Fast and Service-preserving Recovery from Malware Infections Using CRIU

Ryan Eckenrod
University of Maryland, College Park

Abstract

Once a computer system has been infected with malware, restoring it to an uninfected state often requires costly service-interrupting actions such as rolling back to a stable snapshot or reimaging the system entirely. We present CRIU-MR: a technique for restoring an infected server system running within a Linux container to an uninfected state in a service-preserving manner using Checkpoint/Restore in Userspace (CRIU).

We modify the CRIU source code to flexibly integrate with existing malware detection technologies so that it can remove suspected malware processes within a Linux container during a checkpoint/restore event. This allows for infected containers with a potentially damaged filesystem to be checkpointed and subsequently restored on a fresh backup filesystem while both removing malware processes and preserving the state of trusted ones. This method can be quickly performed with minimal impact on service availability, restoring active TCP connections and completely removing several types of malware from infected Linux containers.