Timeliner – Extract Forensic Timeline from Memory Dumps

Overview

Volatility is a powerful memory forensics framework used to extract artifacts from memory dumps, such as running processes, registry keys, network connections, and more. In digital forensics, creating a timeline of activity is crucial. It allows forensic analysts to reconstruct events and identify anomalies or malicious behaviour. The timeliner plugin streamlines the process of generating a forensic timeline from memory dumps using Volatility 3. The final output is a timeline in CSV format that can be easily explored using Timeline Explorer.

Why Timelines Matter

Timelines provide essential context in forensic investigations. Rather than viewing events in isolation, you can correlate file access, process launches, and network activity to better understand a system's state over time. This is especially useful when tracking a threat actor's movements on a compromised machine.

The importance of a timeline can be better understood through exploring the acronym P2FUST (**P**rotocols/Network, **P**rocesses, **F**iles, **U**sers, **S**ystems, **T**imes). This acronym was created by Adam Johnston and explained in a blog post on DFIR MADNESS. The idea surrounding this acronym is to enable you to better understand the context around an event, ultimately being able to determine if an event is a true or false positive. As explained in the post, "the basis of P2FUST is when you come across an event, you take the surrounding information to add context. This helps to decide if an event is a true positive or just a waste of time." The surrounding evidence in this case, can be easily found using a timeline. Take for example you noticed excel contacting an external HTTP server (example given in the blog post)

[P]rotocols/Network:

HTTP/DST 145.23.25.16 SRC: 10.0.2.250:21

[P]rocesses:

excel.exe launched with command line, "c:\program files\microsoft office\root\office16\excel.exe" "c:\users\%user%\AppData\Local\Microsoft\Windows\NetCache\Content.Outlook\IH3E40\InvoicePayment.xlsx"

Child process – regsvr32.exe -s "c: \users\%user%\downloads\reputation.gpx"

[F]iles:

C:\users\%user%\AppData\Local\Microsoft\Windows\NetCache\Content.Outlook\IH3E40\InvoicePayment.xlsx

c: \users\%user%\downloads\reputation.gpx

[U]sers:

John Doe (Role: Accountant)

[S]ystems:

WIN10-WORKSTATION

[T]imes:

16:07UTC

In the above example, a user opened a spreadsheet that was likely downloaded from an email. After opening the spreadsheet, it launched a child process that used regsvr32 to load a file and the process also made a connection to a HTTP server. Based on all of this, it becomes clear that this is a malicious event.

Workflow

This is where the timeliner plugin comes into play. The workflow is as follows:

- Run the timeliner plugin against memory dump using volatility.
- Sort and filter the bodyfile using mactime and export data as CSV.

For those familiar with Log2Timeline/Plaso, this process is similar but built for memory forensics.

Step-by-Step Guide (Volatility 3)

1. Run the timeliner plugin

```
vol.py -f <memory_dump> timeliner --create-bodyfile
```

Example:

```
vol.py -f memdump.mem timeliner --create-bodyfile
```

2. Sort and filter the bodyfile using mactime and export data as CSV

```
mactime -d -b <body_file> > <output_file.csv>
```

Example:

```
mactime -d -b volatility.body > memory_timeline.csv
```

3. Load timeline into Timeline Explorer

Open the timeline in Timeline Explorer. From here, you can filter and search for specific artifacts. For example, if you wanted to look for evidence of execution for FTK Imager, you could search for ftk in the File Name field and voila:

	mac.	0	PsList - Process: 13608 FTK Imager.exe (229798484496576)
	mac.	0	PsScan - Process: 13608 FTK Imager.exe (229798484496576)
	mac.	0	Sessions - Process: 13608 FTK Imager.exe started by user TIMS_PC/timba
	.acb	0	ShimcacheMem - Shimcache: File C:\Program Files\AccessData\FTK Imager\FTK Imager.exe modified
2022-01-19 09:02:40	m...	0	ShimcacheMem - Shimcache: File C:\Program Files\AccessData\FTK Imager\FTK Imager.exe modified

Summary

The timeliner plugin bridges the gap between memory analysis and timeline-based investigation. By automating the aggregation of key forensic artifacts from RAM, it accelerates the identification of malicious behaviour with the clarity and structure of a timeline.