CYBR8420 – Software Assurance

GotRoot? - BitWarden (CLI)

Robert Ernewein

Basic information

Download: BitWarden – Client Interface (CLI) Windows x64
Link: https://vault.bitwarden.com/download/?app=cli&platform=windows
Format: Zipped executable
File Name: bw.exe
Size: 53.6 MB

New Account created: 20191107@2247

Initial testing

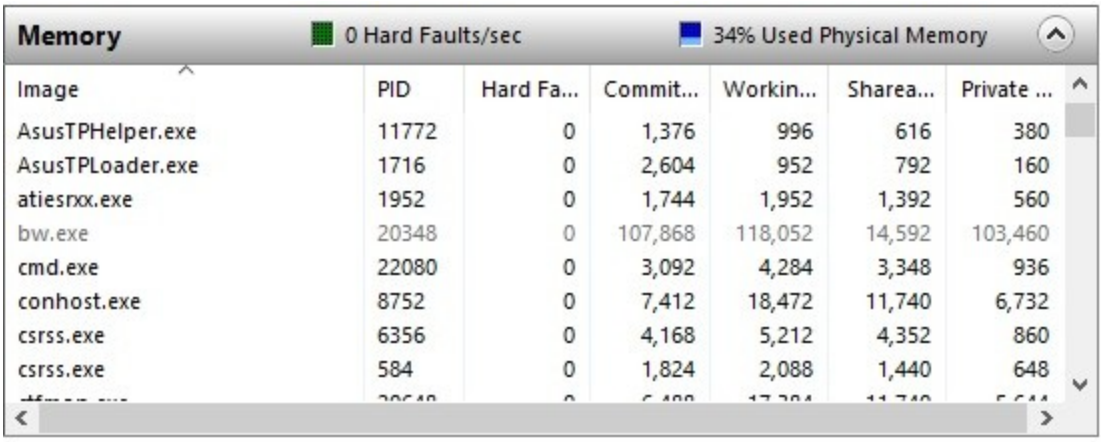
Attempt to determine External Interactors from the Application System using Task Manager, Resources Monitor, & Event Viewer Logs.

Open Command Prompt: cmd

Initial state with command prompt open:

Applications: 4
Processes, Background: 42
Processes, Windows: 95

Command	PID	Commit (KB)	Working (KB)	Shared (KB)	Private (KB)
bw	22508	73,596	67,400	13,224	54,176
bw login	20336	70516	80444	15004	65440
bw login e-mail pw		71184	83352	16528	67004
bw unlock	20888	97908	107876	14344	95532
bw lock	20348	107868	118052	14592	103460



Each of the commands above were executed multiple times as well the following:

bw -v
bw --help
bw sync
bw logout

Initial Findings

Task Manager: No instances, spawned processes, or service changes were indicated. All activity appeared to be contained with the command prompts process space.

Resource Manager: However, BitWarden's memory footprint was indicated following each command performed (See: Table and Image above).

Note: Resource Manager updates the status of background and system processes once per second, but the Windows Memory Manager maintained the resource allocation for 30 seconds before releasing it as cache/available memory. This allowed me to look at the process space.

Event Viewer: Surprisingly, there were no indications in any of the logs of BitWarden's interactions.

Conclusion

These findings lead me to believe that all of BitWarden's functional components are operating within a single process space. I am curious about the contents of the shared memory space and which processes are tied in. I ran about 3 dozen commands and averaged 14.6 MB of shared memory per instance.

The application is only resident while processing a command, but it may be possible to capture the contents of the application space using FTK Imager or logging its execution within a Virtual Machine/ Container.