Presentation Summary

We found that the random forest model was effective for differentiating normal network traffic from attacks. The 3 most important features in classification were direction, appName, and totalSourceBytes. The majority of network attacks were conducted from a local to local connection. HTTP web attacks were the most common application attack. The attacker had established command and control relatively early into their attack. We recommend migrating web servers to HTTPS if possible, and disabling all unused ports. Users should be required to use a VPN to access the SSH interface.