Zeek Package Repository Website

ZAM

zeek asset manager

Akiel Aries, Cody Beck,
David Knight, Nathan Chan

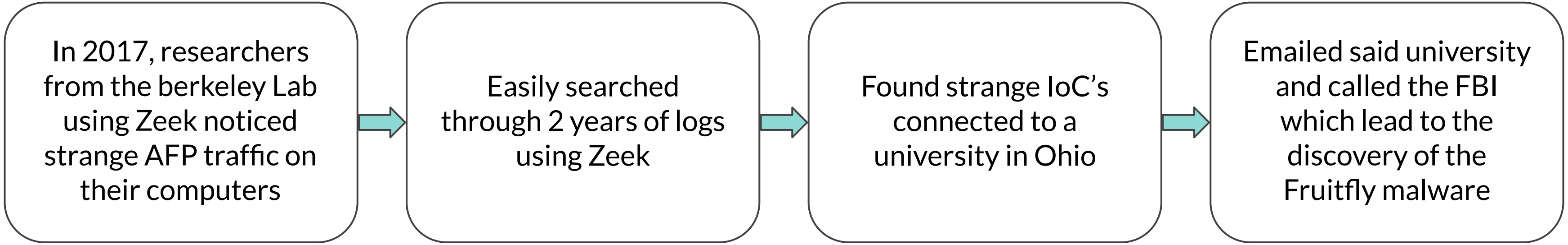
Team Mentor: Daniel Kramer

What is Zeek?

- Network traffic analyzer
- Network security monitor
- Open Source

Meet Our Client: Tim!

- Senior engineer at Corelight
- Release manager for Zeek



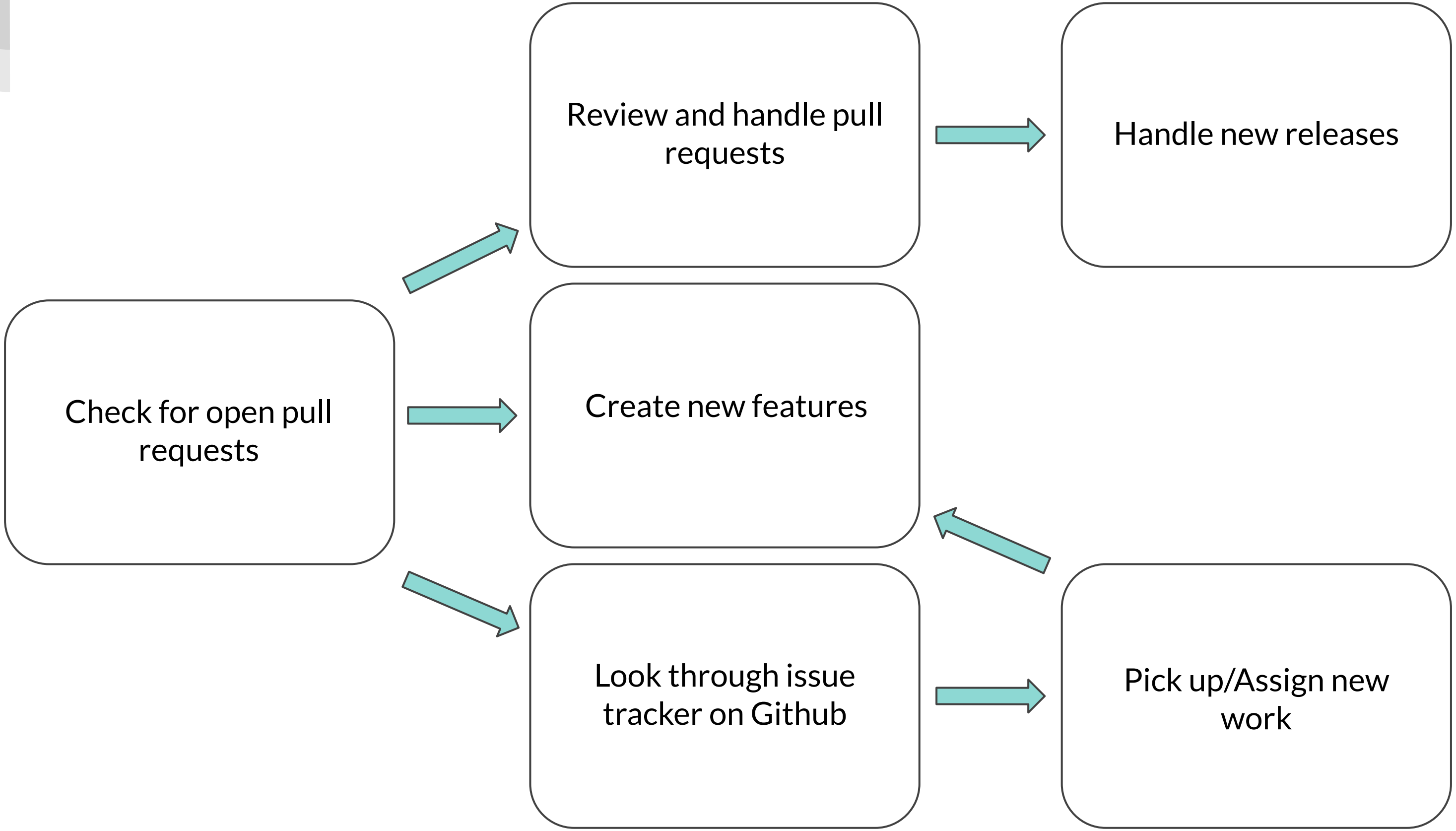
In 2017, researchers from the berkeley Lab using Zeek noticed strange AFP traffic on their computers

Easily searched through 2 years of logs using Zeek

Found strange IoC's connected to a university in Ohio

Emailed said university and called the FBI which lead to the discovery of the Fruitfly malware

Zeek Workflow



Check for open pull requests

Review and handle pull requests

Create new features

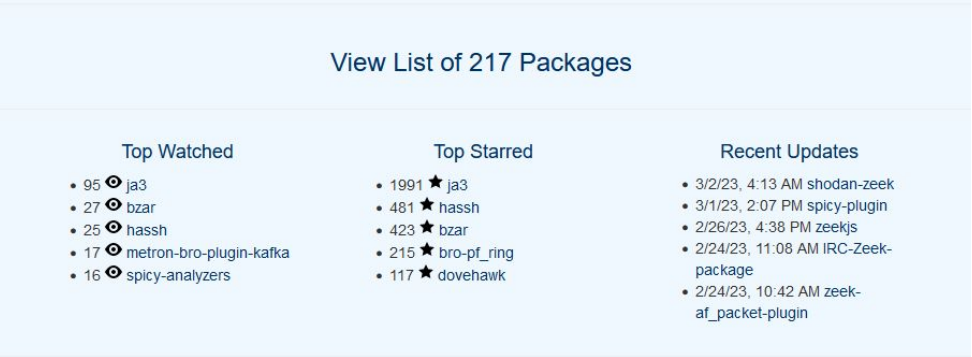
Look through issue tracker on Github

Handle new releases

Pick up/Assign new work

The Problem

- Discoverability of uploaded packages
- Duplicated tags
- Inefficient search engine
- Looks outdated



View List of 217 Packages

Top Watched

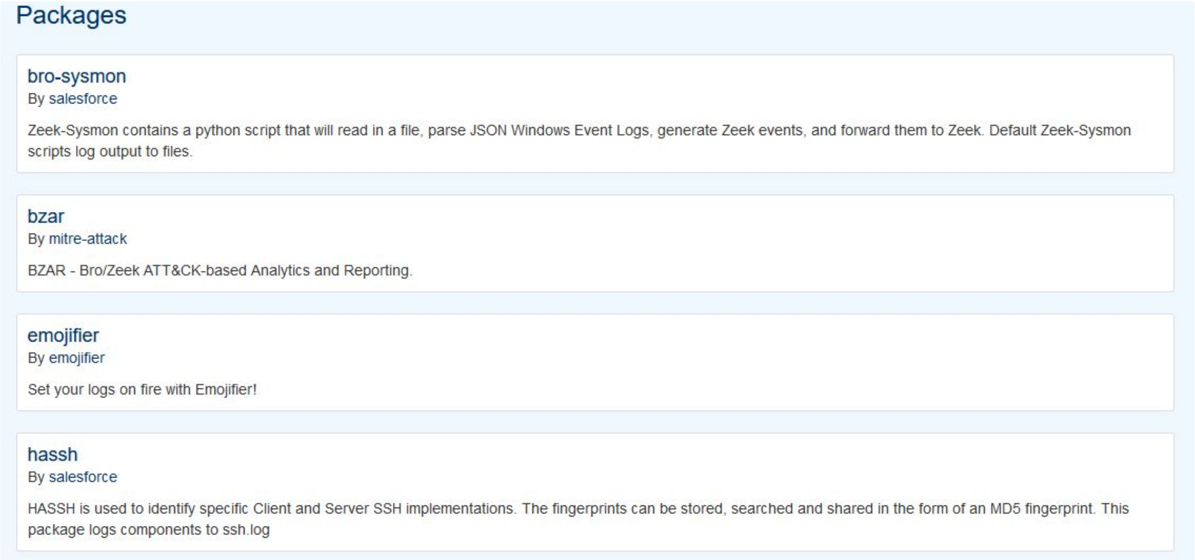
- 95 👁 ja3
- 27 👁 bzar
- 25 👁 hassh
- 17 👁 metron-bro-plugin-kafka
- 16 👁 spicy-analyzers

Top Starred

- 1991 ★ ja3
- 481 ★ hassh
- 423 ★ bzar
- 215 ★ bro-pf_ring
- 117 ★ dovehawk

Recent Updates

- 3/2/23, 4:13 AM shodan-zeek
- 3/1/23, 2:07 PM spicy-plugin
- 2/26/23, 4:38 PM zeekjs
- 2/24/23, 11:08 AM IRC-Zeek-package
- 2/24/23, 10:42 AM zeek-af_packet-plugin



Packages

bro-sysmon
By salesforce

Zeek-Sysmon contains a python script that will read in a file, parse JSON Windows Event Logs, generate Zeek events, and forward them to Zeek. Default Zeek-Sysmon scripts log output to files.

bzar
By mitre-attack

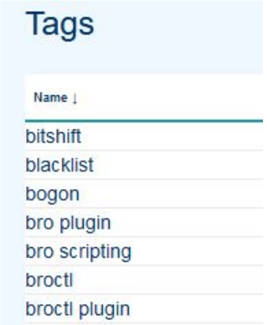
BZAR - Bro/Zeek ATT&CK-based Analytics and Reporting.

emojifier
By emojifier

Set your logs on fire with Emojifier!

hassh
By salesforce

HASSH is used to identify specific Client and Server SSH implementations. The fingerprints can be stored, searched and shared in the form of an MD5 fingerprint. This package logs components to ssh.log



Tags

Name ↓
bitshift
blacklist
bogon
bro plugin
bro scripting
broctl
broctl plugin

Our Solution

- Create an API with a focus on speed and maintainability
- Incorporate a better searching feature
- Use a similar style to the current Zeek.org website
- Automate the site for every new package

HTML

CSS

FastAPI

Jinja

Progression Plan

Requirements:

- Shared requirements document iteratively refined through meetings with the client

Technological Challenges:

- Implementing search functionality
- Storing and serving package information
- Standardizing tags

Other Issues

- Simplicity
- Maintainability
- Discoverability

Thank you!

ZAM

zeek asset manager