Public Entity Network Security Monitoring by Student Security Analysts

Karl Hubbard, Tsuyoshi Baker, Michael Tsikerdekis
Department of Computer Science
Western Washington University

Introduction

The opportunity to monitor live network data has been made available to Computer Science students thanks to the collaboration of Critical Informatics, a private security company, WWU, and the Washington State Fusion Center.

Students in the Advanced Network Security class are taught how to investigate alerts and use Netflow data (condensed IP Packet information) to determine incidents from these alerts. As incidents are found, students learn how to work together using the Mantis ticketing system to further investigate incidents with their peers.

Over the course of the Spring 2018 quarter, over 100 tickets have been created and investigated by students. 10 of them have resulted in escalation, being forwarded to the Washington State Fusion Center.

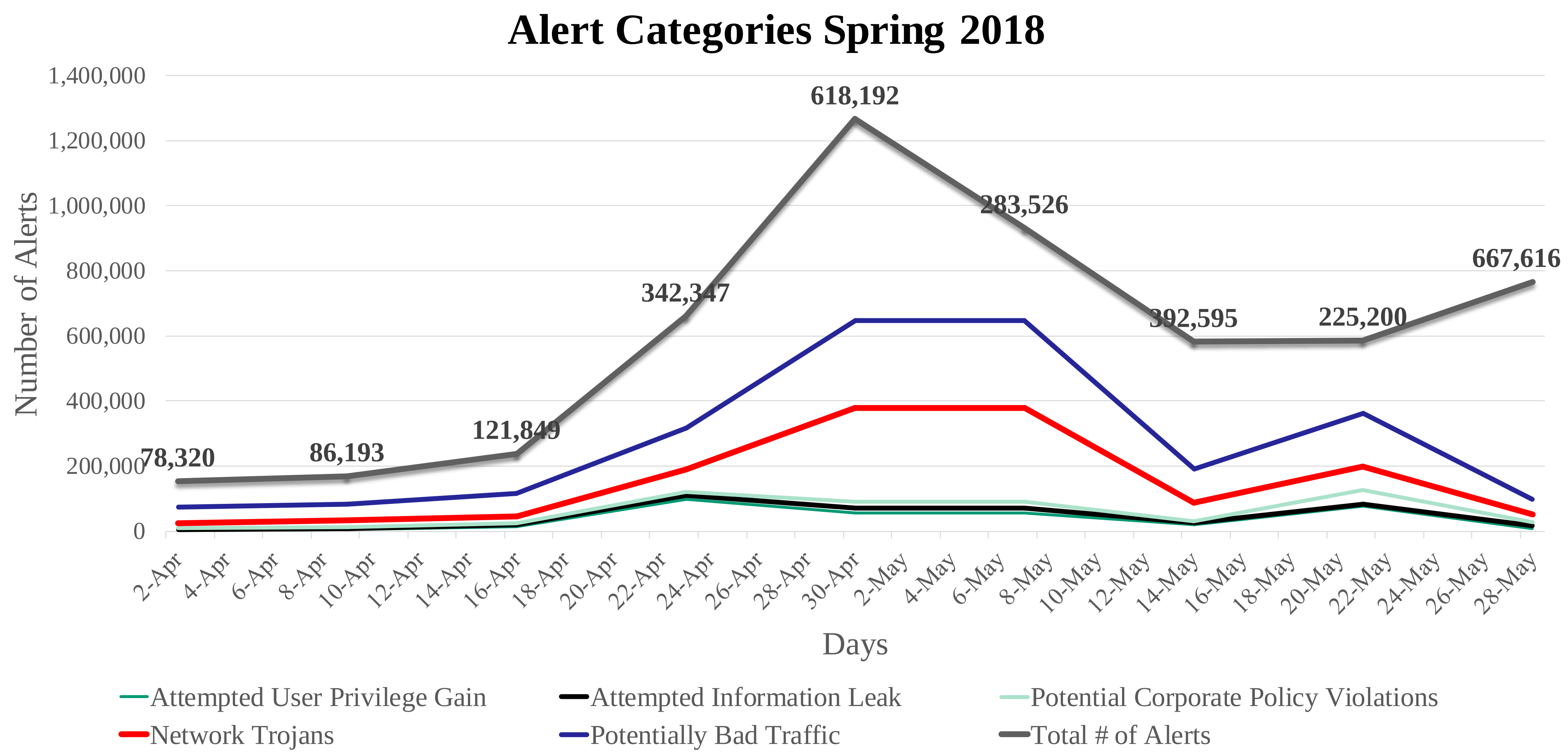


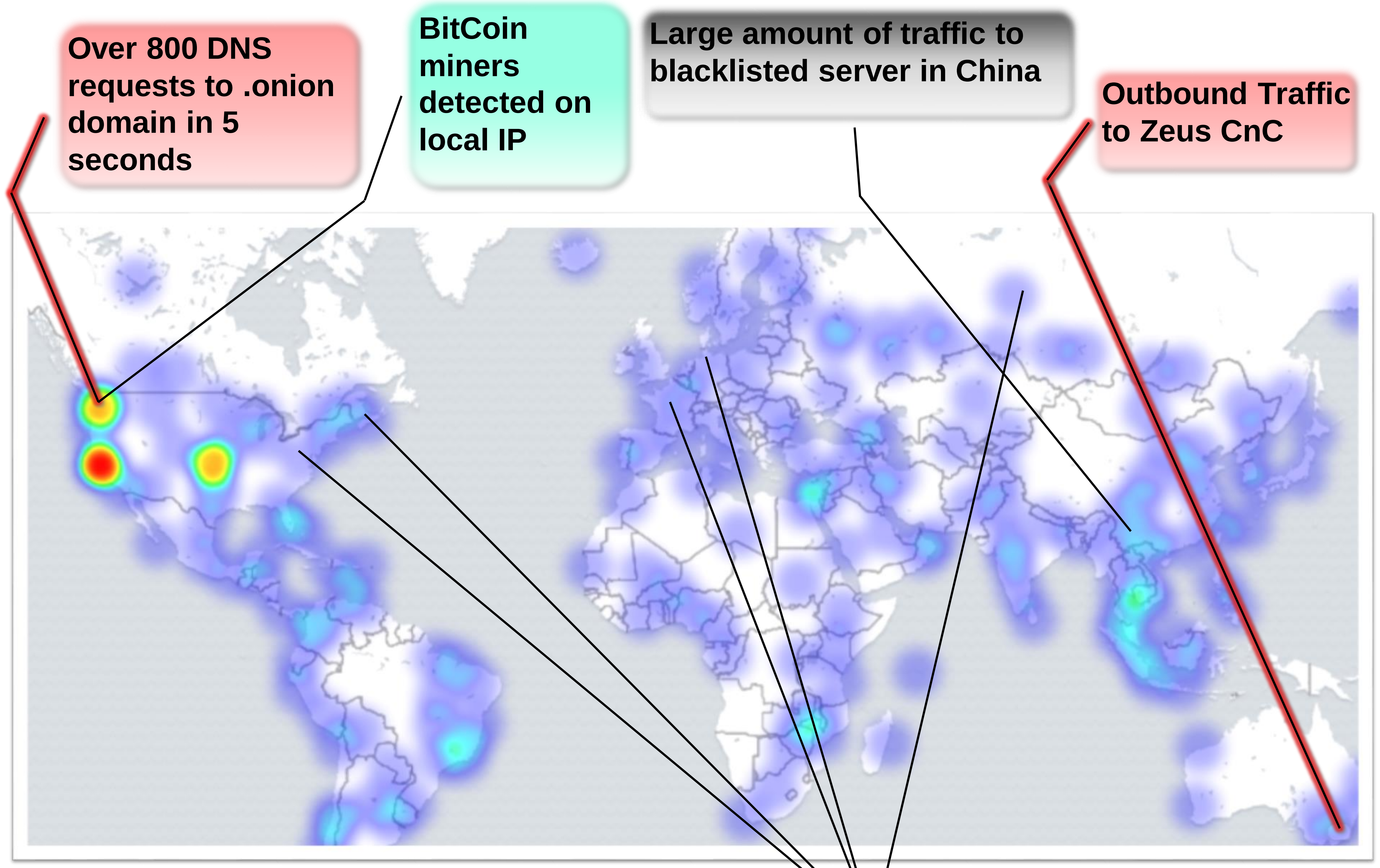
Figure 1. Graph of Alerts per Day by popular categories. Totaling ~3million alerts over ~50TB of data.

Learning using Real vs. Simulated Data

What are the learning differences with Real vs. Simulated Data?

	Real	Simulated
Pros	• Real Data provides more holistic view of traffic trends • Greater overall learning value and sense of accomplishment for students who detect malicious traffic in the wild • Data will always provide an accurate view of current threat trends	• Less False Alarms • Easier to achieve learning outcomes when data content is known • Easier point of entry for new students
Cons	• Many more false alarms than actual noteworthy activity • Students did not have access to full packet capture data	• Strictly *less* overall experience value • Creates an exaggerated perception of how often high-caliber attacks occur

Figure 3. Pros/Cons of Real vs. Simulated Data



Over 800 DNS requests to .onion domain in 5 seconds

BitCoin miners detected on local IP

Large amount of traffic to blacklisted server in China

Outbound Traffic to Zeus CnC

Figure 2. Traffic Map with key reported incidents.

DDOS Attempts on Port 123 from various locations

Conflicts and Issues

There are a number of difficulties which have effects on the project

Configuration Issues

Each location has a unique set of networking hardware. This makes implementation difficult and can lead to misconfigured sensors. This causes data at those locations to be at best inconsistent, and at other times entirely useless.

Student Availability

Access to this project is currently limited to one class, and network monitoring on the system doesn't begin until about 2 weeks in. With no students monitoring the flows in between classes, this decreases the overall value of network monitoring for these municipalities.

Fortunately, there are plans to create a club based around this project. With the addition of this and a project intern somewhere down the line, the project will see more consistent monitoring.