ARMED: How Automatic Malware Modifications Can Evade Static Detection?

Raphael Labaca Castro, Corinna Schmitt, Gabi Dreo Rodosek

Abstract— Modifying existing malicious software until malware scanners misclassify it as clean is an attractive technique for cybercriminals. In particular, fully automatizing the process can bring adversaries to generate faster effective threats. Recent studies suggest that injecting successful malware modifications could lead to corrupt executable files despite of detection. Therefore, we propose ARMED - Automatic Random Malware Modifications to Evade Detection - to bypass classifiers by automatizing valid malware generation based on detected threats. The goal is to understand how successful automatic perturbations can be used to avoid detection. In order to reach this goal, we take portable executable malware and add a number of small random injections to evade detection without affecting the malware structure. Our experiments proved that only six perturbations are required to create new functional malware samples exhibiting exactly the same behavior yet with up to 80% less detections based on original malware that was previously detected. We show that within a few minutes an adversary could take a previously detected malware and convert it in a clean new mutation bypassing static malware scanners.

For the published version of record document, go to:
http://dx.doi.org/10.1109/INFOMAN.2019.8714698