An API Honeypot for DDoS and XSS Analysis

G Leaden, **Marcus Zimmermann**, **Casimer DeCusatis**, and **Alan G. Labouseur**

What

Honeypots are servers or systems built to mimic critical parts of a network, distracting attackers while logging their data to develop profiles. This poster presents how we built a honeypot disguised as a **RE**presentational **S**tate **T**ransfer (REST) **A**pplication **P**rogramming **I**nterface (API) and the analysis of some of the data we collected.

Why

Our NSF-funded *SecureCloud* environment aims to combat the growing number of cyber attacks against cloud networks. G-star, the Dynamic Graph Database, is used within *SecureCloud* to help us organize, visualize, and analyze cyber attack data. After making a web interface to G-star available online we observed a number of unauthorized connection attempts to its REST API. In response to these attacks, we created a new REST API honeypot, “Pasithea" (the Greek goddess of rest).

Analysis

Many unauthorized attempts culminated in a DDoS attack and an XSS insertion performed against the G-star REST API. The XSS attacks are `curl`-like requests sent to load and run a file on our server.

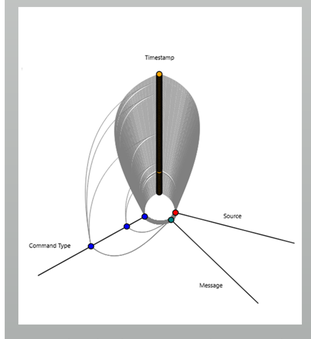
Interestingly, a very similar attack sequence was recently documented by F-Secure, a Finnish cyber-security company.

DDoS

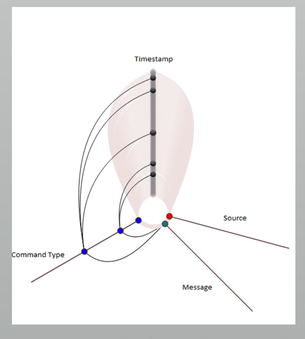
- The attack lasted from May 25, 2017 to June 1, 2017.
- *Responses/second* steadily rose from 500 *R/s* to 6000 *R/s*.
- Created 275,000,000 log entries
  - Log file expanded to 18+ GB (server ran out of storage)
- command type: HEAD
- command text: home

XSS

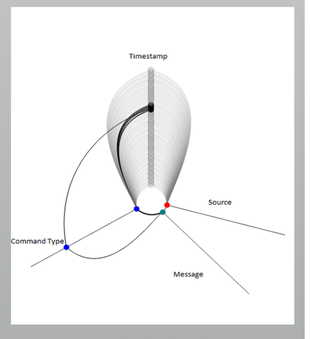
- Command types and text:
  - GET cgi
  - POST command.php
  - GET ;rm$IFS-f$IFS’
  - GET ; wget$IFS-O$IFS’
  - GET ;chmod$IFS’777’$IFS’
  - GET ;sh$IFS-c$IFS’
- took 25 seconds



Hive plot displaying a random sample of 150 points from G-star logs. Data sampled is from February 6, 2017 - May 25, 2017



Prominent nodes denote “injections” into G-star that differ from normal traffic. Data sampled is from February 6, 2017 – May 25, 2017



Prominent nodes display the XSS attempt on G-star. Data sampled is from March 11, 2017 – March 16, 2017

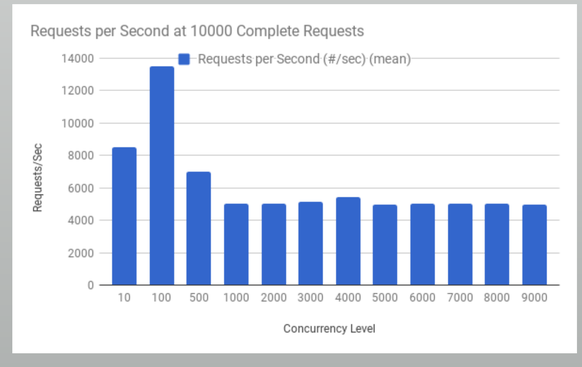
Construction and Performance

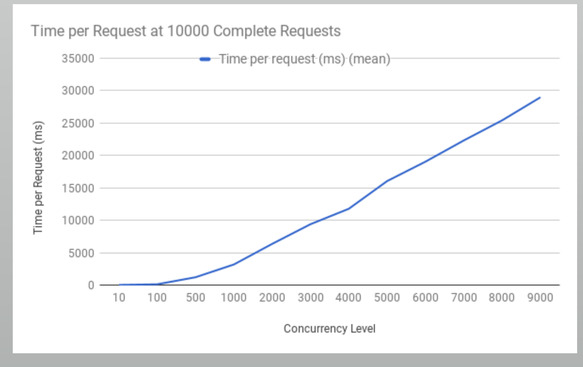
- Java
  - NanoHTTPD
  - Takes any HTTP request and responds with `<h1>404 Not Found</h1>`
- Amazon Web Services Elastic Compute Cloud (AWS EC2)
  - Free micro tier

Data Captured

- current time (yyyy/mm/dd hh:mm:ss)
- command type
- command text
- client IP address
- User Agent

Our log files indicate cursory web crawls from Baidu, a Chinese search engine, and some attempts at exploiting a known vulnerability in Apache Tomcat web servers using “GET /manager/html”.





Performance data suggests that Pasithea should be able to keep a malicious user interested with fast response times — sub 300*ms* under normal traffic — while also maintaining composure and stability under high traffic loads, even at more than 9,000 concurrent requests.

This work is sponsored in part by NSF Grant Award 1541384 — *CC*DNI Integration: Application Aware Software-Defined Networks for Secure Cloud Services.* The authors would like to thank the IBM/Marist Joint Study as well as Dayna Eidle, Thomas Famularo, Jonathan Heiles, Mary Ann Hoffmann, and Thomas Magnusson for their contributions to this work. It is better because of them.