Juicing V8: A Primary Account for the Memory Forensics of the V8 JavaScript Engine
Project PI: Ibrahim Baggili
Grant Number: H98230-20-1-032

Enoch Wang[a,b], Samuel Zurowski[a,b], Orion Duffy[a,b], Tyler Thomas[a,b], Ibrahim Baggili[a,b]

[a] *University of New Haven Cyber Forensics Research and Education Group (UNHcFREG), Samuel S. Bergami Jr. Cybersecurity Center, USA*
[b] *Connecticut Institute of Technology at the University of New Haven, USA*

Abstract

V8 is the open source interpreter developed by Google to enable JavaScript (JS) functionality in Chrome and power other software. Malicious threat actors abuse the usage of JS because most modern-day browsers implicitly trust script code to execute. To aid in incident response and memory forensics in such scenarios, our work introduces the first generalizable account of the memory forensics of the V8 JS engine and provides practitioners with a list of objects and their descriptors extracted from a memory image. These objects can be used to reveal key information about a user and their activity. We analyzed the V8 engine and its garbage collection process. We then developed and validated a Volatility plugin – V8MapScan – to reconstruct V8 objects from a memory image. The runtime of the V8 engine is housed within the V8 isolate which contains its own heap manager and garbage collector. Within the heap of the isolate exists a root object map known as the MetaMap. By using the MetaMap and a *object-fitting* technique, we were able to extract objects, object-maps, and object properties. The V8MapScan plugin scans process memory for the MetaMap data structure contained within the V8 isolate using its data structure, references to objects can be found and extracted. Our findings were verified with Chrome DevTool's *Heap Profiler*. Our approach recovered the majority of objects indicated by the heap profiler with common types such as the ONE_BYTE_INTERNALIZED_STR type returning more than 98.9%. Lastly, we provide a case study using our tools on the Monero Cryptocurrency Miner. This material is primarily based upon work supported by National Security Agency (NSA) and Department of Defense (DoD) under grant H98230-20-1-032.

Keywords: Memory Forensics, Volatility, V8, Javascript, Memory Analysis, Object Recovery

Email addresses: `ewang3@unh.newhaven.edu` (Enoch Wang), `szuro1@unh.newhaven.edu` (Samuel Zurowski), `oduff1@unh.newhaven.edu` (Orion Duffy), `tthom10@unh.newhaven.edu` (Tyler Thomas), `ibaggili@newhaven.edu` (Ibrahim Baggili)