

# Práctica 3

## SYSMON

En determinadas situaciones, resulta crucial llevar a cabo una monitorización efectiva del sistema y generar registros de todos los eventos relevantes, centrándonos especialmente en **Sysmon**. **System Monitor (Sysmon)** es un servicio que, una vez instalado, se mantiene constantemente activo, permitiendo supervisar y registrar de manera exhaustiva la actividad del sistema en el registro de sucesos de Windows.

Para comenzar, descargamos tanto la [herramienta](#) como la [configuración](#) que utilizaremos. Luego, para la instalación, ejecutaremos el siguiente comando desde una terminal con privilegios de administrador: '**sysmon -accepteula -i <archivo\_configuracion>**'

CA Administrador: Símbolo del sistema

```
c:\Users\jose\Downloads\Sysmon>sysmon -accepteula -i C:\Users\jose\Desktop\sysmonconfig-export.xml

System Monitor v15.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

La configuración cuenta con una lista de eventos; en este contexto, se busca describir detalladamente cada uno de ellos.

- **Process Creation [ProcessCreate] (Sysmon ID 1):** Optimiza la monitorización al excluir procesos específicos del registro de creación. Define reglas para omitir procesos y servicios del sistema en Windows, mejorando la eficacia de la seguridad al centrarse en eventos cruciales y reducir la carga del sistema.
- **File Creation Time Retroactively Changed in the Filesystem [FileCreateTime] (Sysmon ID 2):** Identifica cambios en la creación de archivos mediante la detección de manipulación de timestamps (T1099). Supervisa áreas críticas, excluyendo procesos comunes para

minimizar falsos positivos y resalta intentos de ocultar actividades maliciosas mediante la alteración de marcas de tiempo de archivos.

- **Network Connection Initiated [NetworkConnect] (Symon ID 3):** detecta conexiones de red iniciadas. Se enfoca en ejecutables y fuentes sospechosas, excluyendo actividades normales y direcciones conocidas.
- **Reserved for System Service Status Messages (Symon ID 4):** Destinado a mensajes de estado del servicio Sysmon, este canal ofrece detalles cruciales sobre su estado, versión y esquema, siendo indispensable para monitorizar la salud y la versión del servicio Sysmon, sin posibilidad de filtrado debido a su importancia.
- **Process Ended [ProcessTerminate] (Symon ID 5):** Registra la terminación de procesos, crucial para construir líneas temporales de infección. Se enfoca en instancias en carpetas de usuario y ubicaciones críticas, excluyendo otros casos de terminación para mantener la relevancia del registro.
- **Driver Loaded Into Kernel [DriverLoad] (Symon ID 6):** Registra la carga de controladores en el kernel del sistema operativo, focalizándose en posibles escaladas de privilegios. Excluye controladores firmados por entidades confiables como Microsoft e Intel para la monitorización cautelosa. La verificación activa del estado de revocación del certificado de firma asegura la integridad y seguridad del sistema.
- **DLL (image) Loaded by Process [ImageLoad] (Symon ID 7):** Rastrea la carga de DLL por procesos, desactivado por defecto por su impacto en el rendimiento. Crucial para detectar tácticas maliciosas, la configuración actual no registra cargas de DLL, ofreciendo una visión amplia del entorno.
- **Rremote Thread Created [CreateRemoteThread] (Symon ID 8):** Supervisa la creación de hilos remotos por procesos, técnica utilizada por malware para inyectar código y ocultar acciones. Excluye fuentes seguras como procesos del sistema, solo registra eventos de fuentes no convencionales para alertar sobre posibles actividades maliciosas.
- **RAW Disk Access [RawAccessRead] (Symon ID 9):** Detecta accesos crudos a nivel de sector en el disco para alertar sobre intentos de manipulación no autorizada en el sistema de archivos. Desactivado por defecto debido al impacto en el rendimiento, se sugiere probar, especialmente en controladores de dominio.
- **Inter-Process Access [ProcessAccess] (Sysmon ID 10):** Diseñado para detectar acceso interproceso, este monitorea cuando un proceso accede a la memoria de otro. Aunque desactivado por defecto por su impacto en el rendimiento, es valioso para identificar comportamientos anómalos y posibles ataques. La configuración actual alerta solo en la detección de acceso interproceso, indicando posibles actividades maliciosas.
- **File Created [FileCreate] (Symon ID 11):** Detecta la creación de archivos en el sistema para una alerta temprana sobre actividades maliciosas. Se establecen reglas específicas

para incluir o excluir tipos de archivos y ubicaciones, considerando su relevancia para la seguridad y el riesgo asociado.

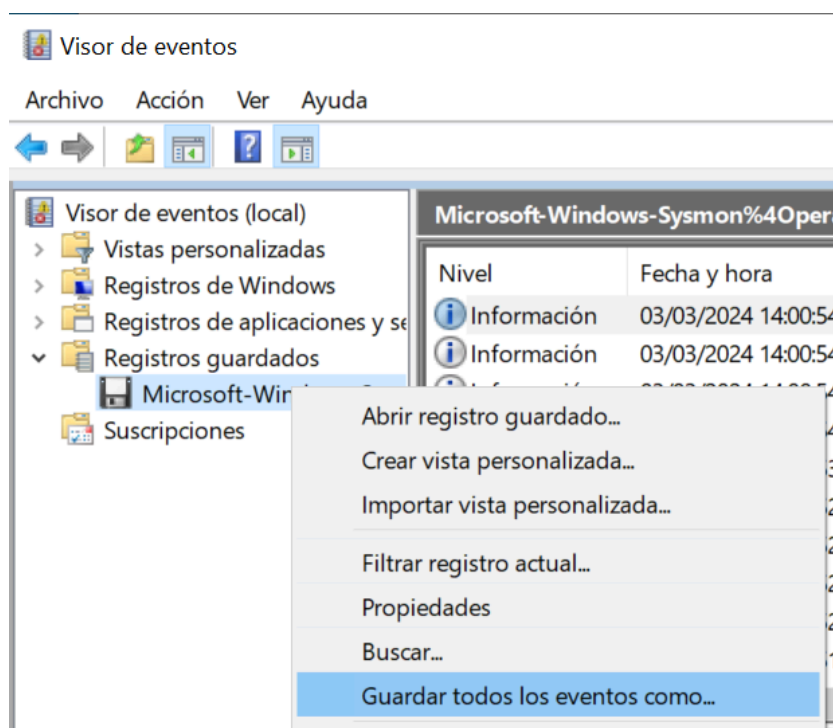
- **Registry Object Added or Deleted [RegistryEvent] (Sysmon ID 12):** Se activa al añadir o eliminar objetos en el registro de Windows, como claves y valores. Identificar estos cambios es esencial para detectar posibles acciones maliciosas, ya que la manipulación del registro es una táctica frecuente para lograr persistencia del malware en el sistema
- **Registry Value Set [RegistryEvent] (Sysmon ID 13):** Este evento se registra al establecer un valor en una clave de registro. La modificación de valores es crítica para las operaciones del sistema, y rastrear estos cambios permite identificar posibles actividades no autorizadas o maliciosas.
- **Registry Object Renamed [RegistryEvent] (Sysmon ID 14):** Se activa este evento al cambiar el nombre de un objeto en el registro, indicando posibles intentos de evasión u ocultación por parte de malware. La detección de estos cambios contribuye a identificar amenazas y actividades sospechosas en el sistema.
- **Alternate Data Stream Created [FileCreateStreamHash] (Sysmon ID 15):** Se activa este evento al crear un flujo de datos alternativo (ADS) en un archivo NTFS, una función que permite asociar datos adicionales. Monitorear esta acción ayuda a identificar comportamientos maliciosos o actividades sospechosas.
- **Sysmon Configuration Change (Sysmon ID 16):** Se activa este evento ante cambios en la configuración de Sysmon, registrando el evento solo cuando el hash de la configuración se ve alterado, no al ejecutar "sysmon.exe -c" con la configuración actual.
- **Pipe Created [PipeEvent] (Sysmon ID 17):** Se activa este evento al crear una tubería (pipe) en el sistema, utilizada para la comunicación interproceso (IPC). La presencia de tuberías puede ser indicativa de actividades maliciosas o herramientas específicas.
- **Pipe Connected [PipeEvent] (Sysmon ID 18):** Se genera este evento al establecer una conexión a una tubería en el sistema. La conexión a tuberías también puede indicar comportamientos sospechosos.
- **WmiEventFilter Activity Detected [WmiEvent] (Sysmon ID 19):** Este evento se genera cuando hay actividad relacionada con los filtros de eventos WMI. Los filtros WMI son utilizados para seleccionar eventos específicos que se deben monitorizar.
- **WmiEventConsumer Activity Detected [WmiEvent] (Sysmon ID 20):** Este evento se genera cuando hay actividad relacionada con los consumidores de eventos WMI. Los consumidores WMI son acciones o scripts que se ejecutan en respuesta a eventos WMI específicos.
- **WmiEventConsumerToFilter Activity Detected [WmiEvent] (Sysmon ID 21):** Este evento se genera cuando hay actividad que conecta consumidores de eventos WMI a filtros WMI.
- **DNS Query [DnsQuery] (Sysmon ID 22):** Este evento se genera cuando se realiza una consulta DNS.

- **File Delete [FileDelete] (Sysmon ID 23):** Este evento se genera cuando se elimina un archivo.
- **Clipboard Event Monitoring[ClipboardChange] (Sysmon ID 24):** Este evento se genera cuando hay un cambio en el contenido del portapapeles.
- **Process Tampering [ProcessTampering] (Sysmon ID 25):** Este evento se activa cuando hay indicios de que un proceso ha sido manipulado desde una fuente externa, como otro proceso.

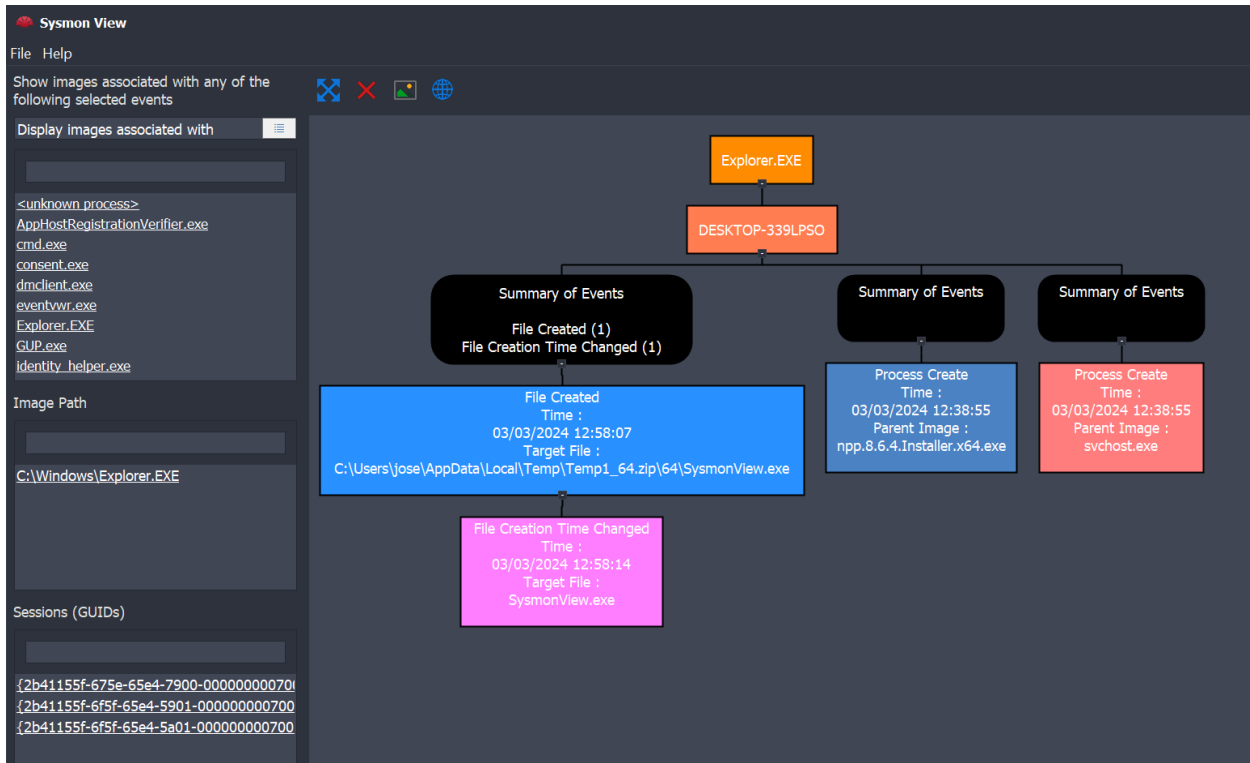
Después de instalar la herramienta, podemos verificar su funcionamiento instalando otro software, como notepad++. Sysmon, por defecto, guarda los registros en el archivo de eventos ubicado en 'C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx'.

Microsoft-Windows-Storage-Storport%4Operat...	03/03/2024 13:05	Registro de eventos
Microsoft-Windows-Store%4Operational	03/03/2024 13:04	Registro de eventos
Microsoft-Windows-Storsvc%4Diagnostic	03/03/2024 13:05	Registro de eventos
Microsoft-Windows-Sysmon%4Operational	03/03/2024 13:37	Registro de eventos
Microsoft-Windows-TaskScheduler%4Maintena...	03/03/2024 13:05	Registro de eventos

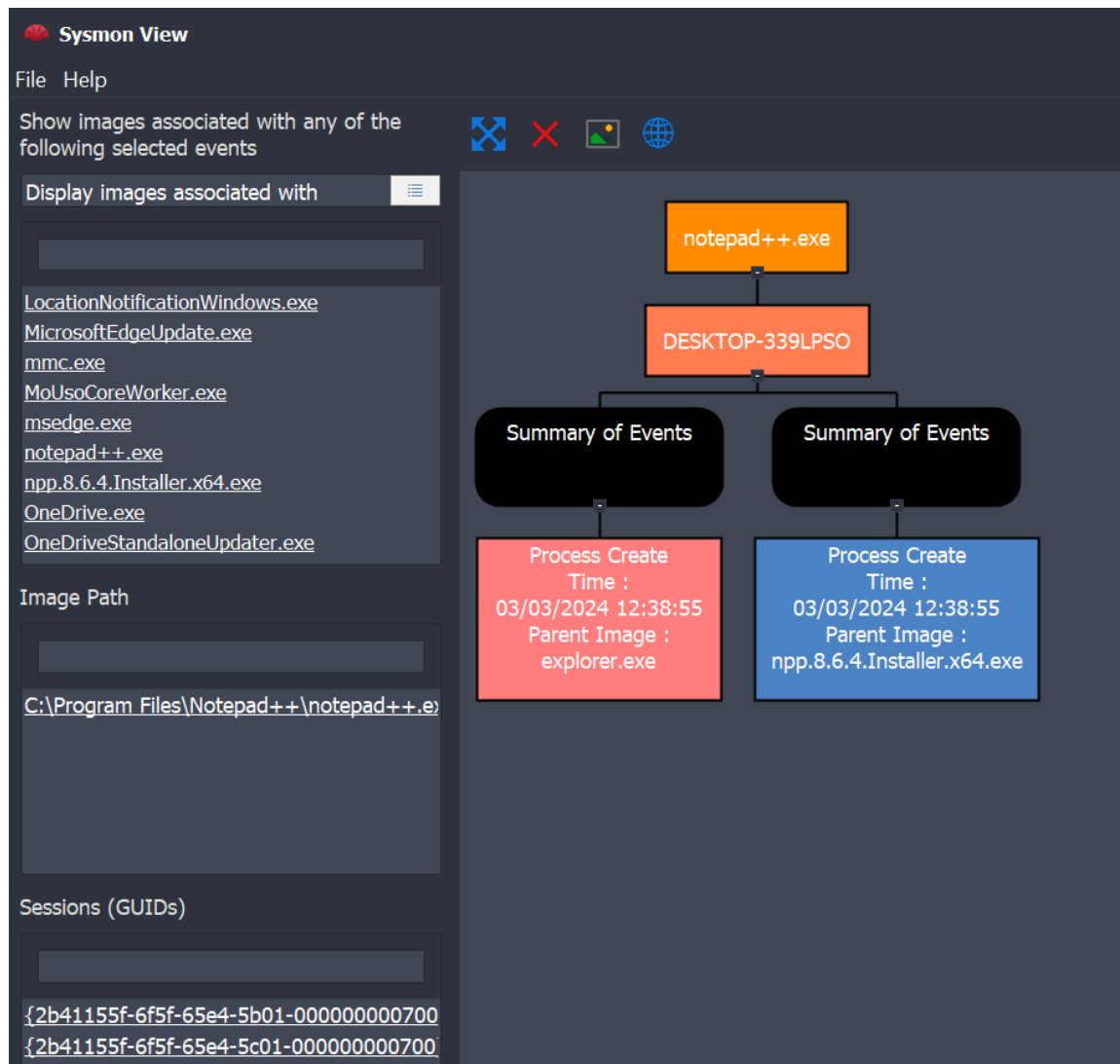
Podemos abrir estos archivos con el Visor de Registros de Windows. Una vez allí, podemos guardarlos en formato XML utilizando el '**Menú contextual > Guardar todos los eventos como XML**' para facilitar el trabajo.

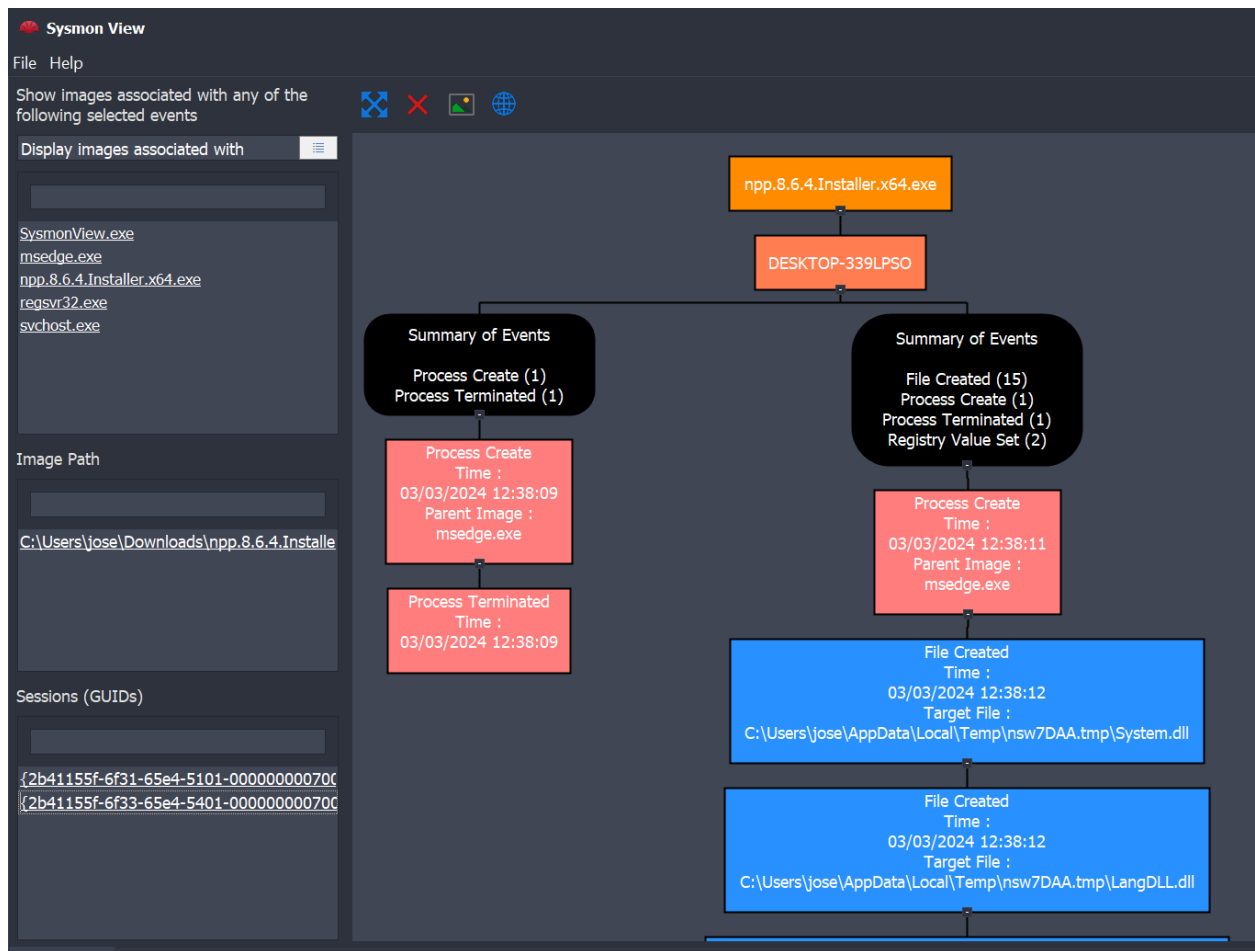


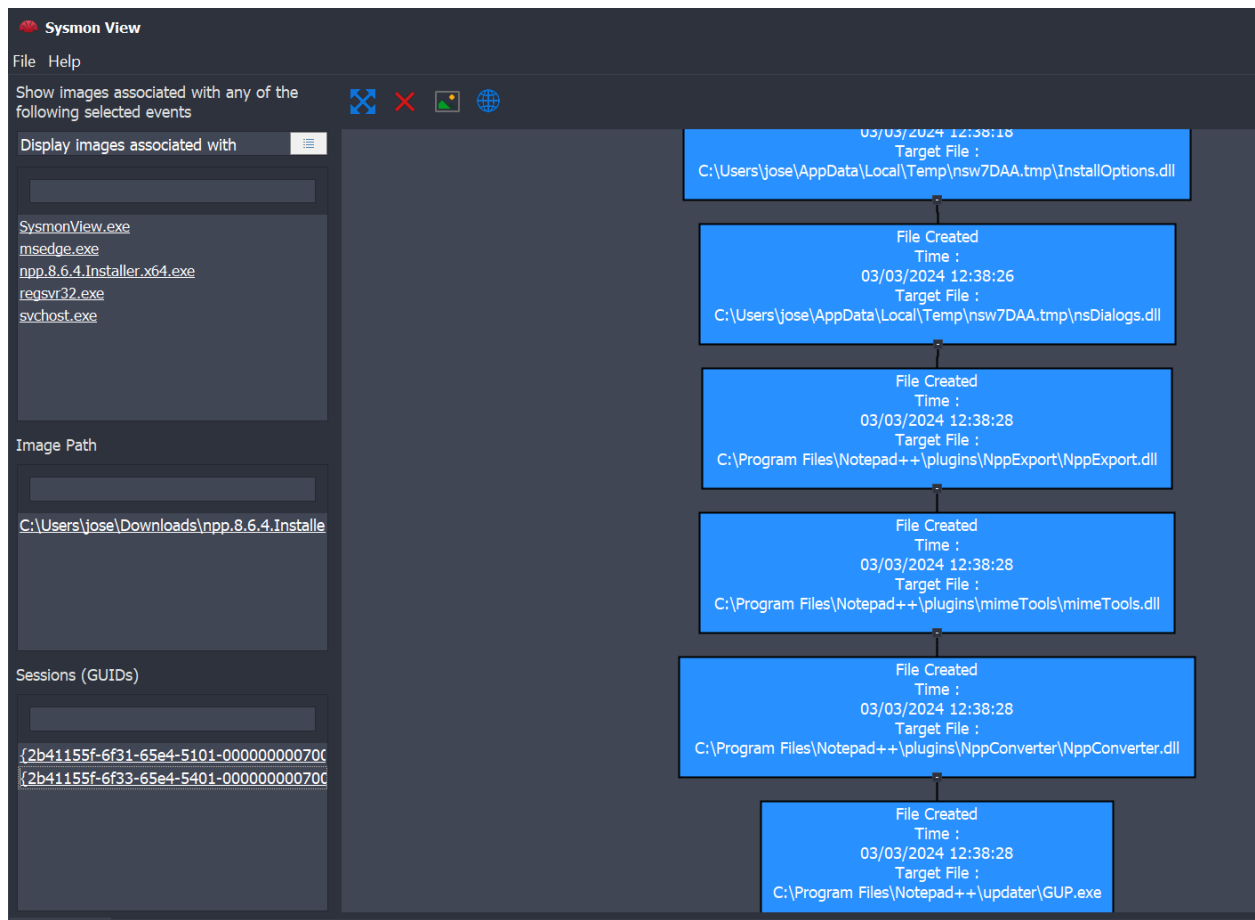
Utilizando el archivo XML generado, podemos aprovechar las [herramientas de Sysmon](#), y en este caso, emplearemos el visualizador de Sysmon (**SysmonViewer**) para una gestión más visual y eficiente de los registros.



ProcessCreate Event Details	
UTC time	03/03/2024 12:38:55
Rule name	-
Process GUID	{2b41155f-6f5f-65e4-5901-000000000700}
Process ID	2176
Image	C:\Windows\explorer.exe
Command line	"C:\Windows\explorer.exe" "C:\Program Files\Notepad++\notepad++.exe"
Current directory	C:\Program Files\Notepad++\contextMenu\
User	DESKTOP-339LPSO\jose
Logon GUID	{2b41155f-675a-65e4-722b-040000000000}
Logon ID	273266
Terminal session ID	1
Integrity level	High
MD5	81886624735B4F8F019E731A8A2E6E69
SHA1	nohash
SHA256	385DBAD0269CAE83598D6706229324EB3CBDEF00E21A0682161477D762AAF2C1
IMPHASH	3D33DFDF6F4BA43E5543CE7637B766DF
Parent process GUID	{2b41155f-6f33-65e4-5401-000000000700}
Parent process ID	224
Parent image	C:\Users\jose\Downloads\npp.8.6.4.Installer.x64.exe
Parent command line	"C:\Users\jose\Downloads\npp.8.6.4.Installer.x64.exe"








En este ejemplo de la instalación de Notepad++, observamos, como ya hemos revisado en la lista de eventos, toda la información recopilada en el sistema, incluyendo datos relacionados con la red, procesos o registros que han cambiado, etc...



 Sysmon View

File Help

Show images associated with any of the following selected events

Display images associated with

OneDrive.exe





OneDriveStandaloneUpdater.exe

Image Path

C:\Users\jose\AppData\Local\Microsoft\One

Sessions (GUIDs)

{2b41155f-6783-65e4-9b00-00000000070}



OneDrive.exe

DESKTOP-339LPSO

Summary of Events

Network Connection Detected  
Time :  
03/03/2024 12:39:11  
Source IP :  
192.168.1.152:50109  
Destination IP :  
20.189.173.3:443

9