1030 - PEIMA (Probability Engine to Identify Malicious Activity): Using Power Laws to address Denial of Service Attacks

Sunday at 10:30 in Track 2
20 minutes | Art of Defense, Demo, Tool
Redezem*Hacker*

Denial of service. It requires a low level of resources and knowledge, it is very easy to deploy, it is very common and it is remarkable how effective it is overall. PEIMA is a brand new method of client side malicious activity detection based on mathematical laws, usually used in finance, text retrieval and social media analysis, that is fast, accurate, and capable of determining when denial of service attacks start and stop without flagging legitimate heavy interest in your server erroneously. However, denial of service attacks aren't the only type of anomalous activity you can look at with PEIMA. Learn what kinds of unusual identifying metrics you can get out of your network and users to help detect intrusions and, ultimately, defend your assets.

Redezem

Redezem hails from the southern hemisphere, specifically Perth, Australia, the most isolated capital city on the planet. He's been an avid computer tinkerer in this desolate, sunny, beach-ridden wasteland from a young age, and has been a "hacker" since he stole his dad's passwords to get at the internet as a kid. Having worked part time as a web application developer during his undergraduate degree in computer science, he specialised into intrusion detection in his honours year, and is currently performing his PhD into new and fantastic network anomaly detection mechanisms at Curtin University. He currently also lectures, and works part-time as a security consultant.

#defcon25/by_track/track2/Sunday #defcon25/By_Day/_Sunday