**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.

* Informe del estado actual informático.
* 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 en este incidente y les realizaron el apagado el día 23 de junio para evitar la propagación vía red del malware.
* Indagación al 89% de los empleados sobre si recibieron algún correo que decía tener en el asunto alguna información y posterior a la apertura de esta ¡, la 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 dichos respaldos estaban fuera de la red en ese momento.
* 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 dinámico del malware, se ha identificado lo siguiente:

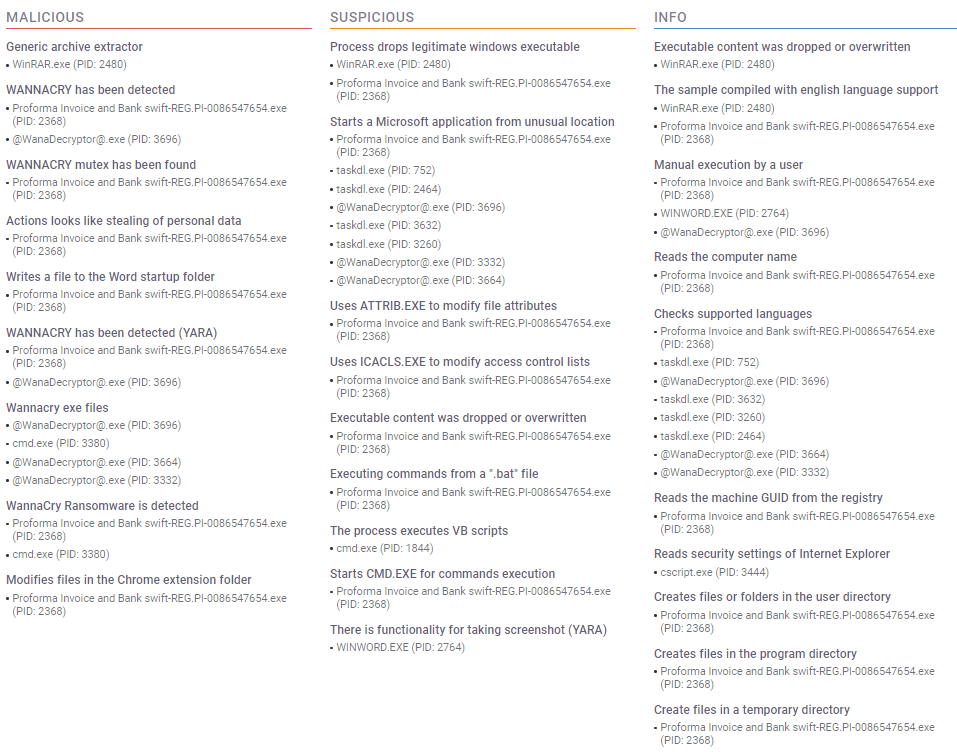
* Hasta el momento no se ha podido determinar inequívocamente la vía de entrada del ataque debido a la ausencia de fuentes de datos clave que permitan conocer el alcance completo del incidente.
* No obstante, planteo las siguientes hipótesis en base a las fuentes de información analizadas y los medios de propagación que se han realizado en estos últimos tiempos y a responder **“¿Por qué ocurrió lo sucedido?”:**
* Un usuario abrió un correo e hizo clic a un mail con link malicioso que descargo el malware (En este caso el ransomware WannaCry).
* Descargado el archivo, ejecutó el archivo comprimido .zip (en adjuntos de correo electrónico no se permiten adjuntar los archivos .exe directamente) extrayendo un ejecutable “Proforma Invoice and Bank swift-REG.PI-0086547654.exe” (.exe) que de inmediato inició procesos:
  + 1. Ocultar archivos maliciosos.
  + 2. Obtener permisos de acceso total a archivos dentro del disco.
  + 3. Eliminar archivos temporales que se crearon durante el proceso de cifrado.
  + 4. Ejecución de script de archivo por lotes .bat en modo silencioso para detectar si existe y luego eliminar toda copia de seguridad de volumenes “Volume Shadow Copy” en los discos.
  + 5. Este mismo .bat ejecuta un script de visual script .vbs en modo silencioso para la creación de un enlace al archivo ejecutable del malware en el escritorio del usuario apuntando al ejecutable malicioso para luego dar el inicio de este ejecutable con el argumento “co” en el ejecutable y así iniciar el proceso de encriptación de archivos en el o los discos del equipo.
  + 6. El malware realizó el escaneo de red buscando **equipos vulnerables para lograr la propagación por red mediante protocolo SMB versión 1, que usa el puerto 445 logrando así el movimiento lateral a otros servidores** (Servidor de archivos compartidos) ya que se comparte carpetas de toda la red.
  + 7. El malware Ransomware ejecutó algunos mecanismos de persistencia, utilizables por el atacante. En registro de windows y en disco 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 WannaCry que causó el cifrado masivo de archivos.

**Informe sobre el análisis de la muestra analizada con Any.run y VirusTotal**

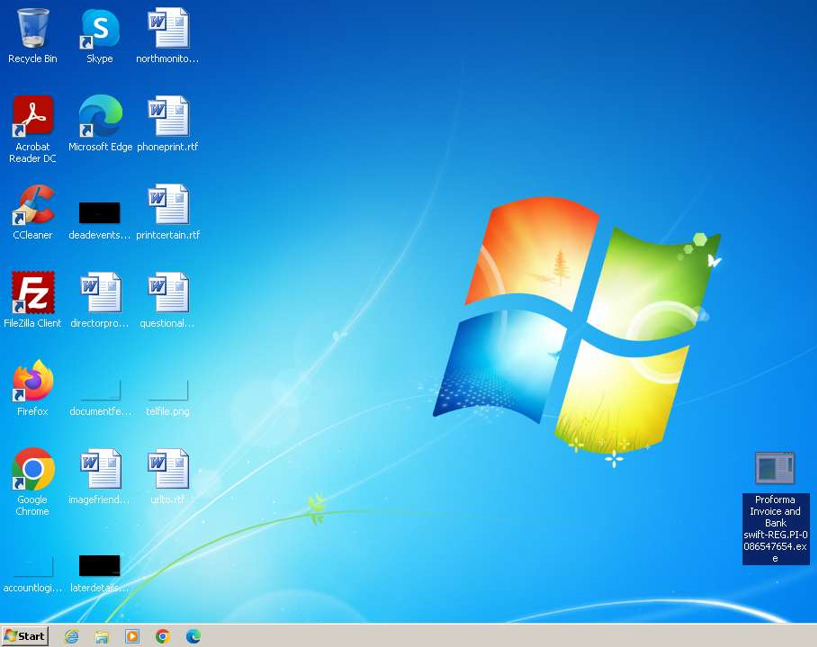
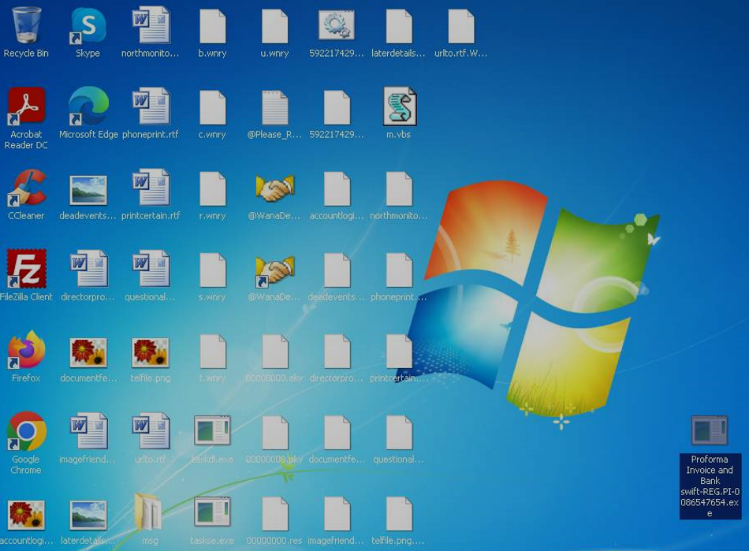
|  |  |
| --- | --- |
| **Nombre de la Muestra** | Proforma Invoice and Bank swift-REG.PI-0086547654.exe |
| **Fecha de Análisis** | 25 de marzo de 2025 a las 19:44:45 |
| **Hash MD5** | d69dc6569b385c0467185d002e252d89 |
| **Sist. Op. Utilizado** | Windows 7 Professional Service Pack 1 (build: 7601, 32 bit) |

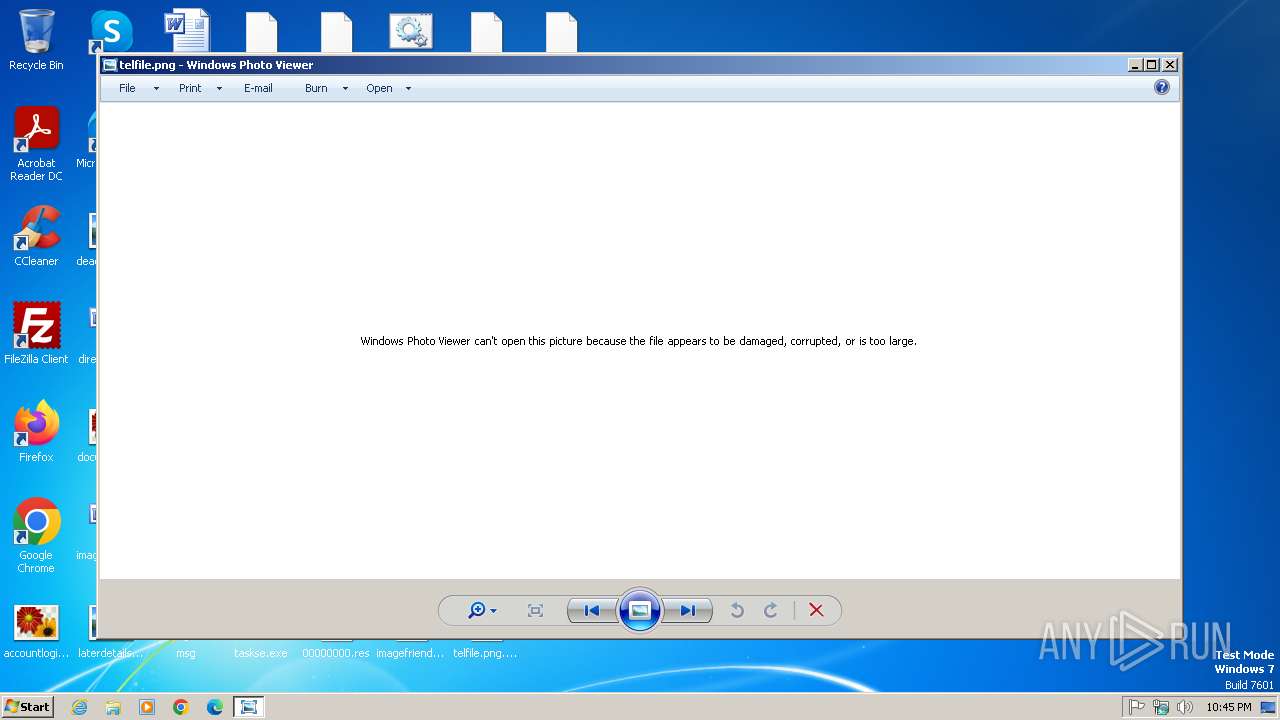
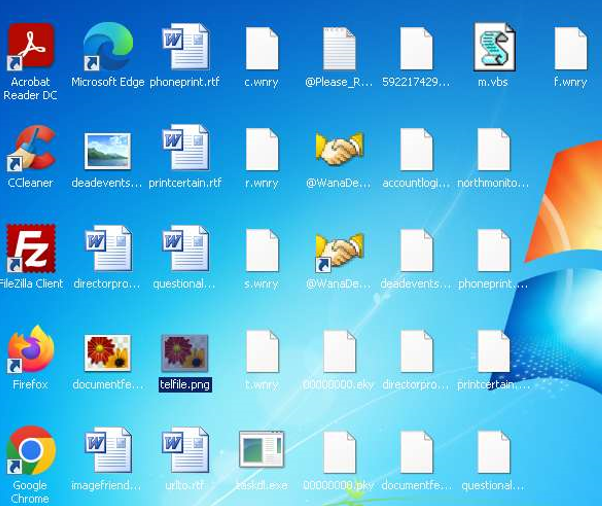
**Información Estática:  
**

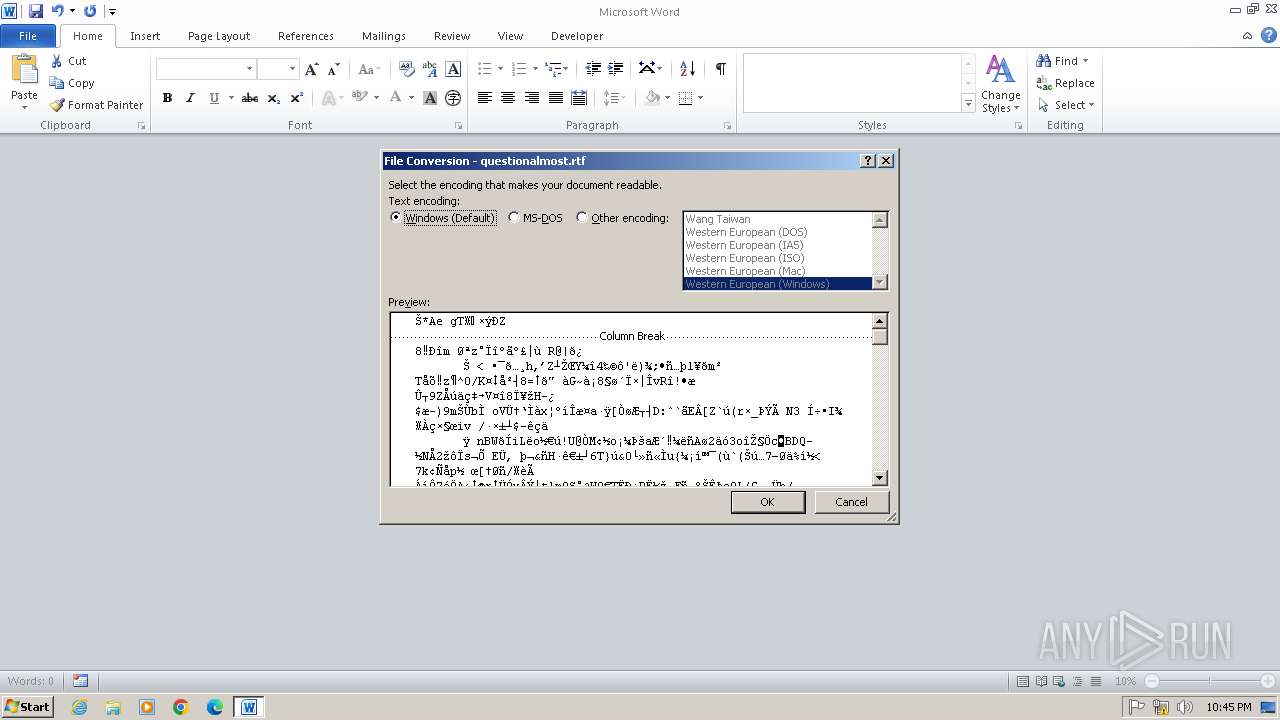
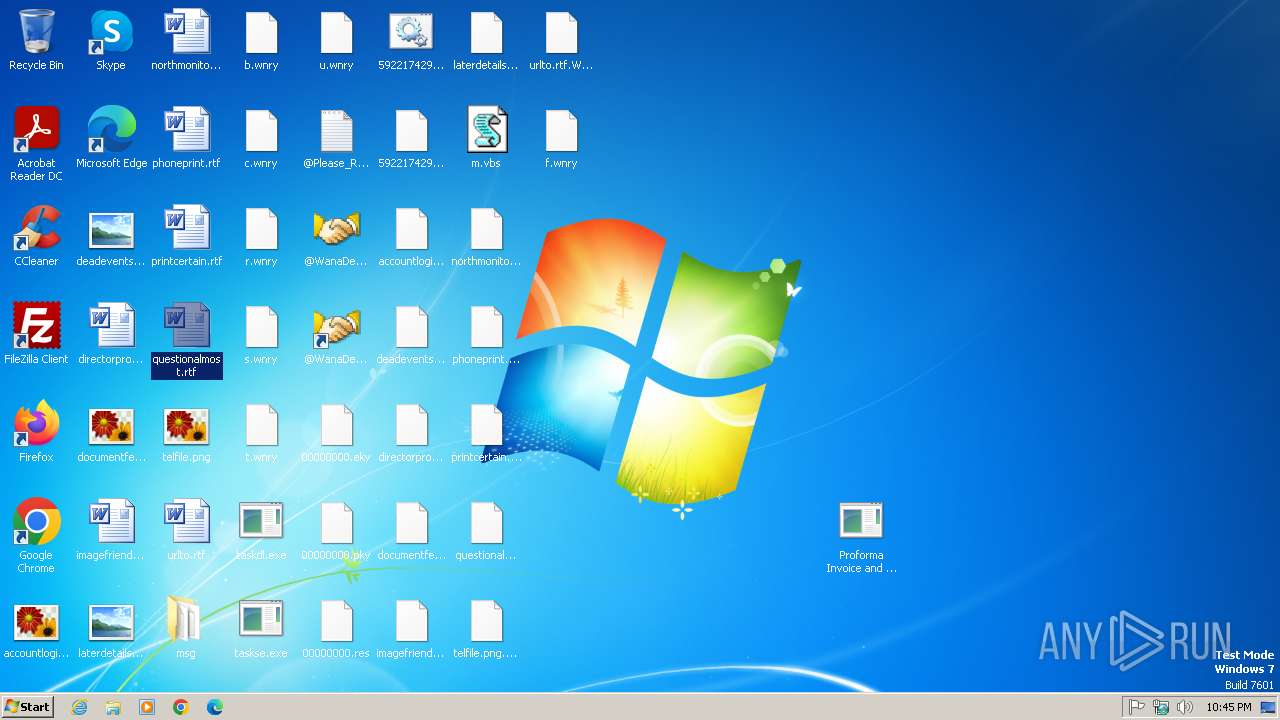
**Comportamiento:**



**Imágenes de Simulación para el análisis:**

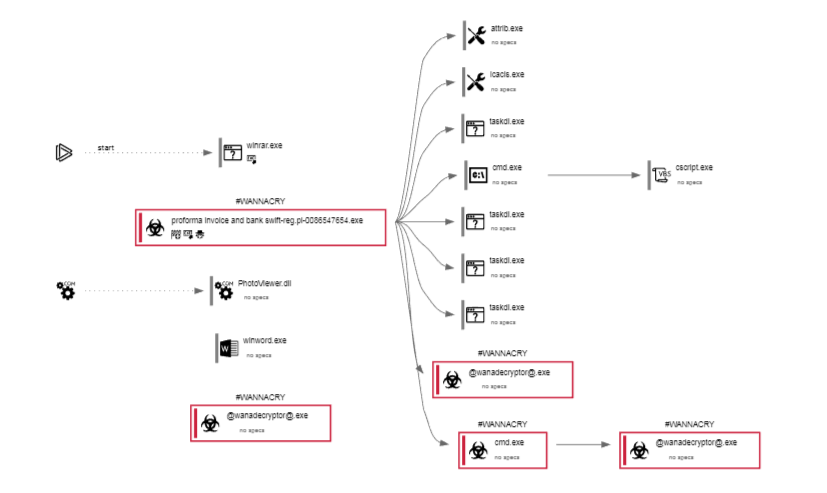
** **





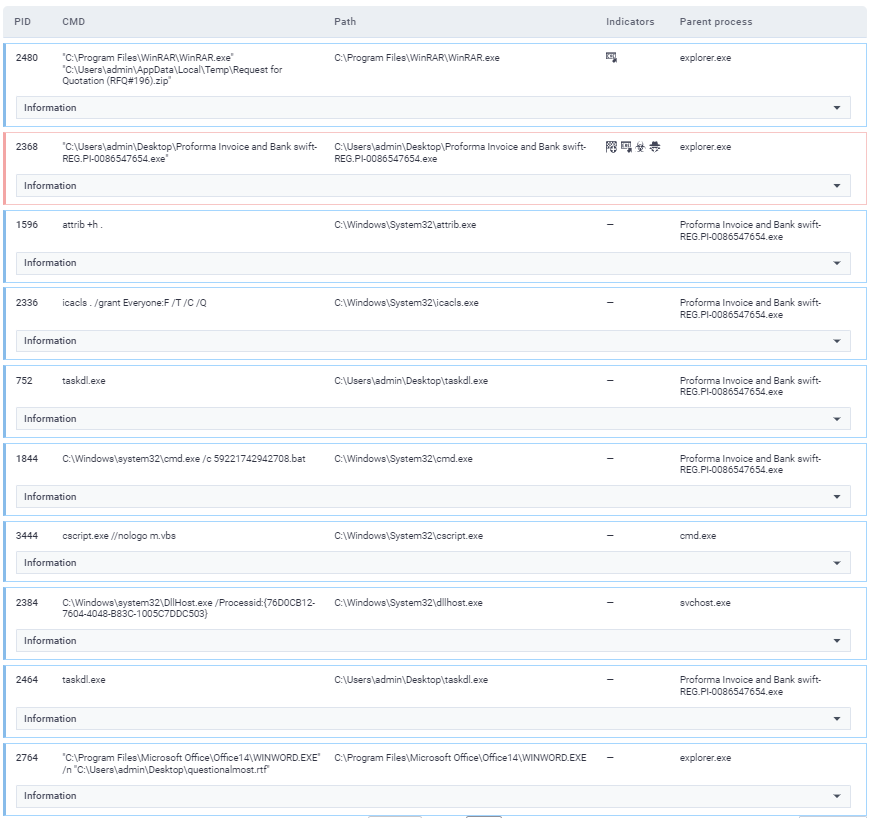


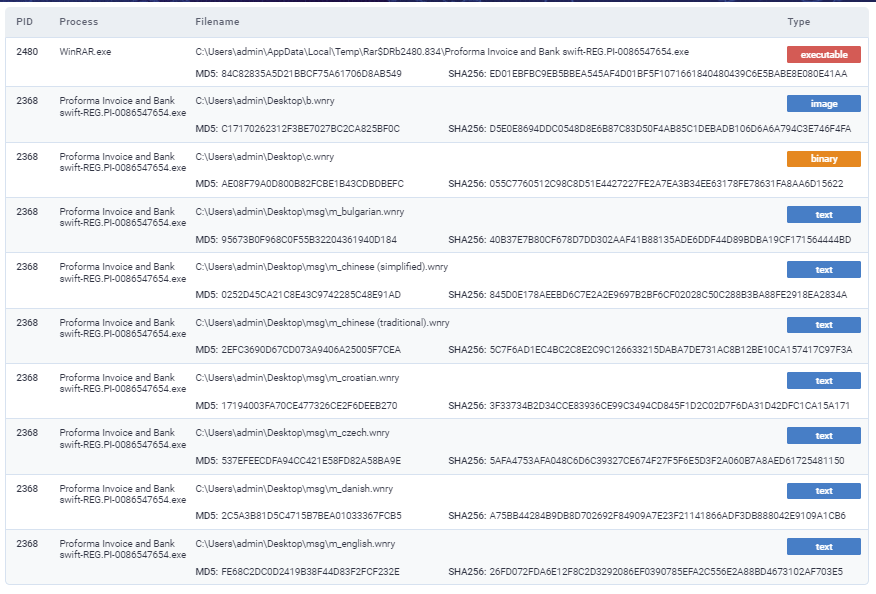
**Diagrama de procesos del comportamiento**

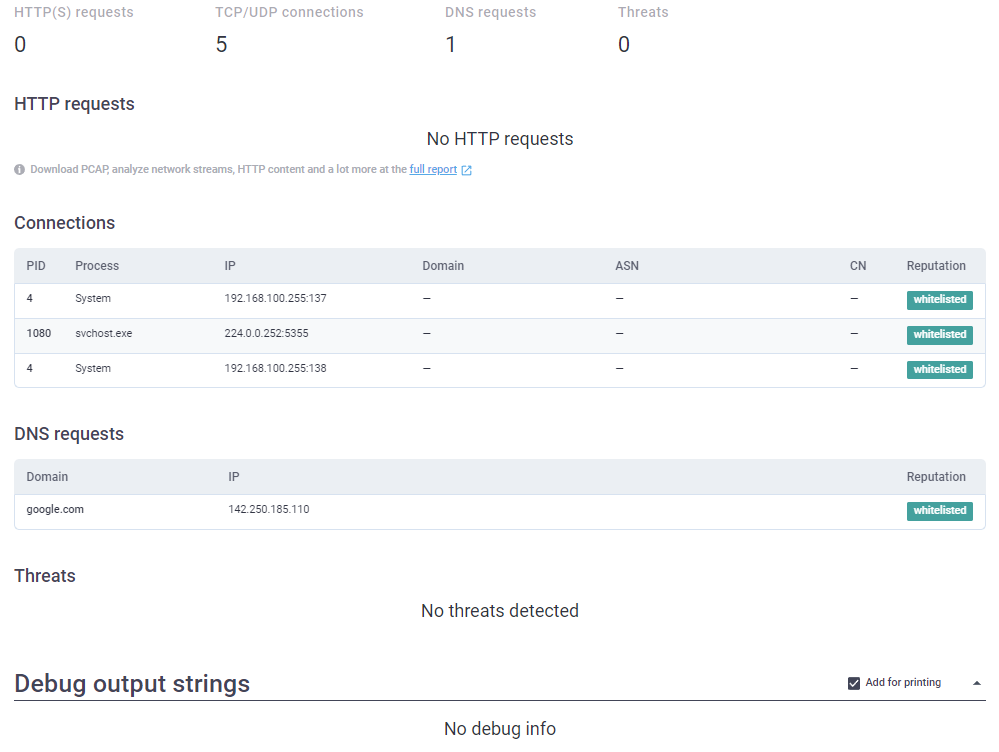


**Eventos del Comportamiento:**

****





**Actividad en la red:**

**Conclusiones**

**Comportamiento del Malware:** WannaCry combina las características de ransomware y gusano, lo que le permite cifrar archivos y propagarse rápidamente de manera masiva mediante la explotación de vulnerabilidades críticas en el protocolo SMBv1 en Sistemas Windows que no tenían aplicado el parche de seguridad para SMBv1. Dispone de poca persistencia. Infringe el daño a las organizaciones a través de las campañas de phishing. Busca y elimina las copias de seguridad “Volume Shadow Copy” para evitar que la víctima las utilice en una rápida recuperación de los datos. La amenaza se propaga 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 detectó que en el binario del malware contiene un mecanismo Kill Switch para limitar su propagación.

**Nombre general**: WannaCry, **Otros**: RansomWare, Other:Malware-gen [Trj], W32/WannaCryptor.6F87!tr.ransom, Artemis!Trojan, Trojan.Win32.Ransom.eoptnj

**Investigación del malware:** Se ha realizado extensas investigaciones, identificando como vector de ataque las vulnerabilidades críticas como EternalBlue (CVE-2017-0144) y técnicas como el uso de DoublePulsar. Se ha profundizado en el análisis de sus mecanismos de propagación, cifrado y limitadas técnicas de persistencia, permitiendo establecer medidas de mitigación y prevención.

**Tipo de malware:** Se clasifica como un ransomware con comportamiento de gusano, diseñado para atacar redes sin intervención humana directa, cifrar datos críticos y exigir rescate para su liberación.

**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/IPS) y antivirus actualizados que puedan identificar actividades anómalas, como el escaneo masivo y la ejecución de exploits.

**Sistema Antivirus:** Disponer de una solución de Antivirus y malware que siempre este actualizada a la fecha.

**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.

**Acción Recomendada:** Eenviar correo de carácter prioritario a todas las gerencias de la corporación para intentar buscar en las casillas de correo algún adjunto que sea el malware, para identificar la causa de este incidente, eliminarlo y notificar a los usuarios si detectan este correo, inmediatamente avisar a soporte y eliminarlo.