Trabajo de Fin de Máster

Tu Nombre

31 de julio de 2025

Índice general

Capítulo 1

Introducción

Aquí se presenta la introducción del trabajo, donde se contextualiza el tema y se establecen los objetivos de la investigación.

crearemos los bypass y los intentaremos detectar con herramientas como:

yara volatility

ctf:

ransomware que tiene la clase hardcodeada, tienes o que encontrar el malware y detenerlo antes de que se ejecute o bien una vez ejecutado de un dump de memoria conseguir la clave

Capítulo 2

EDRs Monitorización

Técnicas de EDR

Introducción

Los EDRs (Endpoint Detection and Response) emplean diversas técnicas para monitorizar y proteger los sistemas contra actividades maliciosas. Estas técnicas pueden utilizarse de forma individual o en combinación, como el Desenganche de API y las Llamadas Directas al Sistema.

Técnicas

- **Uso de APIs no enganchadas**
- **Desenganche en modo usuario**
- **Llamadas indirectas al sistema**
- **Llamadas directas al sistema**

Callbacks del Kernel

- Rastreo de Eventos para Windows (ETW)
- Interfaz de Escaneo Antimalware (AMSI)

Monitorización de Llamadas al Sistema

La monitorización de llamadas al sistema implica diversas técnicas de enganche:

- Enganche de API en línea
- Enganche de la Tabla de Direcciones de Importación (IAT)
- Enganche de SSDT (Kernel de Windows)

La mayoría de los EDRs utilizan la técnica de enganche de API en línea reemplazando `mov eax, SSN` con una instrucción de salto incondicional `jmp`.

Capítulo 3

EDRs Bypass

Llamadas al Sistema (Syscalls)

Capítulo 4

Anexos

4.1. Taxonomía de Malware

4.2. Taxonomía de Shellcodes

4.3. Listado de EDRs

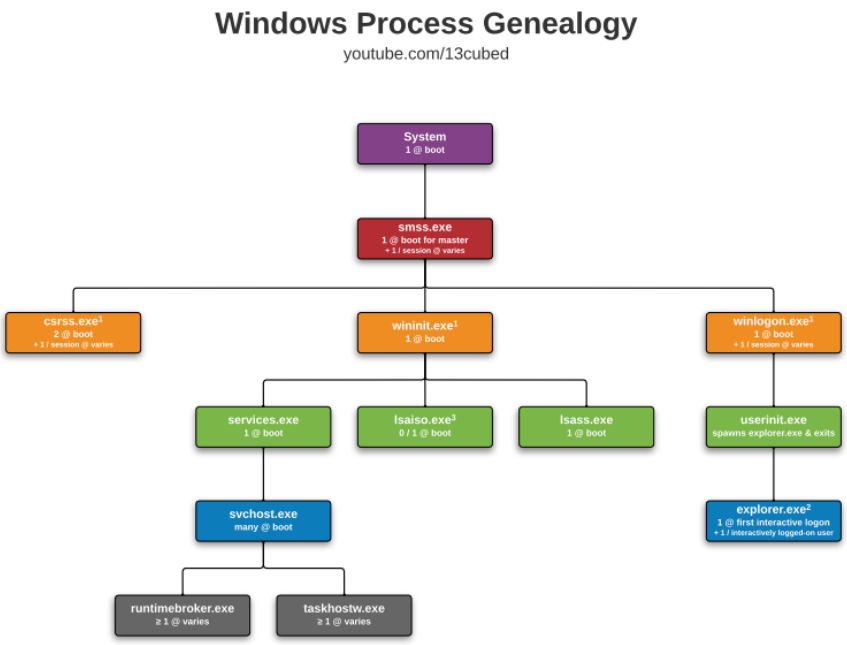
Sylantstrike puede ser utilizado para hacer pruebas de concepto de EDRs

- CrowdStrike Falcon
- Microsoft Defender for Endpoint

4.4. Genealogía de Procesos en Windows

La genealogía de procesos en Windows representa la jerarquía de creación de procesos desde el arranque del sistema hasta el inicio de sesión del usuario. Comprender esta estructura es esencial para el análisis forense, la respuesta a incidentes y la detección de malware, ya que permite identificar comportamientos anómalos en los procesos del sistema.

A continuación se muestra la genealogía de procesos típica en Windows:



Fuente: `youtube.com/13cubed`

Nivel 0: Proceso raíz

- **System**: Primer proceso de espacio de usuario iniciado por el kernel. Tiene un PID fijo (normalmente 4) y no tiene padre.

Nivel 1: Session Manager

- **smss.exe (Session Manager Subsystem)**: Primer proceso real del espacio de usuario. Se encarga de iniciar las sesiones del sistema, lanzar procesos críticos como `csrss.exe`, `wininit.exe` y `winlogon.exe`.

Nivel 2: Procesos críticos del sistema

- **csrss.exe**: Client/Server Runtime Subsystem. Se encarga de funciones esenciales como la gestión de la consola y la creación de procesos. Existe una instancia por sesión.
- **wininit.exe**: Windows Initialization Process. Lanza procesos esenciales como `services.exe`, `lsaiso.exe` y `lsass.exe`.

- **winlogon.exe**: Gestiona la autenticación del usuario y se mantiene activo durante la sesión interactiva.

Nivel 3: Procesos del sistema

- **services.exe**: Service Control Manager. Se encarga de iniciar y gestionar los servicios del sistema, incluyendo los alojados por `svchost.exe`.
- **lsaiso.exe**: Proceso de seguridad aislado que implementa funciones de cifrado y autenticación en versiones modernas de Windows (opcional).
- **lsass.exe**: Local Security Authority Subsystem Service. Encargado de políticas de seguridad, autenticación y gestión de credenciales.

Nivel 4: Servicios alojados y utilidades del sistema

- **svchost.exe**: Proceso contenedor que aloja múltiples servicios del sistema. Existen muchas instancias según el grupo de servicios que aloje.
- **runtimebroker.exe / taskhostw.exe**: Procesos auxiliares para la ejecución de aplicaciones y tareas programadas.

Procesos del usuario interactivo

- **userinit.exe**: Iniciado por `winlogon.exe` tras la autenticación. Lanza el shell principal del usuario y termina.
- **explorer.exe**: Shell gráfico de Windows que representa el escritorio, la barra de tareas y el menú de inicio. Es el proceso raíz del entorno del usuario.

Importancia en Ciberseguridad

Comprender esta estructura es fundamental para:

- Identificar procesos anómalos o fuera de lugar.
- Detectar técnicas de evasión como *Process Injection* o *Parent PID Spoofing*.

- Realizar análisis forense de procesos mediante herramientas como Sysmon, EDR, Process Explorer, o Zeek.

4.5. Memoria Virtual en Windows

4.6. Win32 API

Nombre de la DLL	**Tareas de la DLL**
User32.dll	Esta biblioteca contiene funciones para crear ventanas, manejar mensajes y procesar la entrada del usuario.
Kernel32.dll	Esta biblioteca proporciona acceso a una variedad de servicios esenciales del sistema como la gestión de memoria, operaciones de E/S y la creación de procesos e hilos.
Gdi32.dll	Esta biblioteca contiene funciones para dibujar gráficos y mostrar texto.
Comdlg32.dll	Esta biblioteca proporciona diálogos comunes como los diálogos de abrir y guardar.
Advapi32.dll	Esta biblioteca proporciona funciones para trabajar con el registro de Windows y gestionar cuentas de usuario.

Cuadro 4.1: Descripción de las principales DLLs de la Win32 API