Dynamic Analysis: Monitoring Malware Behavior

Tyler Hudak
INCIDENT RESPONDER

@secshoggoth

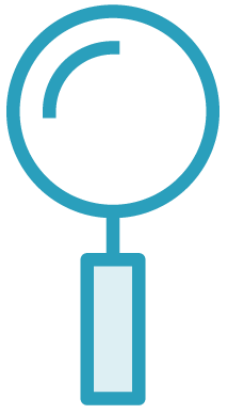
Overview

Monitor what the malware does

What to watch for

Running everything at once

Behavioral Monitoring



Monitors API calls in real time

Sees things system integrity monitoring misses

Susceptible to rootkits

Process Monitor

Records real time system activity

- File
- Registry
- Process
- Network

Functionality

- Filtering
- Record across reboot

Loads driver to record APIs

https://technet.microsoft.com/en-US/sysinternals/processmonitor.aspx

ProcMon Operations

File Operations
CreateFile
ReadFile
WriteFile
SetDispositionInformationFile

Registry Operations
RegCreateKey
RegQueryValue
RegSetValue
RegDeleteKey
RegDeleteValue

ProcMon Operations

Process Operations
ProcessStart
ProcessCreate

Network Operations
TCP*
UDP*

ProcDot

Visualizes ProcMon output

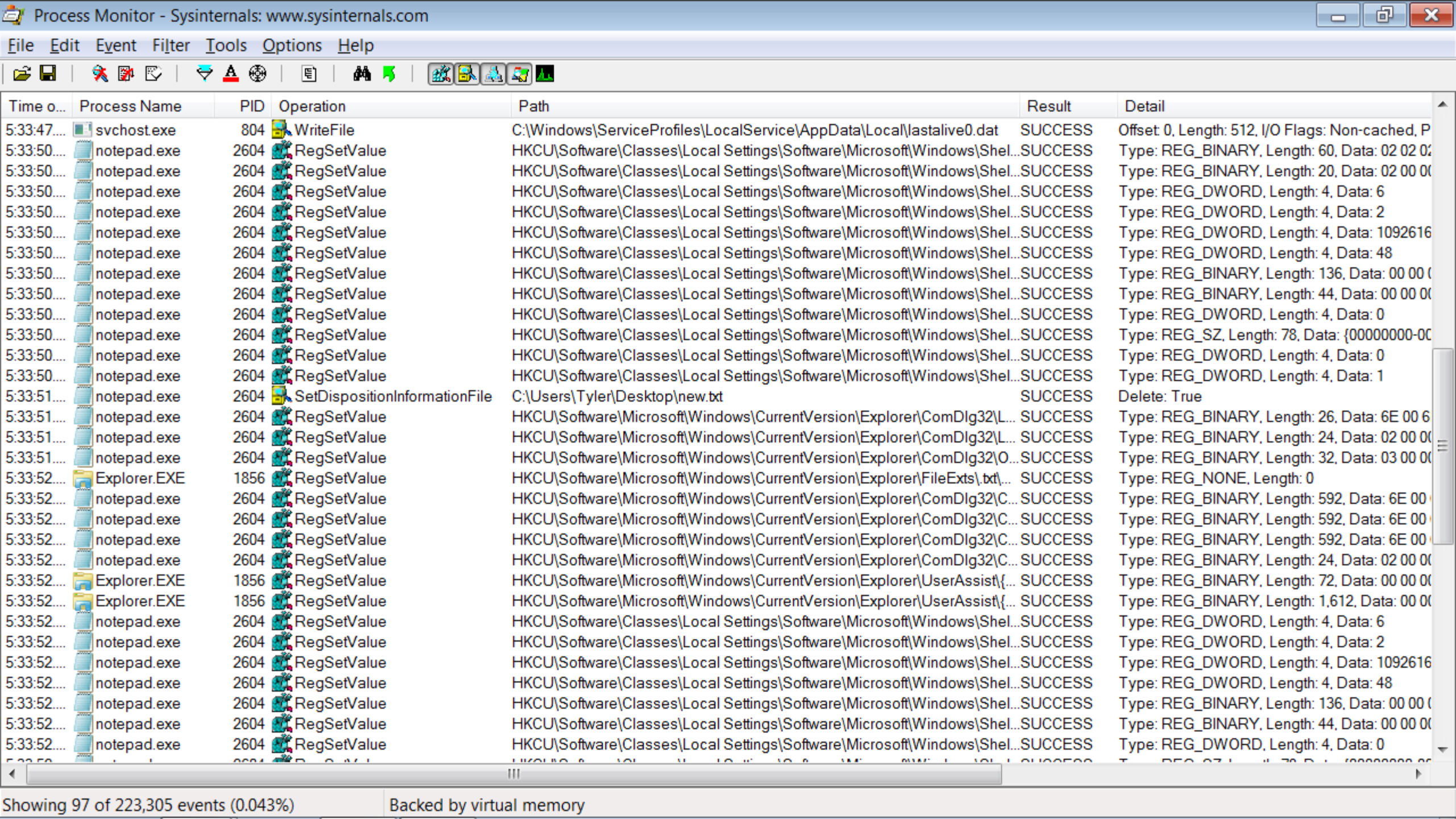
- Requires specific ProcMon config

Integrate network packets

Pre-requisite: GraphViz

- http://graphviz.org/

http://procdot.com/


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
5:33:47.... svchost.exe 804 WriteFile C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat SUCCESS Offset: 0, Length: 512, I/O Flags: Non-cached, P
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_BINARY, Length: 60, Data: 02 02 0
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_BINARY, Length: 20, Data: 02 00 0
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 6
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 2
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 1092616
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 48
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_BINARY, Length: 136, Data: 00 00
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_BINARY, Length: 44, Data: 00 00 0
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 0
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_SZ, Length: 78, Data: {00000000-0
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 0
5:33:50.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 1
5:33:51.... notepad.exe 2604 SetDispositionInformationFile C:\Users\Tyler\Desktop\new.txt SUCCESS Delete: True
5:33:51.... notepad.exe 2604 RegSetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\L... SUCCESS Type: REG_BINARY, Length: 26, Data: 6E 00 6
5:33:51.... notepad.exe 2604 RegSetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\L... SUCCESS Type: REG_BINARY, Length: 24, Data: 02 00 0
5:33:51.... notepad.exe 2604 RegSetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\O... SUCCESS Type: REG_BINARY, Length: 32, Data: 03 00 0
5:33:52.... Explorer.EXE 1856 RegSetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt\... SUCCESS Type: REG_NONE, Length: 0
5:33:52.... notepad.exe 2604 RegSetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\C... SUCCESS Type: REG_BINARY, Length: 592, Data: 6E 00
5:33:52.... notepad.exe 2604 RegSetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\C... SUCCESS Type: REG_BINARY, Length: 592, Data: 6E 00
5:33:52.... notepad.exe 2604 RegSetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\C... SUCCESS Type: REG_BINARY, Length: 592, Data: 6E 00
5:33:52.... notepad.exe 2604 RegSetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\C... SUCCESS Type: REG_BINARY, Length: 24, Data: 02 00 0
5:33:52.... Explorer.EXE 1856 RegSetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{... SUCCESS Type: REG_BINARY, Length: 72, Data: 00 00 0
5:33:52.... Explorer.EXE 1856 RegSetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{... SUCCESS Type: REG_BINARY, Length: 1,612, Data: 00 0
5:33:52.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 6
5:33:52.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 2
5:33:52.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 1092616
5:33:52.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 48
5:33:52.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_BINARY, Length: 136, Data: 00 00
5:33:52.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_BINARY, Length: 44, Data: 00 00 0
5:33:52.... notepad.exe 2604 RegSetValue HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel... SUCCESS Type: REG_DWORD, Length: 4, Data: 0
Showing 97 of 223,305 events (0.043%)
Backed by virtual memory

ProcDOT - C:\Users\Tyler\.procdot\default.pd*

File Edit View Filters Plugins ?

Monitoring Logs

Procmon: C:\Users\Tyler\Desktop\Logfile.CSV

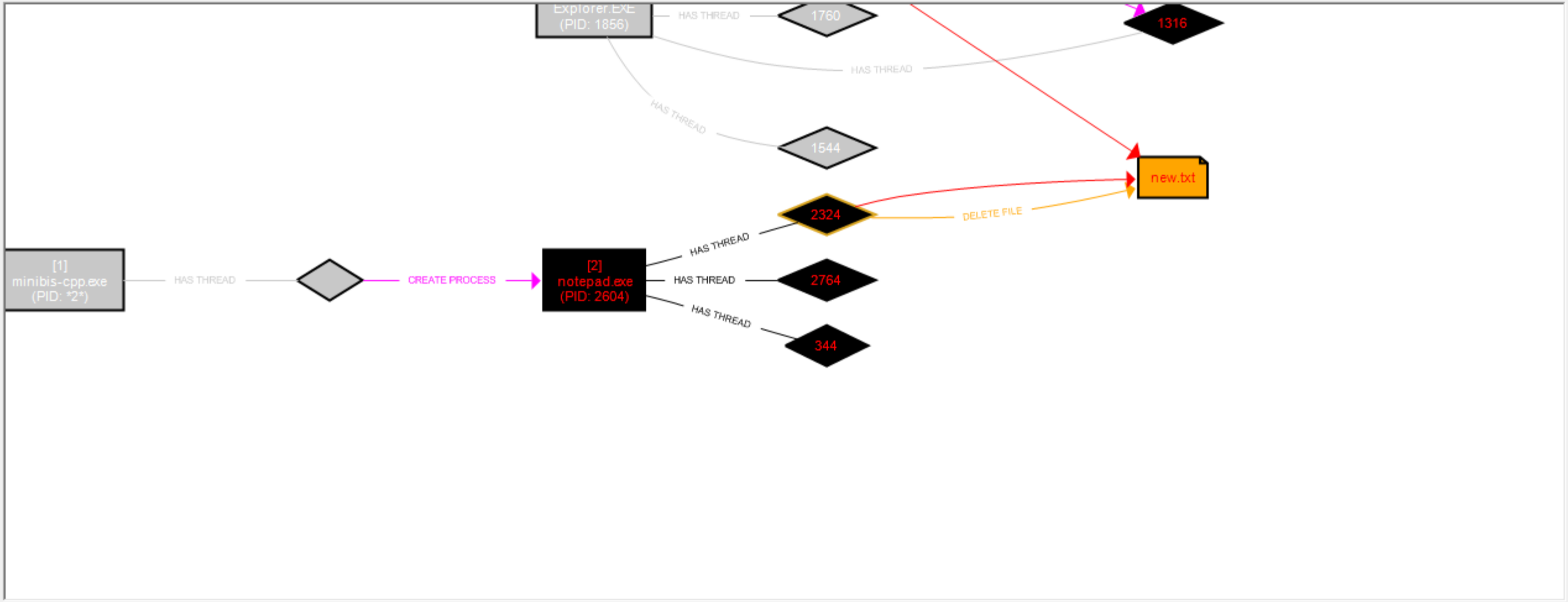
Windump:

Render Configuration

Launcher: 8131999|2604|notepad.exe

no paths compressed dumb

Refresh



10 fps

Status: OK Frame: 0/48 Time: 00:00:00

Thread 1528-o1 of process "Procmon64.exe" (PID: 2816) injects thread 2148-n1 into process "System" (PID: 4)

Baseline your tools.

Demo

Malware Behavioral Monitoring

budget-report.exe

Copied itself to unsecapp.exe

Proved it modified the registry keys

Created a temporary file

Bringing It All Together

1. Start all tools and pause them
2. Take initial snapshot
3. Start system monitor
4. Run malware and wait
5. Pause system monitor
6. Take second snapshot and compare

Demo

How not to run your tools

Summary

Monitor the malware's behavior

Visualize the output

Baseline your tools

Run them in the correct order