Mem2Img: Memory-Resident Malware Detection via Convolution Neural Network

Published: 2021-09-01 · Archived: 2026-04-05 14:32:18 UTC

Process injection is a widely used defensive evasion technique commonly used for malware and fileless adversary transactions and requires running custom code in the address space of another process. Process injection improves invisibility, and some techniques also achieve persistence. We have observed that many APT attacks use this method to evade detection to achieve persistence. Therefore, it is increasingly important to detect such memory-resident malware which is injected through the process. Antivirus software does not have a high detection rate for memory-resident malware. As far as we know, in the face of such attacks, such as volatility, Rekall and Get-InjectedThread, YARA rules may be one of the best solutions, but the disadvantage is that it is impossible to distinguish unknown malware or shellcode-based malware. More and more people are proposing to use machine learning to classify malware family or detect malware. While there are many techniques for applying machine learning to implement malware classification, most works are heavily dependent on handcrafted features that can be evaded easily. In order to get rid of the above weaknesses, we present convolution neural networks (CNNs) with ensemble on memory-resident malware detection framework named Mem2Img..... By: Charles Li & Aragorn Tseng Full Abstract & Presentation Materials: https://www.blackhat.com/asia-21/brie...
