomware WannaCry es un ransomware que se hizo ampliamente conocido en mayo de 2017 por su rápida propagación y por aprovechar vulnerabilidades críticas en sistemas Windows. Se caracteriza por combinar características de ransomware y gusano, permitiendo la infección masiva y el cifrado de datos en corto período. Infringe el daño a las organizaciones a través de las campañas de phishing.

Una vez que se obtiene acceso a una red, los actores de la amenaza se propagan lateralmente a través de toda la red mientras roban los archivos no cifrados para usarlos ante una demanda de extorsión posterior.

Cuando obtienen acceso de administrador en un controlador de dominio de Windows, implementan el ransomware sobre toda la red para lograr cifrar todos los dispositivos.

Se sabe que la banda de ransomware busca y elimina las copias de seguridad “Volume Shadow Copy” para evitar que la víctima las utilice en una rápida recuperación de los datos.

Vulnerabilidades Explotadas

EternalBlue (CVE-2017-0144):

Explota una vulnerabilidad en el protocolo SMBv1 de Windows, permitiendo la ejecución remota de código sin autenticación.

DoublePulsar:

Un troyano de puerta trasera utilizado junto con EternalBlue para instalar la carga útil de ransomware en sistemas vulnerables.

Estas vulnerabilidades permitieron que WannaCry se propagara de forma automática por redes que contaban con sistemas sin parchear.

3. Servicios, Protocolos y Puertos Afectados

SMB (Server Message Block):

Protocolo: La versión 1 (SMBv1) es la principal vía de explotación.

Puertos:

TCP 445: Es el puerto clave utilizado por SMB para la comunicación. WannaCry escanea redes en busca de sistemas con este puerto abierto.

TCP 139: Asociado a servicios NetBIOS, aunque en menor medida, también puede participar en la comunicación para compartir recursos.

Otros Servicios y Protocolos:

En ambientes donde se usan servicios de compartición de archivos sin las debidas medidas de seguridad, la propagación se facilita.

La falta de actualizaciones y la persistencia de configuraciones obsoletas incrementaron el riesgo.

4. Comportamiento del Malware

Propagación y Ejecución

Escaneo de Red:

WannaCry realiza un barrido automático en rangos de IP en busca de sistemas vulnerables mediante el puerto 445, explotando la vulnerabilidad de SMBv1.

Cifrado de Archivos:

Una vez comprometido un sistema, el malware cifra archivos utilizando algoritmos de cifrado robustos y deja una nota de rescate que solicita el pago en criptomonedas (generalmente Bitcoin).

Mecanismo de Kill Switch:

Incluye una verificación de conexión a un dominio específico. Si se logra la conexión, el ransomware se detiene, lo que en un principio ayudó a limitar su propagación.

Persistencia

Persistencia Limitada:

A diferencia de otros malware, WannaCry no se enfocó en establecer mecanismos de persistencia muy sofisticados. Su principal objetivo era propagarse rápidamente y ejecutar el cifrado de archivos.

Registro y Tareas: Algunos análisis identificaron que en ciertos casos el ransomware podría haber creado entradas en el registro o tareas programadas para reiniciarse, pero estas técnicas no eran universales ni tan robustas como las de malware diseñados para permanecer ocultos a largo plazo.

Diseño Transitorio: El diseño de WannaCry priorizaba la propagación masiva en lugar de mantenerse de forma permanente en los sistemas afectados, lo que implicaba que una vez reiniciado el equipo, es probable que no se ejecute nuevamente sin que se reexplote la vulnerabilidad.

5. Impacto en Redes y Sistemas

Velocidad de Propagación:

Su capacidad de escanear y explotar sistemas vulnerables generó una propagación exponencial en entornos sin las actualizaciones críticas (parche MS17-010).

Congestión de Red:

El escaneo masivo de puertos (especialmente el TCP 445) y la actividad de cifrado de archivos contribuyeron a congestionar redes y afectar el rendimiento de los sistemas.

Daños en Infraestructuras Críticas:

Al infectar sistemas críticos en empresas, hospitales y organismos gubernamentales, el ransomware demostró cómo la falta de actualización y el uso de protocolos obsoletos pueden generar grandes vulnerabilidades a nivel global.

6. Medidas de Mitigación y Prevención

Aplicar Parches y Actualizaciones:

Instalar el parche MS17-010 de Microsoft y otras actualizaciones de seguridad es fundamental para mitigar la vulnerabilidad de SMBv1.

Deshabilitar SMBv1:

La recomendación de Microsoft es deshabilitar SMBv1 y, en su lugar, utilizar versiones más seguras del protocolo.

Segmentación de Redes:

Implementar reglas en firewalls para bloquear el puerto TCP 445 y aislar segmentos de red críticos ayuda a limitar la propagación de ataques similares.

Monitorización y Detección:

Utilizar sistemas de detección de intrusiones (IDS) y antivirus actualizados que puedan identificar actividades anómalas, como el escaneo masivo y la ejecución de exploits.

**1. Introducción**

**El ataque en cuestión se enmarca en una de las ciberamenazas más significativas de los últimos años. Se caracteriza por la rápida propagación y la capacidad de cifrar datos en sistemas vulnerables, generando un impacto global en infraestructuras críticas. Este informe analiza los aspectos técnicos y operativos del incidente, con el objetivo de aportar claridad sobre el vector de ataque y el nivel de compromiso en los sistemas afectados.**

**2. Tipo de Malware**

**El malware analizado corresponde a un ransomware de estilo gusano. Sus características principales son:**

**Ransomware:**

**Cifrado de Archivos: Una vez que infecta un sistema, el malware procede a cifrar los archivos del usuario, dejándolo inaccesible sin el descifrado correspondiente.**

**Nota de Rescate: Tras el cifrado, se despliega una nota de rescate que exige el pago, generalmente en criptomonedas (como Bitcoin), para la recuperación de los archivos.**

**Gusano (Worm):**

**Propagación Automática: El malware explota vulnerabilidades en los sistemas para propagarse de forma autónoma a través de la red, sin intervención directa del usuario.**

**Escaneo de Red: Realiza barridos en rangos de IP para identificar y comprometer sistemas vulnerables, ampliando su impacto de forma exponencial.**

**Esta combinación de características permite que el malware no solo cause daños a nivel individual (cifrado de datos), sino que también se extienda rápidamente entre dispositivos y redes, aumentando el nivel de compromiso general.**

**3. Vector de Ataque**

**El vector de ataque principal se basa en la explotación de vulnerabilidades en el protocolo SMBv1 de Windows, concretamente:**

**Explotación de Vulnerabilidades:**

**EternalBlue (CVE-2017-0144):**

**Esta vulnerabilidad permite la ejecución remota de código en sistemas Windows a través del protocolo SMBv1. El malware utiliza este exploit para penetrar en sistemas sin aplicar autenticación, facilitando la propagación a gran escala.**

**DoublePulsar:**

**Funciona como un troyano de puerta trasera que se instala en el sistema comprometido, permitiendo la ejecución de la carga útil del ransomware de manera efectiva.**

**Servicios y Puertos Afectados:**

**SMB (Server Message Block):**

**Puerto TCP 445: Es el principal canal de comunicación utilizado para la explotación de la vulnerabilidad. El malware escanea activamente este puerto en busca de sistemas vulnerables.**

**Puerto TCP 139: Asociado a servicios NetBIOS, aunque en menor medida, también puede contribuir al proceso de propagación.**

**Proceso de Infección:**

**Escaneo de Red: El malware inicia escaneos en la red local y, en algunos casos, en redes extendidas, para identificar hosts con el puerto 445 abierto y que estén ejecutando SMBv1.**

**Explotación y Propagación: Una vez identificado un objetivo vulnerable, se ejecuta el exploit EternalBlue, seguido de la implantación del troyano DoublePulsar, que permite el cifrado de archivos y la propagación automática a otros sistemas.**

**Cifrado y Notificación: Tras el compromiso del sistema, se procede a cifrar la información y se despliega una nota de rescate informando sobre las medidas a seguir para el posible desbloqueo del sistema.**

**4. Nivel de Compromiso y Impacto**

**El incidente derivado del ataque presenta un alto nivel de compromiso en múltiples frentes:**

**Impacto en la Infraestructura:**

**Sistemas Críticos: La infección afecta sistemas esenciales en empresas, hospitales, y organismos gubernamentales, lo que puede traducirse en interrupciones significativas de servicios.**

**Congestión en la Red: El escaneo masivo y la propagación automática generan congestión en las redes, afectando la conectividad y el rendimiento global de la infraestructura.**

**Persistencia del Malware:**

**Aunque el diseño del malware no priorizaba mecanismos de persistencia sofisticados (su principal objetivo era la propagación y el cifrado rápido), algunas técnicas de persistencia mínimas (como entradas en el registro o tareas programadas) podrían haberse empleado en ciertos casos para reinfectar el sistema tras un reinicio.**

**Sin embargo, la mayoría de las infecciones dependen de la persistencia del exploit en la red, lo que significa que la reinfección puede ocurrir de forma reiterada si no se corrigen las vulnerabilidades explotadas.**

**Riesgo a Largo Plazo:**

**Reinfección: Sistemas que no aplican los parches necesarios o que mantienen habilitado SMBv1 siguen siendo vulnerables a ataques similares en el futuro.**

**Propagación Externa: La capacidad del malware para extenderse a través de redes no segmentadas incrementa el riesgo de contagio en entornos interconectados, haciendo indispensable la revisión y actualización de políticas de seguridad.**

**5. Conclusiones y Recomendaciones**

**Conclusiones:**

**El malware es un ransomware de tipo gusano que explota vulnerabilidades críticas en el protocolo SMBv1.**

**Su vector de ataque se basa en la explotación de EternalBlue y el uso del troyano DoublePulsar, permitiendo una propagación masiva y rápida.**

**El nivel de compromiso es elevado, especialmente en infraestructuras que no han aplicado las actualizaciones de seguridad necesarias, lo que facilita tanto la propagación interna como la reinfección.**

**Recomendaciones:**

**Aplicar Parches: Instalar urgentemente los parches de seguridad, en particular el parche MS17-010 de Microsoft, que soluciona la vulnerabilidad explotada.**

**Deshabilitar SMBv1: Migrar a versiones más seguras del protocolo SMB o desactivar SMBv1 en todos los sistemas.**

**Segmentación de Red: Implementar una segmentación de red eficaz y aplicar reglas estrictas en el firewall para bloquear el tráfico no autorizado en el puerto TCP 445.**

**Monitorización y Detección: Establecer sistemas de detección de intrusiones (IDS/IPS) y soluciones antivirus actualizadas que puedan identificar comportamientos anómalos.**

**Concienciación y Formación: Capacitar al personal en prácticas de ciberseguridad, haciendo hincapié en la importancia de mantener los sistemas actualizados y en la identificación temprana de comportamientos sospechosos.**

**Recomendación**

**buscar mail malicioso y borrarlo del buzon de correo**

**capacitar para que antes de abrir un correo verifiquen el origen, si tienen duda enviar un correo nuevo informando si se envio ese mail. Comprobar los enlaces de correo.**