**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 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.
* En las máquinas que disponían de copia de seguridad (back up), se restauraron al estado del día 19 de junio (fecha de último back up disponible previo al ataque). Solo un 10% del Parque contaba con back up.
* El 24 de junio, **LexCorp** solicita los servicios de un analista de ciberseguridad para analizar una muestra y emitir recomendaciones para su infraestructura de red y mejorar su postura de ciberseguridad.
* **LexCorp** solicita la elaboración de un informe de análisis del ataque, que tipo de malware es y el vector de ataque para aportar más detalles sobre el incidente y el nivel de compromiso derivado del mismo.

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

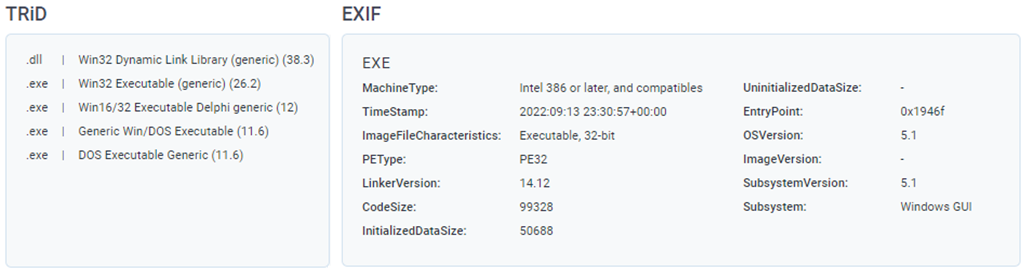
* Hasta el momento no se ha podido determinar inequívocamente la vía de entrada del ataque debido a la ausencia de fuentes de datos clave que permitan conocer el alcance completo del incidente.
* No obstante, planteo las siguientes hipótesis en base a las fuentes de información analizadas y los medios de propagación que se han realizado en estos últimos tiempos y a responder **“¿Por qué ocurrió lo sucedido?”.**

**“¿Por qué ocurrió lo sucedido?”:**

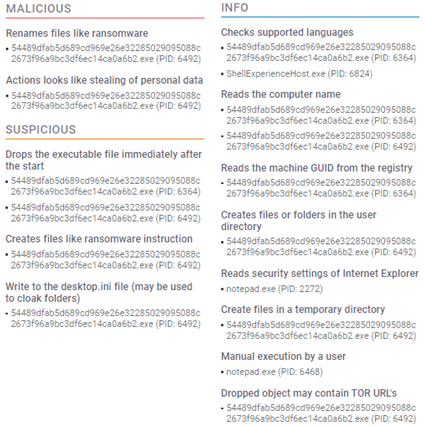
* Un usuario abrió un correo e hizo clic a un mail con link malicioso que descargo el malware (En este caso el ransomware LockBit).
* Descargado el archivo en carpeta de temporales del usuario (“**C:\Users\{UserName}\AppData\Local\Temp\**”), se ejecutó el malware ("**54489dfab5d689cd969e26e32285029095088c2673f96a9bc3df6ec14ca0a6b2.exe**“), que de inmediato inició los procesos para asignar permisos elevados en el sistema, desactivar programas de seguridad (Contrafuegos, AntiVirus, etc), de recuperación del sistema (Restauración de Sistema, Copia de Seguridad de Volumen (Volumen Shadow Copy)) y posteriormente inicia el proceso de encriptado en todas las unidades escribibles en el equipo.
* Una vez que el malware LockBit está ejecutándose en el equipo de la red, realiza todas las tareas necesarias para distribuirse por la red y completar la configuración del ataque. Utiliza herramientas de "pos explotación" para obtener privilegios escalonados, lograr el nivel de acceso necesario para lanzar los ataques y realizar movimiento lateral para examinar la viabilidad de distribuirse en otros objetivos, como servidores de archivos.
* El malware ejecutó mecanismos de persistencia utilizables por el atacante (Registro de Windows y Sistema de archivos) para acceder al sistema tras la consecución de su objetivo.
* Las acciones del atacante se centraron en la distribución del malware 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 Lockbit que causó el cifrado masivo de archivos.

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

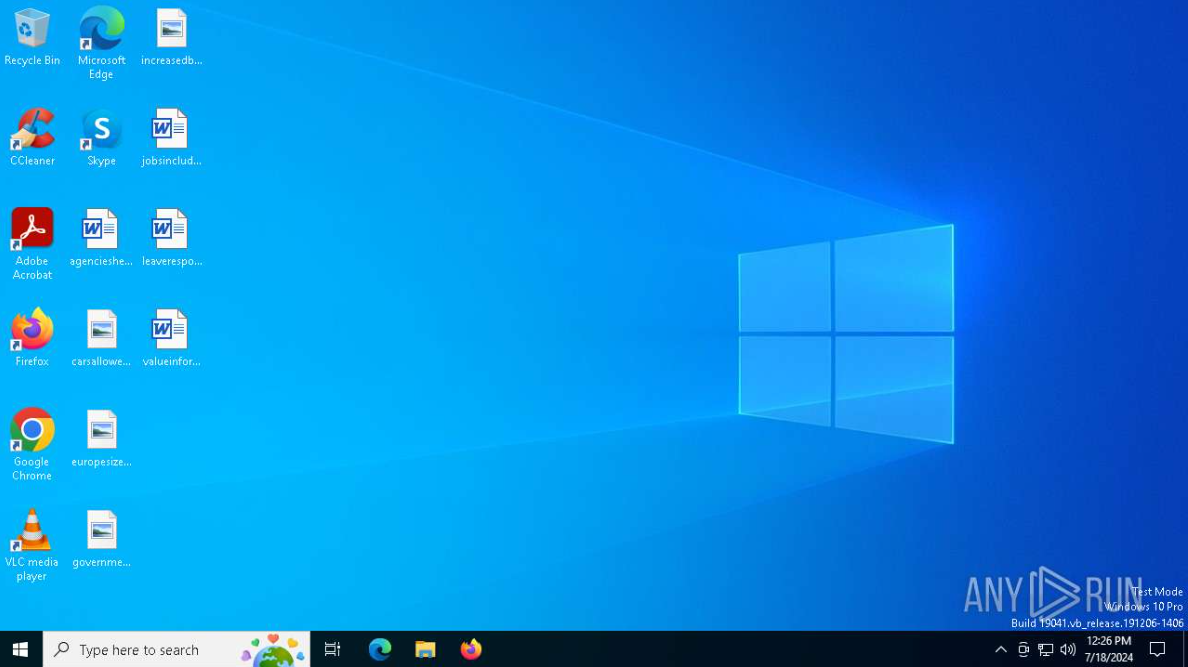
|  |  |
| --- | --- |
| **Nombre de la Muestra** | 54489dfab5d689cd969e26e32285029095088c2673f96a9bc3df6ec14ca0a6b2.exe |
| **Fecha de Análisis** | 16 de Agosto de 2024 a las 02:44 |
| **Hash MD5** | 013ed22a28eca6d06219da1d6fdc1c2b |
| **Tipo** | Ransomware. Lockbit |
| **Sist. Op. Utilizado** | Windows 10 Professional (build: 19045, 64 bit) |

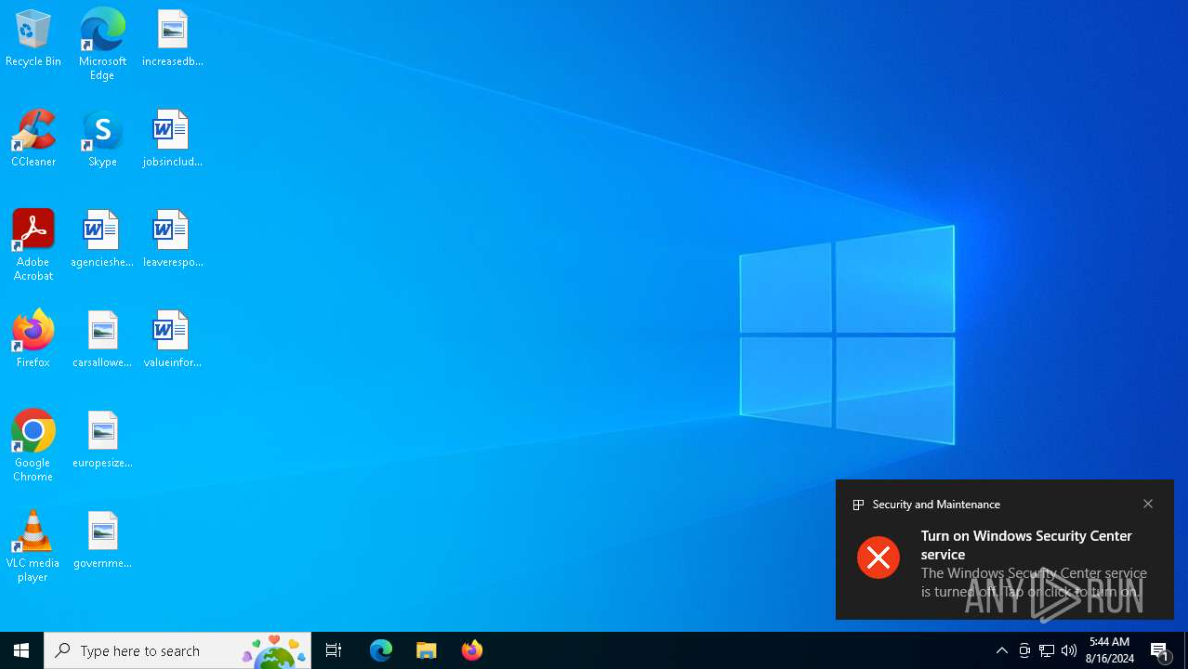
**Información Estática:  
**

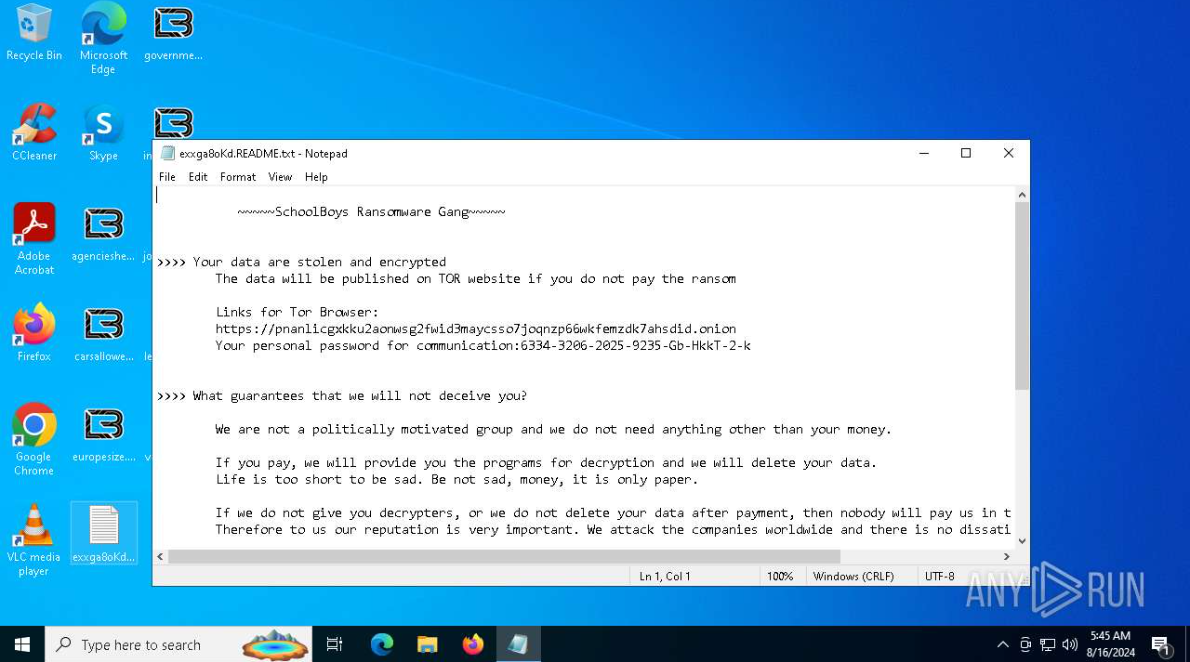
**Comportamiento:**

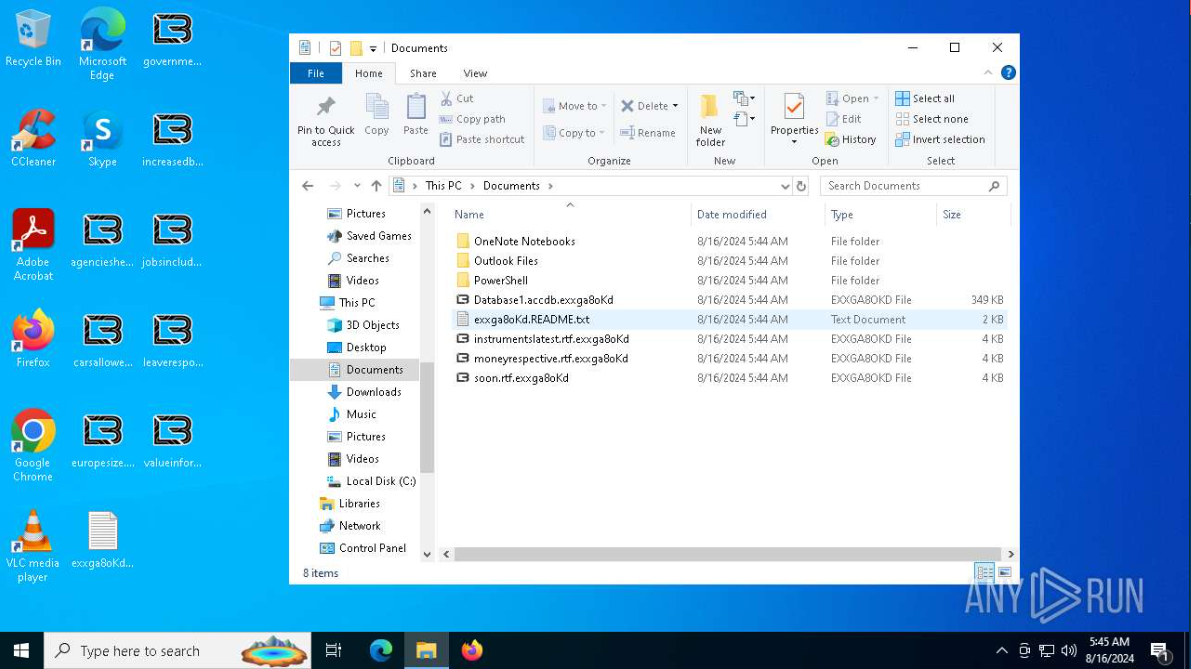
****

**Imágenes de Simulación para el análisis:**

****

****

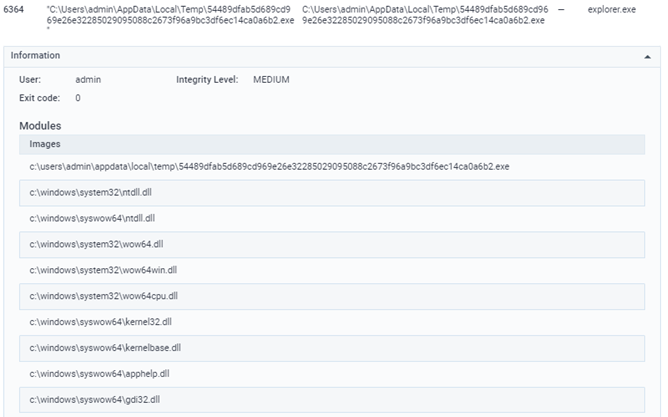
****

****

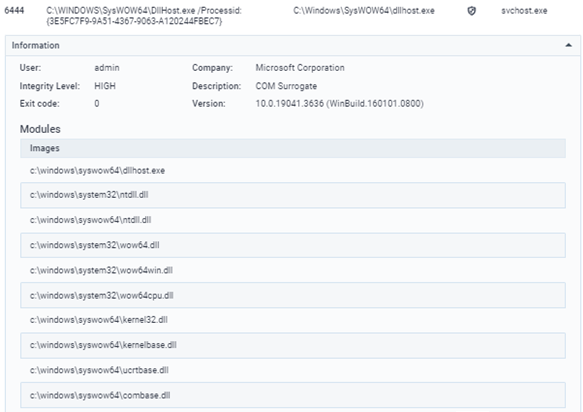
**Diagrama de procesos del comportamiento**

****

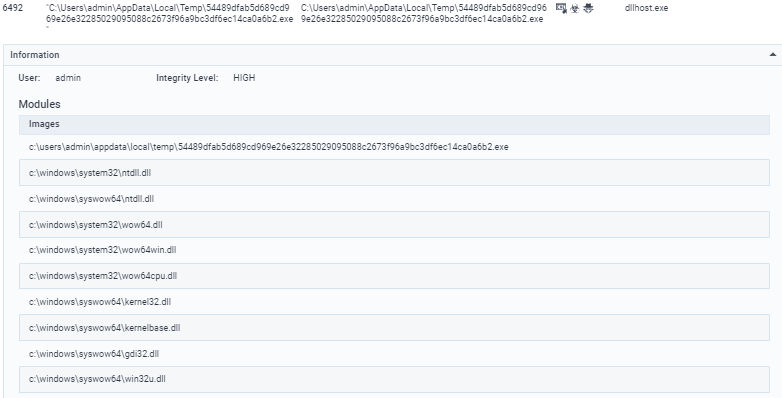
**Eventos del Comportamiento:**

****

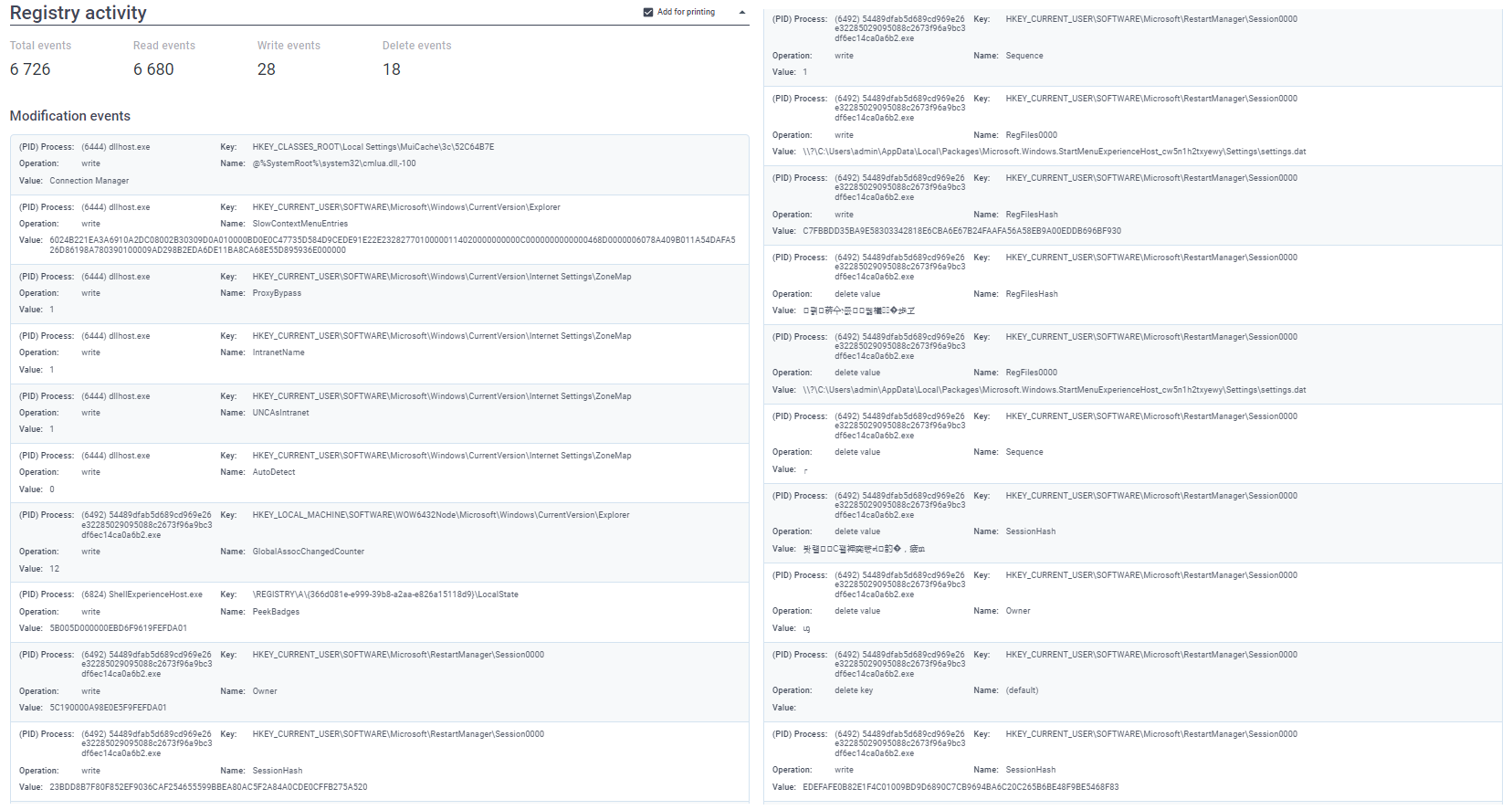
**1**. Ejecución del malware

****

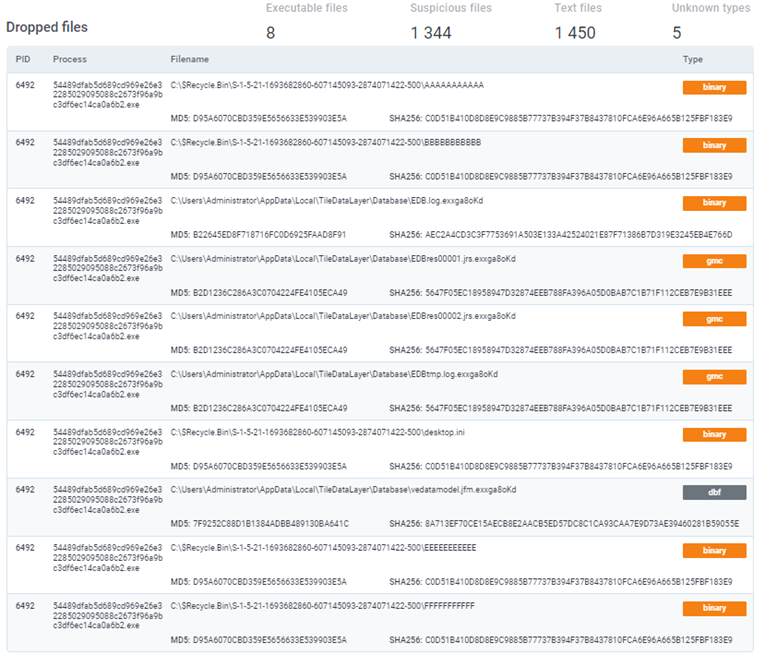
**2**. Elevación de accesos al malware

****

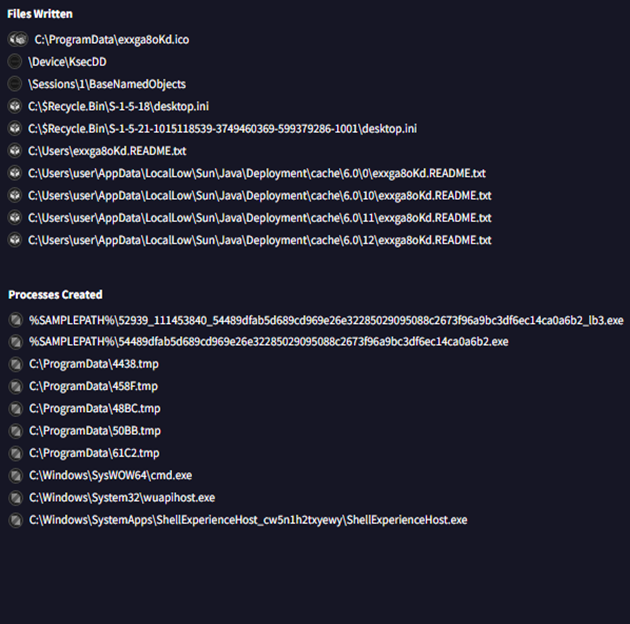
**3**. Malware ejecutado

****

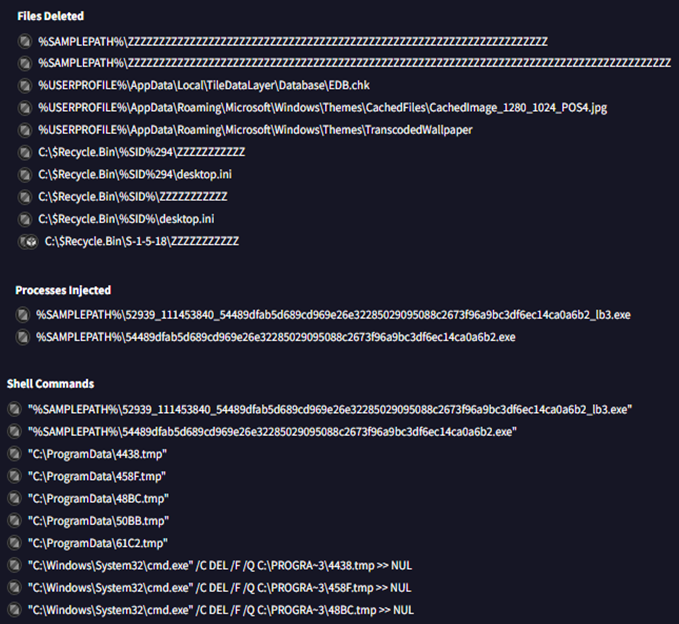
**4**. Malware realizando cambios en registro de Windows (Proxy, Session, Internet Options)

****

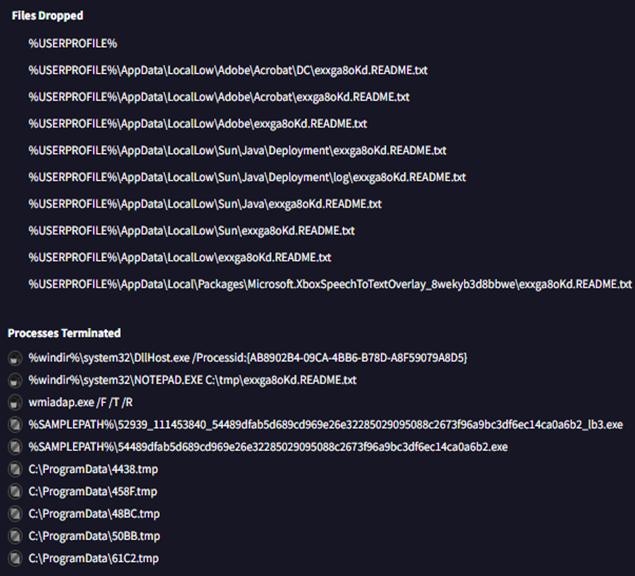
. Malware realizando los cambios a nivel de sistema de archivos



. Evidencia de comportamiento de archivos y procesos

****

. Evidencia de comportamiento de archivos y procesos

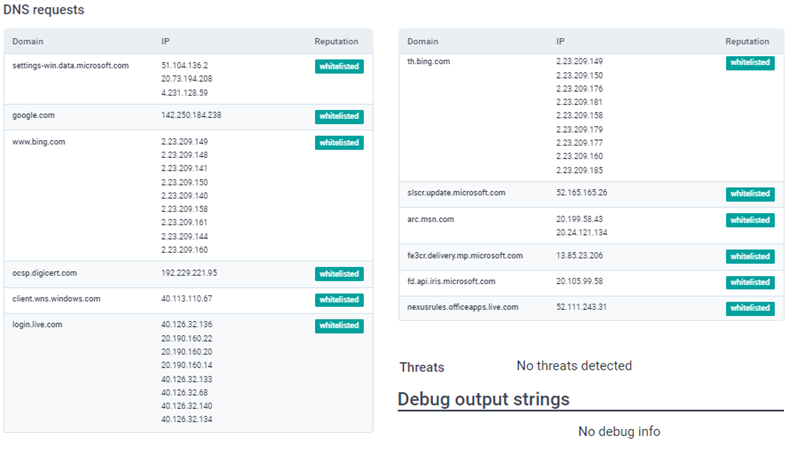
****

. Evidencia de comportamiento de archivos y procesos

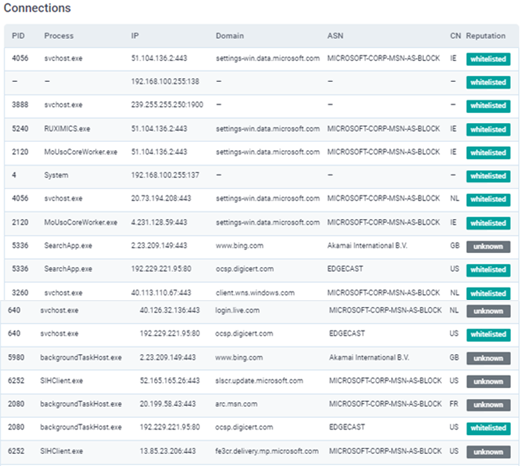
**Actividad en la red:**

****

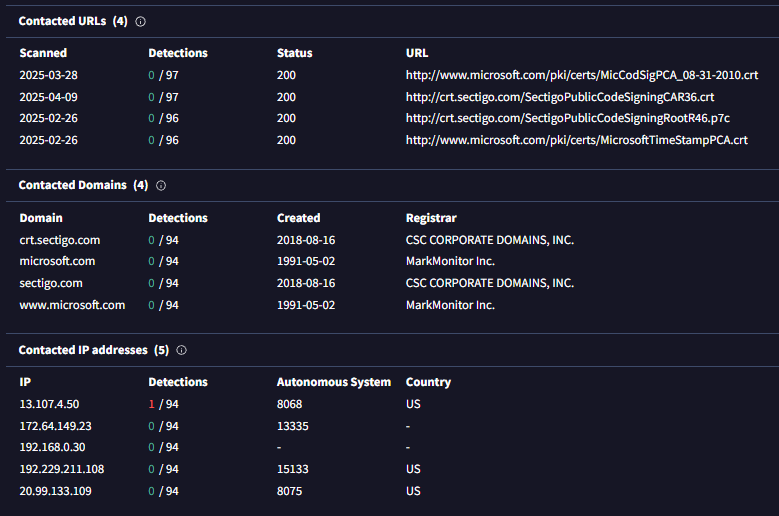
9. Solicitudes HTTP

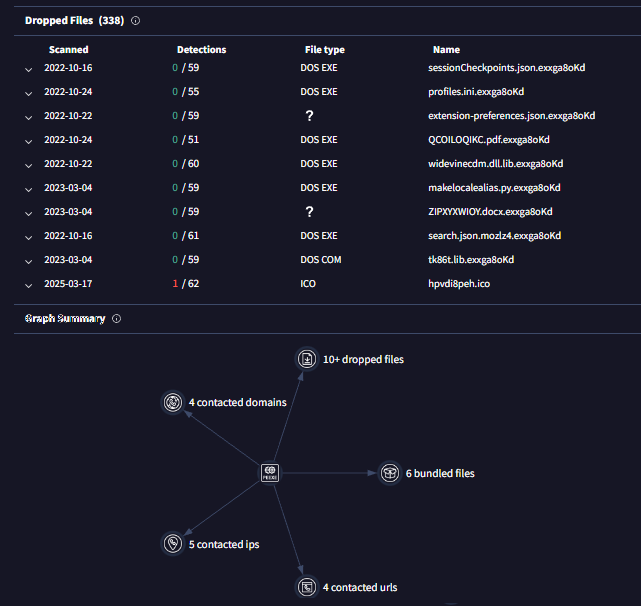
****

. Solicitudes DNS.



**11**. Conexiones

****

****

**12**. Resumen de Conexiones

**Nombre General, Comportamiento y Vector de Ataque**

**Nombre general:** LockBit, es el nombre del grupo de ciberdelincuencia y del software de ransomware bajo el modelo de Ransomware-as-a-Service (RaaS). Originalmente se conocía como “ABCD” que añadía a los archivos cifrados la extensión “.abcd” antes de evolucionar a versiones como LockBit 2.0 y 3.0.

**Tipo de malware:** Se trata de un crypto-ransomware con doble extorsión (encryptor + filtración de datos), ofrecido como Ransomware-as-a-Service. Los operadores de LockBit desarrollan y actualizan el código (incluyendo versiones especializadas para ESXi y Linux). Diseñado para atacar redes sin intervención humana directa, cifrar datos críticos y exigir rescate para su liberación.

**Investigación del malware:** Desde el año 2020, LockBit se ha convertido en la variante de ransomware más desplegada a nivel mundial, afectando al sector público como privado. Emplea AES para cifrar bloques de archivos y RSA para proteger la clave de descifrado.

**Comportamiento del Malware:**

**Privilegio inicial y estabilización:** Creación de cuentas de servicio y persistencia vía tareas programadas o modificación de registros de arranque.

**Escalado de privilegios:** Uso de herramientas como Mimikatz o kerberoasting para extraer hashes y elevar privilegios a nivel dominio.

**Limpieza de Rastros:** Eliminación de volúmenes Shadow y logs locales para dificultar la recuperación.  
Ex filtración de datos: Utiliza la herramienta “StealBit” para robar datos antes de cifrarlos, habilitando la doble extorsión (rescate o amenaza de filtración).

**Cifrado:** Solo cifra los primeros kilobytes de cada archivo para acelerar el proceso de encriptación, añadiendo extensiones como “.lockbit”. **Notas de rescate:** Sustituye el fondo de pantalla por instrucciones de pago y puede imprimir notas en impresoras de red.  
**Movimiento lateral:** Propagación por SMB, WinRM o conexiones directas RDP entre hosts internos.

**Vector de ataque**

**“Campañas de phishing y spearphishing”:** con archivos o enlaces maliciosos**.  
“Credenciales válidas”:** obtenidas en el mercado negro o mediante herramientas de robo de credenciales. **“Drive-by compromise”:** donde el usuario descarga sin saberlo un exploit al visitar un sitio comprometido.  
**“Explotación de RDP” (Remote Desktop Protocol):** para acceso directo al entorno Windows.  
**“Vulnerabilidades”:** en aplicaciones públicas (Ejemplo: Log4Shell), para comprometer servidores expuestos.

**Medidas de Mitigación y Prevención**

1. **Software de Protección:** Implementar una solución de Protección EDR o XDR (Palo Alto Cortex XDR, Acronis Cyber Protect EDR/XDR, CrowdStrike) para detectar y responder ante una actividad maliciosa en tiempo real en los endpoints de la corporación.
2. **Parches y Actualizaciones:** Aplicar en los sistemas endpoints los últimos parches y actualizaciones, sobre todo del tipo “Seguridad” y “Criticas” de manera inmediata. Para Windows se pueden aplicar mediando un servidor propio con el servicio de WSUS configurado.
3. **Copias de Respaldo:** Contar con copias de seguridad de todos los equipos (endpoints, servers, etc, que sean necesarios), para tener el 100% de LexCorp operativo. La baja cobertura de back ups representa un riesgo elevado para la continuidad del negocio y grave deficiencia en la estrategia de recuperación ante desastres. Se Puede usar Veritas Backup como también Veeam Backup. Es buena práctica:
   1. **Aplicar la estrategia “3-2-1”** (Tener 3 copias de datos, en 2 tipos de soportes diferentes, 1 fuera del sitio, desconectada/inmutable.
   2. **Tener versionado de back ups y retención a largo plazo**, se recomienda tener a plazo de 30 a 90 días para cubrir ataques silenciosos con activación tardía.
   3. **Realizar Test de restauración de back ups**, no basta con verificar que se hayan realizado completa y correctamente, se deberá planificar para realizar pruebas de restauración mensualmente.
4. **Contraseñas complejas y Bloqueo de Usuario:** Establecer en el controlador de dominio de la corporación, en una GPO, la longitud mínima en 10 caracteres, combinando letras mayúsculas, minúsculas, números y caracteres especiales. Se debe cambiar la contraseña cada 65 días y no se deben repetir las ultimas 12 contraseñas. Luego del 5º ingreso fallido de las credenciales de un usuario, este debe ser bloqueado por 15 minutos.
5. **Autenticación con Multifactor:** Permite (según en qué sistema se habilito) evitar que un usuario mal intencionado pueda validar completamente una sesión y así acceder a información, vpn o equipo, aunque conozca las credenciales. Duo para servicios Cisco, Azure para servicios Microsoft.
6. **Sistemas Operativos y Software Soportado:** Evitar tener dispositivos o equipos, con sistemas operativos o software fuera de soporte y de actualizaciones. Al no recibir más actualizaciones críticas o de seguridad quedan expuestos a vulnerabilidades no corregidas o nuevas, y también a posibles nuevas técnicas de ataque. Windows 7 finalizo su ciclo el 14/01/2020 y Windows Server 2003 finalizo su ciclo el 14/07/2015.
7. **Realizar el Endurecimiento “Hardering**” a todos los equipos endpoint para deshabilitar configuraciones y servicios (por Defecto) que puedan tener una vulnerabilidad (Ejemplo: Registro Remoto, WinRM, SMB v1).
8. **Revisar el Perímetro de Seguridad e implementar mejores prácticas:**
   1. **Implementar reglas de Firewall** para bloquear tráfico en puertos/aplicaciones/url’s que no se requieran. Se recomienda obtener un Firewall de próxima generación (FWNG Firewall Next-Gen).
   2. **Segmentar las Redes** para aislar segmentos críticos de red y evitar la propagación de ataques.
   3. **Mantener los sistemas actualizados** y verificar periódicamente si requieren algún parche (fix) que corrija algún error (bug) o vulnerabilidad que deberá ser corregido de manera inmediata.
   4. **Utilizar sistemas de monitoreo para detección/prevención de intrusiones (IDS/IPS)** para identificar intentos de acceso no autorizado, bloqueo de amenazas en tiempo real, escaneo masivo. Un Firewall de próxima generación integra tecnología IDS.
   5. **Realizar el Endurecimiento “Hardering”** a todos los dispositivos para deshabilitar configuraciones y servicios (por Defecto) que puedan tener una vulnerabilidad.
   6. **Implementar VPN con IPSec**, para el acceso a la red corporativa y sus servidores de recursos.
   7. **Monitoreo de Logs para equipos y** dispositivos que permitirá centralizar los eventos en un sistema para automatizar las alertas (de ciertos eventos configurados) y realizar él envió por correo. Se puede usar Kiwi SysLog.
9. **Concienciación y Formación:** Disponer de personal responsable de DAO (Digital Awareness Officer) para capacitar y supervisar que se apliquen buenas prácticas de ciberseguridad dentro de la empresa y así evitar el error humano. Supervisando estrategias de concientización sobre amenazas cibernéticas, phishing, ingeniería social, filtraciones de datos, importancia de mantener los sistemas actualizados, correo malicioso, sitios maliciosos, uso de contraseñas seguras y únicas, identificación temprana de comportamientos sospechosos y de ataques.
10. **Escaneo de vulnerabilidades:** Cada 30 días realizar un escaneo de vulnerabilidades en todos los equipos y dispositivos, para resolver problemas del tipo Medium, High y Critical. Se puede usar Tenable.io o Acunetix.
11. **Pruebas de Penetración:** Programar semestralmente un servicio de pruebas de Pentest, para conocer las vulnerabilidades de la red de Corporación LexCorp.