1300 - Starting the Avalanche: Application DoS In Microservice Architectures

Friday at 13:00 in Track 3
45 minutes | Demo, Tool

Scott Behrens*Senior Application Security Engineer*

Jeremy Heffner*Senior Cloud Security Engineer*

We'd like to introduce you to one of the most devastating ways to cause service instability in modern micro-service architectures: application DDoS. Unlike traditional network DDoS that focuses on network pipes and edge resources, our talk focuses on identifying and targeting expensive calls within a micro-services architecture, using their complex interconnected relationships to cause the system to attack itself — with massive effect. In modern microservice architectures it's easier to cause service instability with sophisticated requests that model legitimate traffic to pass right through web application firewalls.

We will discuss how the Netflix application security team identified areas of our microservices that laid the groundwork for these exponential-work attacks. We'll step through one case study of how a single request into an API endpoint fans out through the application fabric and results in an exponential set of dependent service calls. Disrupting even one point within the dependency graph can have a cascading effect throughout not only the initial endpoint, but the dependent services backing other related API services.

We will then discuss the frameworks we collaborated on building that refine the automation and reproducibility of testing the endpoints, which we've already successfully leveraged against our live production environment. We will provide a demonstration of the frameworks which will be open sourced in conjunction with this presentation. Attendees will leave this talk understanding architectural and technical approaches to identify and remediate application DDoS vulnerabilities within their own applications. Attendees will also gain a greater understanding on how take a novel new attack methodology and build an orchestration framework that can be used at a global scale.
Scott Behrens
Scott Behrens is currently employed as a senior application security engineer for Netflix. Prior to Netflix Scott worked as a senior security consultant at Neohapsis and an adjunct professor at DePaul University. Scott's expertise lies in both building and breaking for application security at scale. As an avid coder and researcher, he has contributed to and released a number of open source tools for both attack and defense. Scott has presented security

research at DEF CON , DerbyCon, OWASP AppSec USA, Shmoocon, Shakacon, Security Forum Hagenberg, Security B-sides Chicago, and others.

@helloarbit

#defcon25/by_track/track3/friday #defcon25/By_Day/_Friday