**Mapeo de Eventos Mitre ATT&CK**

**Objetivo del Informe:**

Este informe tiene como propósito contextualizar el análisis forense realizado sobre el sistema Windows comprometido, utilizando la matriz ATT&CK para estructurar las tácticas y técnicas empleadas por el atacante. Además, se destacan los hallazgos principales del análisis, integrando las herramientas y técnicas utilizadas.

**Herramientas y Metodología Utilizadas:**

1. **Volatility Framework:** Análisis de memoria volátil para identificar procesos, conexiones y archivos sospechosos.
2. **Foremost:** Recuperación de archivos borrados mediante data carving.
3. **VirusTotal:** Identificación de malware en archivos extraídos.
4. **Linux Tools:** Uso de comandos avanzados como strings, grep y xxd para análisis de artefactos.
5. **ATT&CK Navigator:** Mapeo de tácticas y técnicas relevantes.

**1. Resumen del Incidente**

El análisis forense de un sistema Windows XP comprometido reveló un ataque dirigido que inició con un archivo PDF malicioso. Este archivo contenía un script de JavaScript ofuscado que descargó un payload (Zbot) desde un servidor remoto. Zbot es un troyano bancario que se inyectó en procesos legítimos para persistir y evadir la detección.

**2. Tácticas y Técnicas Identificadas (ATT&CK):**

| **Táctica** | **Técnica** | **Descripción** |
| --- | --- | --- |
| Initial Access | Spearphishing Attachment (T1566.001) | El ataque comenzó con un archivo PDF enviado por correo electrónico, diseñado para engañar al usuario. |
| Execution | Scripting (T1059.007) | El script de JavaScript incrustado en el PDF fue ejecutado en el lector Acrobat Reader. |
| Persistence | DLL Search Order Hijacking (T1574.001) | El malware inyectó procesos legítimos para mantenerse activo tras reinicios del sistema. |
| Defense Evasion | Obfuscated Files or Information (T1027) | El código malicioso estaba ofuscado para dificultar su análisis y detección. |
| Discovery | System Information Discovery (T1082) | El troyano recopiló información del sistema operativo y la red para planificar movimientos. |
| Command and Control (C2) | Application Layer Protocol (T1071.001) | Se estableció una conexión HTTP con un servidor remoto para descargar el payload. |
| Collection | Input Capture (T1056) | Se recolectaron credenciales mediante técnicas de keylogging. |
| Exfiltration | Exfiltration Over C2 Channel (T1041) | Los datos fueron exfiltrados utilizando el canal de comunicación del servidor C2. |

**3. Hallazgos Clave del Análisis Forense:**

1. **Procesos Sospechosos:**
   * firefox.exe ejecutó AcroRd32.exe, desencadenando la carga del PDF malicioso.
   * Proceso sospechoso identificado: e.exe, un archivo ejecutable relacionado con Zbot.
2. **Puertos Abiertos:**
   * Identificación de conexiones sospechosas en puertos relacionados con tráfico HTTP.
3. **URLs Maliciosas:**
   * https://onlineeast#.bankofamerica.com/cgi-bin/ias/\*/GotoWelcome.
   * URL asociadas con actividades bancarias maliciosas detectadas en memoria.
4. **Archivos Embebidos:**
   * Extracción de 7 archivos PDF, de los cuales 1 fue identificado como malicioso por VirusTotal.
5. **Payload Identificado:**
   * Zbot, un troyano bancario conocido por su capacidad de robar credenciales y escalar privilegios.

**4. Visualización ATT&CK Navigator:**

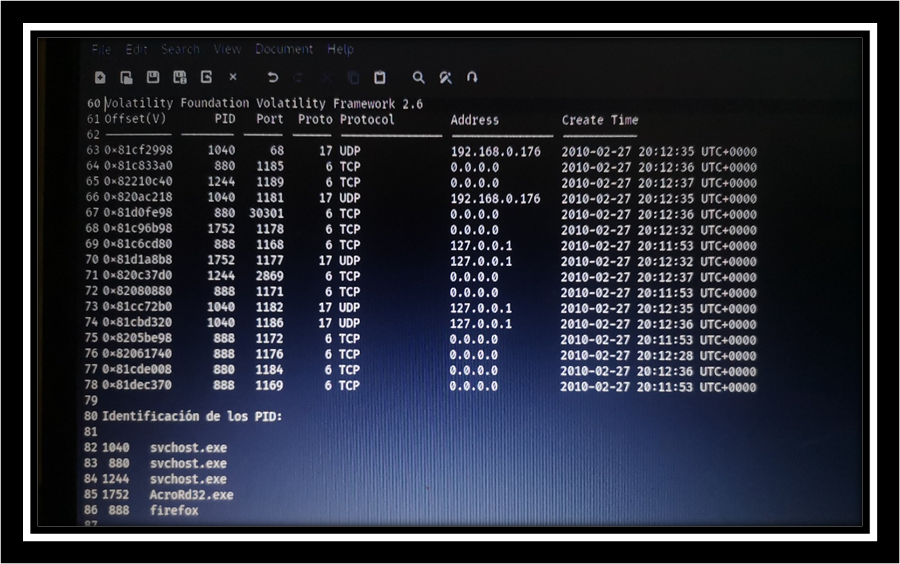
Se generaron mapas de tácticas y técnicas relevantes usando ATT&CK Navigator, mostrando:

* El flujo del ataque desde el acceso inicial hasta la exfiltración.
* La persistencia del malware a través de la inyección en procesos legítimos.
* Técnicas de evasión empleadas para evitar detección.

**Capturas de las Visualizaciones:** *(Incluir capturas o enlaces a los mapas generados en ATT&CK Navigator.)*

**Adjuntos:**

* Resultados del análisis en ATT&CK Navigator.
* Extractos del análisis forense.
* Mapas tácticos generados.

****

**Análisis de malware:** Los archivos sospechosos se analizaron con VirusTotal para obtener información sobre su posible naturaleza maliciosa.