**Pre Entrega de Proyecto Final**

**Dato fuente de la información**

**Para la elaboración del presente informe, han sido analizadas las siguientes fuentes**

**de información:**

**● Informe de estatus de situación actual**

**● Muestra de malware entregado por el equipo de soporte técnico de**

**Corporación Acme**

**Análisis de Malware**

**El presente informe responde a la necesidad de conocer el alcance del incidente de**

**seguridad provocado por el cifrado masivo de archivos (ransomware) en la**

**infraestructura de LexCorp, identificado del 20 al 23 de junio de 2021. Con base en**

**las actuaciones de respuesta, los técnicos de Corporación Acme tomaron las**

**medidas de contención que consideraron necesarias y llevaron a cabo la**

**restauración de los sistemas afectados por el ataque. Como resultado del análisis**

**de malware, se ha identificado lo siguiente:**

**Adicionales:**

**➔ 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:**

**◆ Un usuario abrió un correo e hizo click a un mail con link malicioso que**

**descargo la muestra del malware (En este caso un ransomware)**

**◆ Descargado el archivo, ejecutó el .zip explotando el archivo que de**

**inmediato inició el proceso de encriptación.**

**◆ Realizó posible movimiento lateral a otros servidores (Servidor de**

**archivos comportartidos) 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.**

**Muestra analizada con Any.run**