2. Análisis y metodología

2.1 Introducción

Un usuario común utiliza el correo electrónico, trabaja con documentos del procesador de texto, imágenes, archivos de música y video, usa Internet en todo momento, utiliza dispositivos extraíbles, entre otras actividades. El escenario anterior es en el cual se basa la herramienta descrita en este informe.

Un escenario de infección puede ser cuando un usuario, que realiza las actividades del párrafo anterior, se encuentra interactuando con su sistema de cómputo como lo hace cotidianamente y de pronto recibe un correo electrónico con un archivo adjunto (por mencionar un ejemplo), el cual es malicioso y su equipo se ve infectado al haberlo ejecutado.

En ese momento un código malicioso se ha instalado efectivamente en su equipo. El éxito de la acción anterior se debió por parte del usuario a la falta de una buena práctica, la cual dice que no se debe ejecutar ningún programa de procedencia e identidad desconocida. Desde luego, no es una máquina virtual, al menos no en una implementación doméstica.

Probablemente ese software malicioso creó y alteró archivos, modificó llaves de registro, levantó conexiones hacia Internet, levantó ciertos procesos, todo lo anterior o en combinaciones. Conocer el comportamiento de cada código malicioso en particular, puede persibirse sencillo. Sin embargo, las complicaciones surgen cuando se dispone a realizarlo. Para ello se ha desarrollado esta herramienta, que resuelve la mayoría de los problemas clásicos con los que los analistas se encuentran diariamente. A continuación dos diagramas que describen las diferencias estructurales de la solución original y la ampliada. (Figs. 2.1 y 2.2)

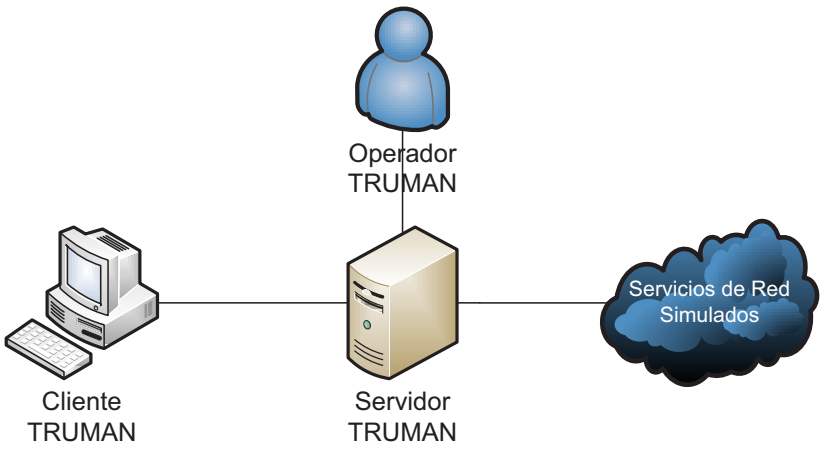

Fig. 2.1. Estructura de la herramienta TRUMAN sin ampliar.

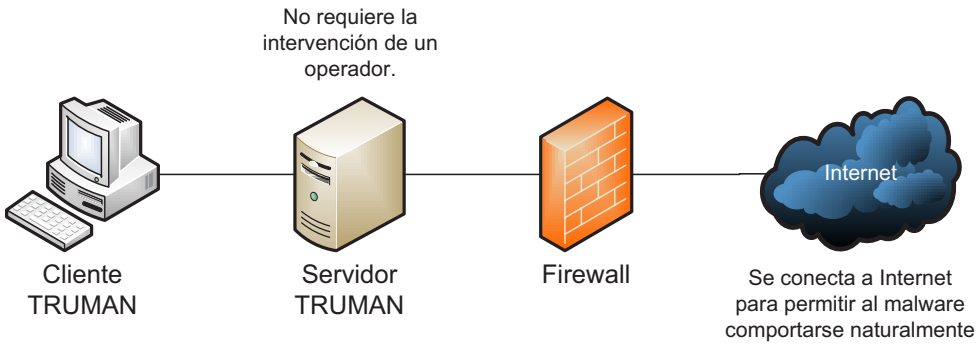

Fig. 2.2. Estructura de la herramienta TURMAN ampliada.

2.2 Procesos del sistema

Un proceso, en realidad, es un programa en ejecución. Los procesos son gestionados por el sistema operativo y se componen de:

- Instrucciones de programa para ser ejecutadas por el microprocesador.
- Estado de ejecución en algún instante, es decir, los valores de los registros de la CPU para dicho programa.
- Memoria de trabajo, esto es, la memoria que tiene reservada y sus contenidos.
- Alguna otra información que permita al sistema operativo su planificación, como puede ser su prioridad e importancia.

La definición anterior es de manera formal. Pues en los sistemas operativos más recientes (Microsoft Windows XP, Vista y Seven) se habla del concepto multihilo. Donde un proceso puede

conformase de uno o más hilos, memoria de trabajo e información de planificación. Cada hilo se compone de instrucciones y estado de ejecución.

Los procesos son creados y destruidos por el sistema operativo, al igual éste se encarga de llevar a cabo la comunicación entre procesos, aunque lo hace a petición de otros más. El mecanismo para que un proceso cree otro proceso se conoce como bifurcación. Estos nuevos procesos pueden ser independientes y no compartir el espacio de memoria con el proceso padre, o bien, pueden ser creados bajo el mismo espacio de memoria. En los sistemas multihilo se pueden crear tantos hilos como se requiera. Sin embargo, un proceso sólo puede crear hilos para sí mismo y dichos hilos comparten toda la memoria que tiene reservada el proceso original.

Los procesos son un elemento más en el análisis de códigos maliciosos. La ejecución de un código malicioso implica el levantamiento de ciertos procesos; pueden ser numerosos en el transcurso de su ejecución, o bien, sólo uno. Analizar los procesos a detalle podría entregar una buena perspectiva del código malicioso en cuestión, sin embargo, se debe obtener un volcado de la memoria RAM del sistema y posteriormente un análisis de ésta misma, lo cual no es una tarea trivial. Es por ello que para este informe se toman como un elemento más, aunque puede darse el caso de que el mismo código malicioso oculte su propio proceso.

2.3 Ejecución de un binario en Microsoft Windows

Un ejecutable o archivo ejecutable es un archivo binario cuyo contenido se interpreta por la computadora como un programa o aplicación. Generalmente contiene instrucciones en código máquina de una arquitectura en concreto, pero también puede contener código para ser interpretado y ejecutado. Adicionalmente se conforma de funciones específicas de un sistema operativo como las llamadas al sistema.

EXE es la extensión que se refiere a un archivo ejecutable de código reubicable, es decir, sus direcciones de memoria son relativas. Resulta de la abreviación del inglés *executable* y que en español significa ejecutable. DOS, Microsoft Windows, OS/2 y ReactOS son sistemas operativos que los utilizan de forma nativa.

Los archivos EXE constan de una cabecera seguida de los segmentos definidos en el código fuente. Los datos de la cabecera son utilizados por el sistema operativo para realizar las inicializaciones

necesarias para el correcto funcionamiento del programa, aunque dicha estructura no forma parte de la imagen final del programa en memoria principal.

Un archivo COM es un tipo sencillo de archivo ejecutable. A diferencia de los archivos EXE, los COM tienen una estructura muy simple y almacenan en forma directa y lineal la imagen de memoria que será el programa.

Un binario sobre los sistemas operativos Microsoft Windows es, prácticamente, un archivo ejecutable y que la mayoría de las veces posee la extensión ".exe", pero en algunas ocasiones utiliza el formato antiguo ".com". Existen diversas formas de ejecutar un archivo de este tipo, sin embargo, para el interés de este informe señalo sólo tres por tratarse de las más utilizadas.

- Ejecución de un binario desde una terminal de comando (símbolo del sistema). A través de la aplicación "cmd.exe" es que se logra ejecutar un binario (fig. 2.3). Se puede elegir su ubicación en el sistema de archivos utilizando comandos de DOS.

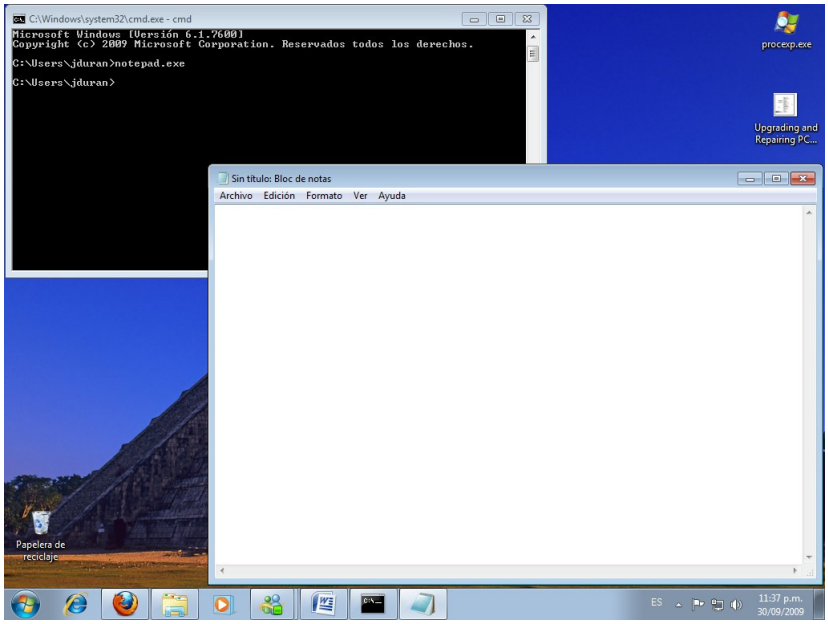

Fig. 2.3. Ejecución desde terminal cmd.exe.

- Un binario también puede ser ejecutado desde el clásico recuadro llamado “ejecutar” presente en Microsoft Windows. Es posible elegir su ubicación exacta en el sistema de archivos con el uso del botón examinar. (Fig. 2.4)

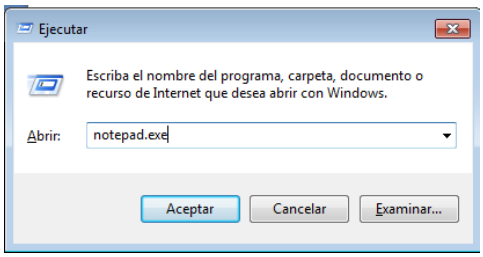

Fig. 2.4. Ejecución desde recuadro “ejecutar”.

- La manera más utilizada por los usuario para la ejecución de un binario en la interfaces gráficas es el doble clic en el archivo con el botón izquierdo de ratón del equipo (fig. 2.5). Para llegar a su ubicación exacta en el sistema de archivos probablemente se necesiten varios clics.

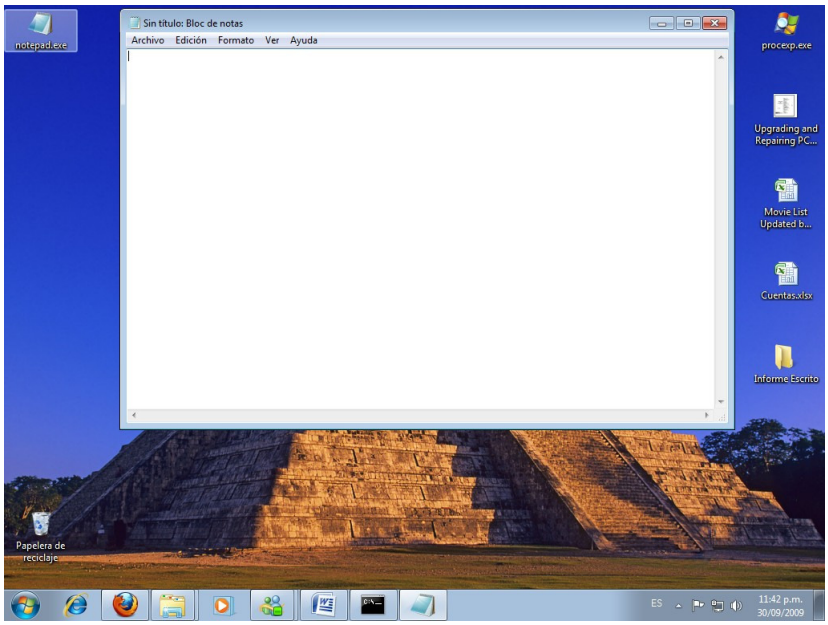

Fig. 2.5. Ejecución con doble clic.

2.4 Protocolos de red

Los protocolos de red son conjuntos de reglas que especifican el intercambio de datos u órdenes durante una comunicación entre sistemas computacionales. En otras palabas son reglas de comunicación que controlan el flujo de información entre computadoras.

Es de vital importancia mencionar que protocolos diferentes no pueden comunicarse entre sí. Y normalmente se han estandarizado con el pasar de los años para que en todo el mundo se manejen procedimientos compatibles para las comunicaciones. La publicación que usualmente los estandariza es el Request For Comments (RFC), el cual está a cargo de la Internet Engineering Task Force (IETF). Dichos escritos detallan métodos, comportamientos, investigaciones o mejoras aplicables para trabajar con Internet, así como la conexión de sistemas de cómputo a la red de redes.

Es relevante hacer referencia, aunque de manera general, a los protocolos de red en la capa de aplicación; porque algunos de los protocolos más utilizados son de importancia en la realización de este proyecto. Los protocolos DNS (RFC 1034), HTTP (RFC 2616), FTP (959), IRC (RFC 2810) y DHCP (RFC 2131) son parte de la estructura de funcionamiento y análisis de la herramienta desarrollada.

El DNS se utilizó para conocer las direcciones IP de los dominios consultados por el código malicioso. De manera inversa también puede ser utilizado, aunque no tan frecuentemente.

El HTTP se empleó en el servidor de TRUMAN para transmitir el archivo malicioso ejecutable al equipo cliente.

El protocolo de IRC tuvo que ser manejado en la parte de análisis de tráfico para la extracción de la información importante en los casos que así lo ameritaban.

El servicio de DHCP fue utilizado para lograr que el cliente Microsoft Windows XP obtuviera siempre una misma configuración de red. Esto se logró mediante la funcionalidad del protocolo DHCP para asociar direcciones IP con direcciones MAC o físicas.

2.5 Sistema de archivos

Es un cunjunto de tipos de datos abstractos que son implementados para el almacenamiento, la organización jeráquica, la manipulación, el acceso, el direccionamiento y la recuperación de datos. Puede interactuar con dispositivos de almacenamiento como discos duros o medios ópticos. También existen aquellos que son accedidos por medio de la red a través de un protocolo.

El sistema de archivos actual en Windows XP es el NTFS, Sistema de Archivos de Nueva Tecnología o New Technology File System. Entre sus características más significativas se encuentran las siguientes:

- Tamaño máximo de archivo: 16 EiB (exbibyte).
- Número máximo de archivos: 4,294,967,295 ((2^32)-1).
- Tamaño máximo de volumen: 16 a 256 Tb.
- Caracteres no permitidos en nombres de archivos: “\0, / \ * ? “ < > |”.
- Fechas almacenadas: creación, modificación, modificación POSIX y acceso.
- Atributos: sólo lectura, oculto, sistema, archivo.
- Compresión transparente: Per-file, LZ77.
- Cifrado transparente: Per-file.

El sistema de archivos del GNU/Linux Debian utilizado para realizar la herramienta es el ext3, sistema de archivos extendido versión tres o third extended file system. Sus características más representativas son las siguientes:

- Tamaño máximo de archivo: 16 Gb a 2 Tb.
- Número máximo de archivos: Variable, establecido al momento de la creación.
- Tamaño máximo de volumen: 2 a 16 Tb.
- Caracteres no permitidos en nombres de archivos: NULL y “/”.
- Fechas almacenadas: modification (mtime), attribute modification (ctime) y access (atime).
- Atributos: No-atime, append-only, synchronous-write, no-dump, h-tree (directory), immutable, journal, secure-delete, top (directorio), allow-undelete.
- Compresión transparente: No.
- Cifrado transparente: No.

Los sistemas de archivos son importantes para este informe, ya que resulta necesario analizar el sistema de archivos de Windows XP para la detección de archivos creados, modificados y eliminados como producto de la actividad del código malicioso. Una base de datos de un sistema de archivos NTFS sin contaminar es comparada con otra base de datos de un NTFS contaminado, esta labor la realiza la herramienta desarrollada de manera automática y lo más eficiente posible con la ayuda de utilerías de UNIX y ya sobre el sistema de archivos ext3.

2.6 Registro de Microsoft Windows

El registro de Windows es una base de datos que almacena las configuraciones y opciones del sistema operativo Microsoft Windows en sus versiones de 32 bits, 64 bits y Windows Mobile.

Contiene información y configuraciones de todo el hardware, software, usuarios y preferencias del equipo personal. Si un usuario hace cambios en las configuraciones del "Panel de control", en las asociaciones de archivos, en las políticas del sistema o en el software instalado, los cambios son reflejados y almacenados en el registro.

El registro mantiene tal información en una arquitectura de árbol y ordenada por jerarquía por la cual el sistema operativo y otros programas deben acceder continuamente, como las preferencias de usuario, hojas de ajustes para directorios e iconos de programas, enumeración de hardware instalado y los puertos usados.

Las llaves de **\HKEY_LOCAL_MACHINE\DEFAULT**, **\HKEY_LOCAL_MACHINE\SOFTWARE** y **\HKEY_LOCAL_MACHINE\SYSTEM**, son las de interés para la herramienta por ser las que entregarán información sobre la instalación del código malicioso y sobre su mecanismo de permanencia en el sistema víctima.

2.7 Sistemas de detección de intrusos

Un sistema de detección de intrusos (o IDS por sus siglas en inglés Intrusion Detection System) es un programa o aplicación usada para detectar accesos desautorizados a una computadora o a una red. Estos accesos pueden ser ataques de habilidosos atacantes o de simples Script Kiddies, los cuales sólo usan herramientas automáticas.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos o internos (generalmente sobre el tráfico de red o archivos). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

Para este reporte cabe mencionar dos tipos de sistemas de detección de intrusos los cuales son:

- HIDS (Host IDS)
- NIDS (Network IDS)

Los IDS por lo regular disponen de una base de datos de "firmas" de ataques conocidos. Dichas firmas permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento, así también entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.

2.7.1 Sistemas detectores de intrusos de host, HIDS

Un Host IDS vigila una única computadora y por tanto su interfaz corre en modo no promiscuo. La ventaja es que la carga de procesador es mucho menor. Puede resultar efectivo para las siguientes tareas:

- Analizar el tráfico sobre un único servidor o PC.
- Detectar intentos fallidos de acceso.
- Detectar modificaciones en el sistema de archivos, ya sean críticos o no.

Para este proyecto se hace alusión a la tercera funcionalidad, al lograr que la herramienta registre los movimientos realizados en el sistema de archivos y en el registro de Windows para este caso.

2.7.2 Sistemas detectores de intrusos de red, NIDS

Un Network IDS, está basado en red y detecta ataques a todo el segmento de ésta. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red o bien, recibiendo la información a través de un puerto espejo configurado en el conmutador.

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El NIDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento. Luego entonces, es efectivo para las siguientes labores:

- Analiza el tráfico de toda la red.
- Examina paquetes en búsqueda de opciones no permitidas y diseñadas para no ser neutralizadas por los firewalls.
- Produce alertas cuando se intenta explotar alguna vulnerabilidad sobre algún programa de un servidor.

El NIDS que se utiliza en este proyecto es Snort, el cual es de distribución libre y con muchos años de desarrollo por una comunidad que realiza aportes día con día. Se utiliza en este informe para el

análisis de una captura de tráfico que logre obtener información relevante de la actividad de red de cada código malicioso.

2.8 Análisis de tráfico de red

Es el proceso de interceptar y examinar mensajes con el objeto de obtener información desde patrones establecidos en las comunicaciones. Puede ser ejecutado incluso cuando los mensajes están cifrados y no pueden ser descifrados. El análisis de tráfico puede ser desempeñado en el contexto de inteligencia militar, contraespionaje y seguridad en cómputo.

En lo que respecta a la seguridad en cómputo, se puede decir que un atacante sería capaz de obtener información importante al monitorear la frecuencia y el tiempo de los paquetes de la red. Un ataque de tiempo sobre el protocolo SSH puede usar la información del tiempo para obtener datos como la contraseña, durante una sesión interactiva, SSH transmite cada bloque de teclas como un mensaje.

El análisis de tráfico también es una herramienta que permite conocer los detalles de una comunicación. Con ello se puede saber qué sitios visitó, a qué servidores se conectó y qué información intercambió cada uno de los programas maliciosos que sean analizados. Un pequeño, pero concreto módulo de análisis de tráfico ha sido agregado a la funcionalidad de la herramienta TRUMAN ampliada, para complementar su reporte de manera enriquecedora.

2.9 Análisis dinámico de códigos maliciosos

El análisis de malware se integra principalmente de dos técnicas: el comportamiento (análisis dinámico) y el código (análisis estático).

En el análisis de comportamiento, o también llamado análisis dinámico, se observa la actividad del código malicioso en el sistema de cómputo comprometido. Este proceso se realiza bajo un ambiente controlado (una máquina virtual) o bien, mediante una red donde esté limitada la comunicación, con el objetivo de evitar la propagación e infección de otros equipos adyacentes. Esto se hace para monitorear la actividad de los procesos maliciosos que ejecuta el agente malintencionado en el sistema infectado, las conexiones que establece, su actividad en Internet, la manera cómo se comunica con otro equipo remoto y la forma en que se activa o instala en el sistema.

La bondad apreciable de las máquinas virtuales es la facultad de regresar al escenario anterior al ataque del software malicioso. Ello se realiza de manera sencilla, para evitar alguna infección en un equipo real. Entonces es prudente tener presente que, en esta primera década del siglo XXI, gran parte del software malintencionado capturado tiene la capacidad de detectar si es ejecutado bajo estos ambientes virtuales. Y así evitar que se puedan analizar y recopilar datos, retrasando el tiempo de respuesta por parte de los analistas. El desarrollo de TRUMAN permite a los analistas despreocuparse de la no ejecución de software malicioso sobre ambientes virtuales, pues tiene la capacidad de trabajar en ambientes 100% reales y sin mantener contaminado un equipo real.

Finalmente, algo con lo que los analistas se han tenido que enfrentar es cuando algunos códigos maliciosos emplean técnicas especializadas para pasar desapercibidos por las firmas antivirus y hacer ilegible su código. Otros archivos maliciosos utilizan mecanismos para cifrar la comunicación entre el equipo infectado y el servidor remoto con el cual se comunican. Esto, aunado al empleo de técnicas de polimorfismo y metamorfismo en el código (las cuales modifican su apariencia y su comportamiento respectivamente, cada vez que son ejecutados), complican aún más su análisis.