DOCUMENTACIÓN TÉCNICA

Herramientas utilizadas:

- **Análisis de texto y estructuras:** Notepad++, Total Commander
- **Registro de Windows:** RegRipper, OSForensics, Registry Explorer v2.1.0, MiTeC Windows Registry Recovery
- **Análisis de artefactos del sistema de archivos:** mftdump.exe, WinPrefetchView.exe, OpenOffice Calc
- **Red y tráfico:** Wireshark, Linux Bash

Archivos analizados:

- `netstat.txt`: muestra de conexiones de red activas.
- `$MFT`: tabla maestra de archivos del sistema NTFS.
- `SVHOST.EXE-20CE1088.pf`: archivo Prefetch de ejecución de procesos.
- `NTUSER.dat`, `SOFTWARE`, `SYSTEM`, `SECURITY`, `DEFAULT`, `SAM`: hives del registro de Windows.
- `capturaRED.pcapng`: captura de tráfico de red.
- Archivos maliciosos ubicados en `C:\Users\Fraile\Desktop\borrar\svhost\...`

Evidencias encontradas:

1. **Proceso sospechoso:**
    - Proceso `svhost.exe` imitando al legítimo `svchost.exe`.
    - Conexión saliente desde 192.168.168.10 hacia 192.168.168.14:80.
2. **Ruta de los archivos maliciosos:**
    - `C:\Users\Fraile\Desktop\borrar\svhost\LlamadaVB\bin\Release\sv host.exe`
    - Otros archivos: `CapturaImgJpg.dll`, `svhost.exe.config`, `svhost.pdb`
3. **Archivo de configuración:**
    - `svhost.exe.config` contiene URL: `http://192.168.168.14/BlackServiceBasic.asmx`
4. **Origen del malware:**
    - Archivo `BlackManagerServiceWeb.zip` con marca `Zone.Identifier`
    - Descarga detectada desde Internet.
5. **Persistencia:**

    - Tarea programada `Windows Update` que ejecuta `svhost.exe` al inicio de sesión.
    - Ruta analizada: `C:\Windows\System32\Tasks\Windows Update`
6. **Ejecuciones del malware:**
    - 26 veces según Prefetch; 31 según clave de registro `UserAssist`.
7. **Tráfico de exfiltración:**
    - POST HTTP desde 192.168.168.10 hacia 192.168.168.14.
    - Datos codificados en Base64 reconstruidos como archivo JPEG.
8. **Protecciones del sistema:**
    - **Windows Defender:** exclusión activa para `C:\Users\Fraile\Desktop`.
    - **UAC:** habilitado y operativo según claves de registro.
    - **Firewall:** activo, sin reglas personalizadas para `svhost.exe`.

Conclusión: El sistema fue comprometido mediante la instalación de un malware camuflado como `svhost.exe`, el cual capturó y exfiltró una imagen JPEG utilizando HTTP POST. El programa se instaló mediante un archivo ZIP descargado desde Internet, utilizó el programador de tareas para persistencia, y evitó ser detectado por Windows Defender gracias a una exclusión previamente configurada en la carpeta del usuario. El UAC y el Firewall estaban activos, pero no fueron suficientes para impedir la actividad del malware.