ACIDBOX Clustering — The Lost Reports

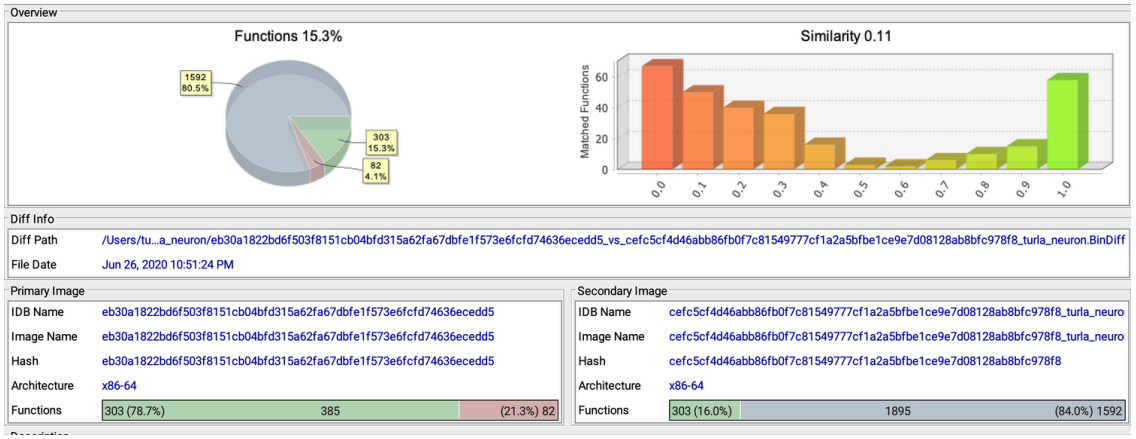
By Jun 26 Written By J A G-S

Published: 2001-06-26 · Archived: 2026-04-06 00:05:40 UTC

As I was looking over this blog, I realized I'd inadvertently settled into a once a month post and hadn't been planning to post anything for June. However, doing some routine code similarity work, I stumbled upon something I felt like sharing for others to enjoy over the weekend.

Last week, Palo Alto Unit42 researchers Dominik Reichel and Esmid Idrizovic revealed their discovery of ACIDBOX (a.k.a. KL: MagicScroll), a new and fascinating activity set reminiscent of Remsec (a.k.a., KL_Project Sauron or SYMC_Strider) and using an exploit technique of our dear Turla (namesake of this blog). Researchers were cautious about affirmatively clustering ACIDBOX to either in lieu of stronger evidence.

With the prospect of possibly finding a new Remsec or Turla campaign or more of an unknown threat actor, I was eager to work on rules for this set in the hopes of unearthing more context. A few samples have trickled onto VirusTotal over the past week and based on these I was able to construct a well tested code similarity rule. While I haven't had a chance to dig deeper into the findings, I wanted to present a curious early finding others may find interesting:



ACIDBOX (left) and Turla Nautilus Payload (right)
