

ML Model: Resilience to Malware Modifications Due to Signatureless Approach

The following charts reveal scan results for 33 thousand malicious ELF executables.

There were 2 tests performed: in the first test, the original samples were scanned.

In the second test, each sample out of the entire set was appended with one extra zero byte. The entire set was then scanned again.

In both tests, Prevasio's ML scanner has reached 95.6% detection at 0.1% False Positive Rate (on par with ClamAV's FPR).

The VirusTotal hash lookup has failed in the second test, as it contained no hashes of the modified samples.

Some AV vendors have demonstrated a reduction of the detection rate, revealing how much they depend on hashes.

Other tests conducted by Prevasio prove that Prevasio ML scanner demonstrates excellent resilience to substantial malicious source code modifications and re-compilations.

