The OWASP Amass Project

DNS Enumeration written in Go

September 6, 2018
Presented by Jeff Foley

Introduction

- Jeff Foley (a.k.a caffix), Project Lead for OWASP Amass

- US Manager, Penetration Testing & Red Teaming at National Grid

- https://github.com/caffix

- https://twitter.com/jeff_foley

What is Amass?

- DNS enumeration and network mapping to aid in understanding an organization's attack surface on the Internet

- The project provides a suite of tools that employ active and passive techniques:
  - Traditional subdomain enumerator
  - Maltego local transform
  - TLS certificate subdomain name grabber
  - More coming soon

- Amass also supports the visualization of findings to better understand the networks being investigated.

OWASP
Open Web Application
Security Project

Getting Amass

- On Linux, Amass is easy to get with Snapcraft:
  $ sudo snap install amass

- Use docker:
  $ sudo docker build –t amass
  https://github.com/OWASP/Amass.git
  $ sudo docker run amass –v –ip –freq 480 –d owasp.org

- Use Go to install Amass:
  $ go get –u github.com/OWASP/Amass/…

OWASP
Open Web Application
Security Project

Collaboration / Current Goals

- Keeping up with new data sources and possibly add services that require API keys

- Add support for additional package managers

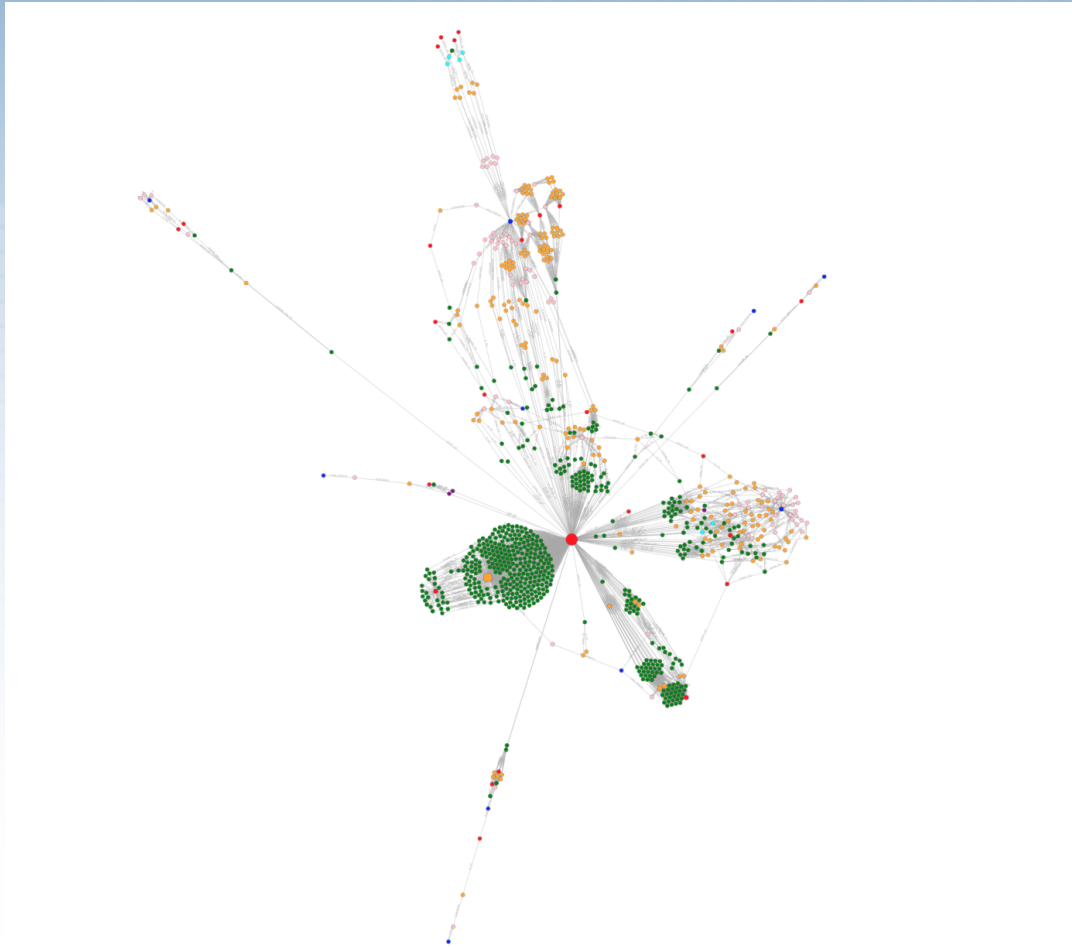- Continue turning Amass functionalities into smaller suite tools.

Lessons Learned

- One of largest Amass contributions is the "Alt & Sweep" technique
  - Alterations & permutations of names (AltDNS)
  - Reverse DNS sweeps around discovered IP addresses
  - In a cyclic relationship, additional network infrastructure is revealed

- During the life of the project, many data sources have increased the number of names provided.
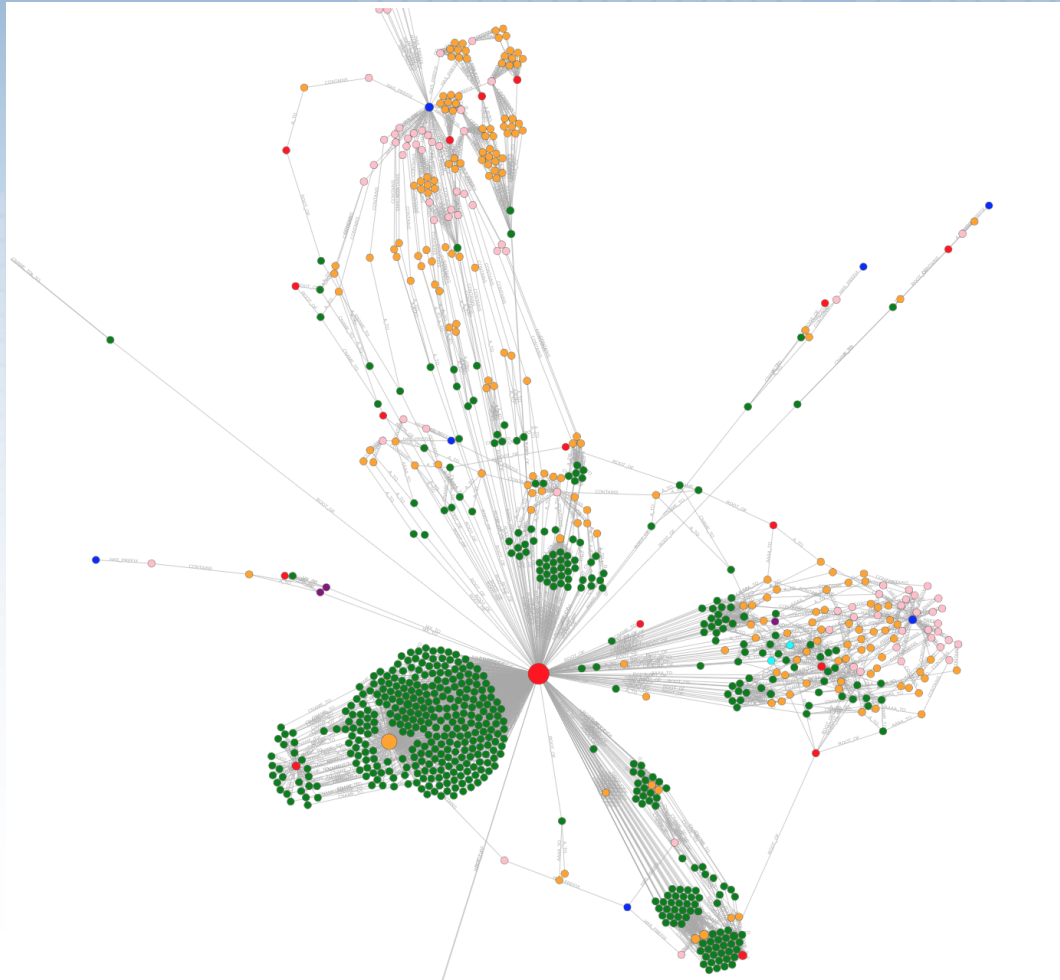
OWASP
Open Web Application
Security Project

Demonstration

- The owasp.org enumeration: https://asciinema.org/a/ P2kuxzy164LgCfc8uL2YtCMoM

- The fb.com enumeration: https://asciinema.org/a/ v6B1qdMRILRUflpkwRPhvCTaY

OWASP
Open Web Application
Security Project

Demonstration Cont.

Demonstration Cont.

Demonstration Cont.

Thank you!

Questions?