Fovea Information Security Threat Modeling Through Log Analysis

Problem
- Situational awareness is critical to mature information assurance
- The data are there, but complex systems generate complex logs
- Security staff at a local financial software company spent so much time collecting and processing data, there was no time to analyze them deeply
- We lacked a long-term trending capability

Solution
- Security Information and Event Management (SIEM) tools streamline log collection and analysis
- Fovea is a custom SIEM that includes a variety of novel, mission-specific analysis and enrichment tools, including geomapping and cross-referencing lists of known threats

Results
- Comprehensive threat picture shows we are not a long term primary target
- Discovered traffic from addresses on FBI’s list of known hacktivist IPs during Anonymous’ OpUSA distributed denial of service (DDoS) attacks in early May
- Discovered serious network misconfigurations that create unnecessary risk and operational cost, and reduce situational awareness

Distributed Denial of Service (DDoS) Threats Hitting our Network

Processing data with a SIEM
- Collection
- Aggregation
- Normalization
- Enrichment
- Analysis
- Action