Introduction to Cisco IOS analysis

Adrian Justice[1]
[1]*Australian Cyber Security Centre*

2015 saw the discovery of SYNful Knock, the first known instance of malware for Cisco IOS devices. Fast forward to 2018 and no additional samples of IOS malware have been found which begs the question, is no one writing IOS malware anymore or are we just not finding it? This presentation will provide a look at what makes up an IOS system image and memory dump, how to process IOS system images so they play nicely with traditional analysis and reverse engineering tools and ultimately lower the barrier for security researchers to get started analysing Cisco IOS and discovering new malware. We will also take a quick look at some of the non-malware based attacks that are being utilised today.