Malware Analysis and Automation with Binary Ninja

Erika Noerenberg[1]
[1]*Logrhythm*

As threats have increased in prevalence and sophistication over the years, analysts simply need more time and resources to manually analyze available samples. As a result, the need to automate malware analysis has become of paramount importance. Analysts are continuously developing tools and scripts to assist in these tasks, but malware is constantly changing and evolving to evade these techniques.

As analysts, it is crucial to leverage automation whenever possible to save time for these complex samples that must be reversed manually. With the continuous mutation of attacker methodologies, we need to be able to adapt our automation solutions quickly.

There are many tools available to us as malware analysts, and one of the latest is a reverse engineering platform called Binary Ninja. However, in speaking with colleagues, I've found that many either haven't heard of this tool or have found it hard to incorporate it in their daily work. In this talk, I hope to demystify the Binary Ninja interface by demonstrating how to perform basic analysis and utilize the API for the common automation task of dumping and decoding configuration data using a practical, real-world sample.