Análisis del Malware Tema 1

Introducción

El malware se define como un software malicioso que realiza acciones mal intencionadas. Generalmente e busca analizar el malware para asesorar daños, identificar vulnerabilidades, capturar a los “chicos Malos” y responder respuestas.

¿Por que se crea malware?

El primer malware fue un gusano que trataba de medir el tamaño de internet en los 80. El gusano se comportaba como una forkbomb y se propagó de forma increíblemente rápida. En los 90 los virus se hicieron para ganar gloria personal, haciendo que el malware mostrara mensajes en pantalla. En la actualidad se crean para ganari dinero, robar contraseñas, información bancaria o secretos industriales. En el futuro se cree que se utilizarán para guerra cibernética con malware que utilizaría vilnerabilidades de tipo Zero Days con el objetivo de causar daño en instalaciones físicas.

Cuestiones prácticas

- ¿Cual es el objetivo de este malware?
- ¿Como y cuando fui infectado?
- ¿Quien me ha establecido como objetivo?
- ¿Como evitarlo?
- ¿Que han obtenido mediante el malware?
- ¿Es capaz de reproducirse?
- ¿Como lo puedo encontrar en otro lugar?
- ¿Como se previene otra futura infección?

Cuestiones técnicas

- ¿Cuales son los indicadores de red?
- ¿Cuales son los indicadores a nivel de host?
- ¿Persistencia?
- ¿Fecha de compilación?
- ¿Fecha de instalación?
- ¿Leguaje de programación?
- ¿Empaquetado?
- ¿Tiene funcionalidades rootkit?

Términos popilares de análisis del malware

- Virus: Código que va unido a una aplicación que busca replicarse en aplicaciones similares hasta que pueda ejecutar una payload.
- Gusano: Malware que se propaga muy rápido a través de la red.
- Troyano: Malware que se camufla como otra aplicación para infectar el sistema.
- Spyware/adware: Malware para espiar o meter publicidad
- Backdoor: Vulnerabilidad dejada de forma deliberada por el fabricante
- Rootkut sniffers: Rootkit que escucha todos los paquetes que pasan por la red.
- Exploit: comandos que toman ventajas de vulnerabilidades del sistema
- Disassembler: Programa que recibe un ejecutable y genera un archivo de texto con el código en del programa en ensamblador.
- Decompiler: Toma un archivo binario y trata de producir código de alto nivel usando este como base
- Debugger: Programa que permite observar el código mientras se ejecuta.
- Sinkhole: host de la red interna que recibe tráfico malicioso redireccionado desde un dominio malicioso.
- Intrusion Detection System (IDS): Sistema de Software/Hardware que trata de detectar uso no autorizado de la red.
- Intrusion Prevention System (IPS): Intentan detener un intruso que se haya colado en el sistema.
- Operations Security (OPSEC): Proceso de prevenir que un adversario obtenga información sensible.