# Proyecto Final

Primera entrega

## Dato fuente de la información

Para la elaboración del presente informe, han sido analizadas las siguientes fuentes de información:  
● Informe del incidente reportado por LexCorp  
● Muestra de malware entregada por el equipo de soporte técnico  
● Análisis dinámico con las plataformas VirusTotal y ANY.RUN

## Análisis de Malware

El presente informe responde a la necesidad de conocer el alcance del incidente de seguridad ocurrido en LexCorp entre el 20 y el 23 de junio de 2021. El objetivo es identificar el tipo de amenaza, su comportamiento, origen y posibles mecanismos de persistencia.

### Hipótesis de compromiso

* • Un usuario descargó y ejecutó un archivo camuflado como “Notificación Judicial” desde un correo electrónico.
* • El ejecutable usó procesos legítimos (WinRAR.exe) para evadir la detección.
* • El malware aplicó técnicas de persistencia y trató de descargar carga útil adicional.
* • Pudo haber existido movimiento lateral dentro de la infraestructura.
* • El objetivo principal es servir de loader para otros códigos maliciosos.

### Muestra Analizada

Nombre de la muestra: 4 NOTIFICACION JUDICIAL.exe

Fecha del análisis: 27/05/2025

OS utilizado para análisis: Windows 7 Professional SP1 (32 bit)

MD5: 723e114a3b04ae46c9542647e19682f8

SHA‑1: 0c4232f19b7203eaf3b6b4e390ac176c88745a15

SHA‑256: 188596839f2390436fc8c0585820180c616c642dd1443cddd26370a1cf3e63d7

### Información estática encontrada

* • Formato: EXE (PE32)
* • Sistema operativo objetivo: Windows
* • Técnica de evasión: Carga de ejecutables legítimos (WinRAR.exe)
* • Compilador/Linker: Versión 48
* • Punto de entrada: 0x3162
* • Nombre interno: 4 NOTIFICACION JUDICIAL.exe
* • Descripción: Loader de malware (PrivateLoader)

### Diagrama de procesos de comportamiento

Inicio  
 |  
 v  
Ejecución de 4 NOTIFICACION JUDICIAL.exe  
 |  
 v  
Carga de WinRAR.exe (legítimo)  
 |  
 v  
Lectura de configuraciones de Internet Explorer  
 |  
 v  
Autoinicio en el sistema (persistencia)  
 |  
 v  
Establecimiento de conexiones remotas  
 |  
 v  
Creación de procesos hijackloader  
 |  
 v  
Fin

### Eventos asociados

* • Creación de procesos secundarios maliciosos
* • Persistencia en el sistema
* • Lectura de configuraciones de seguridad
* • Intento de descarga de payload adicional

### HTTP Request / Conexiones / DNS Request

Se observó tráfico HTTP saliente a dominios e IPs dinámicas, característico de loaders que descargan código malicioso adicional. Las resoluciones DNS apuntan a dominios de corta vida y servicios de alojamiento temporal.

### Amenazas

* • Ejecución de código arbitrario
* • Persistencia y evasión de antivirus
* • Descarga de malware adicional
* • Posible exfiltración de información

## Conclusiones

Comportamiento del malware: Evasión / Loader / Persistencia  
Nombre general: PrivateLoader  
Tipo de malware: Loader (Dropper)  
  
PrivateLoader es un malware utilizado para distribuir otros códigos maliciosos. En este caso, actúa como intermediario entre el atacante y una posible carga útil, pudiendo incluir ransomware, spyware o bots.  
  
Recomendaciones:

* • Implementar filtrado avanzado de correo electrónico.
* • Restringir ejecución de archivos desconocidos en rutas de usuario.
* • Desplegar EDR para detección basada en comportamiento.
* • Realizar campañas de concientización para identificar correos maliciosos.
* • Actualizar y parchear sistemas operativos y aplicaciones.
* • Incrementar la cobertura de copias de seguridad confiables.