0.1 Related work

Using host-based telemetry gathering to detect exploitation of vulnerabilities, both known and unknown, has been widely discussed before[6][3]. One example hereof is DACODA[3], which traces a network packet through the relevant processes until an unintended memory state happens, such as jumping to an address present in the packet.
[7]
Many security software vendors claim to have developed models and techniques to detect against Zero-day attacks[2][1][5], most of the work is proprietary and not available for study. Furthermore, based on the public information none of the vendors explain what telemetry is used other than *"host and network based data"*.
As with any other computer science field, machine learning has also been applied to vulnerabilities. One example hereof is FastEmbed[4] which attempts to use machine learning to predict the number of exploits present in the wild, but is not related to detection of exploitation attempts.

Purpose

Mention that Matt Graeber did stuff, but most "research" is not done academically