

Telematics for Risk Scoring Cyber Attacks

Heeyun Kim*, Siddhartha R Dalal, Vishal Misra, Dan Rubenstein
Department of Computer Science | Columbia University

Introduction

Cyber-attacks including ransomware and other attacks have surged dramatically in last few years. In 2025 it is expected that the total costs of cyber insurance world-wide will go to over \$25 billion. However, the insurance companies so far do not have good tools to assess the riskiness of their clients. The objective of this research is to create a telematics like service which will automatically measure real risks faced by a particular enterprise.

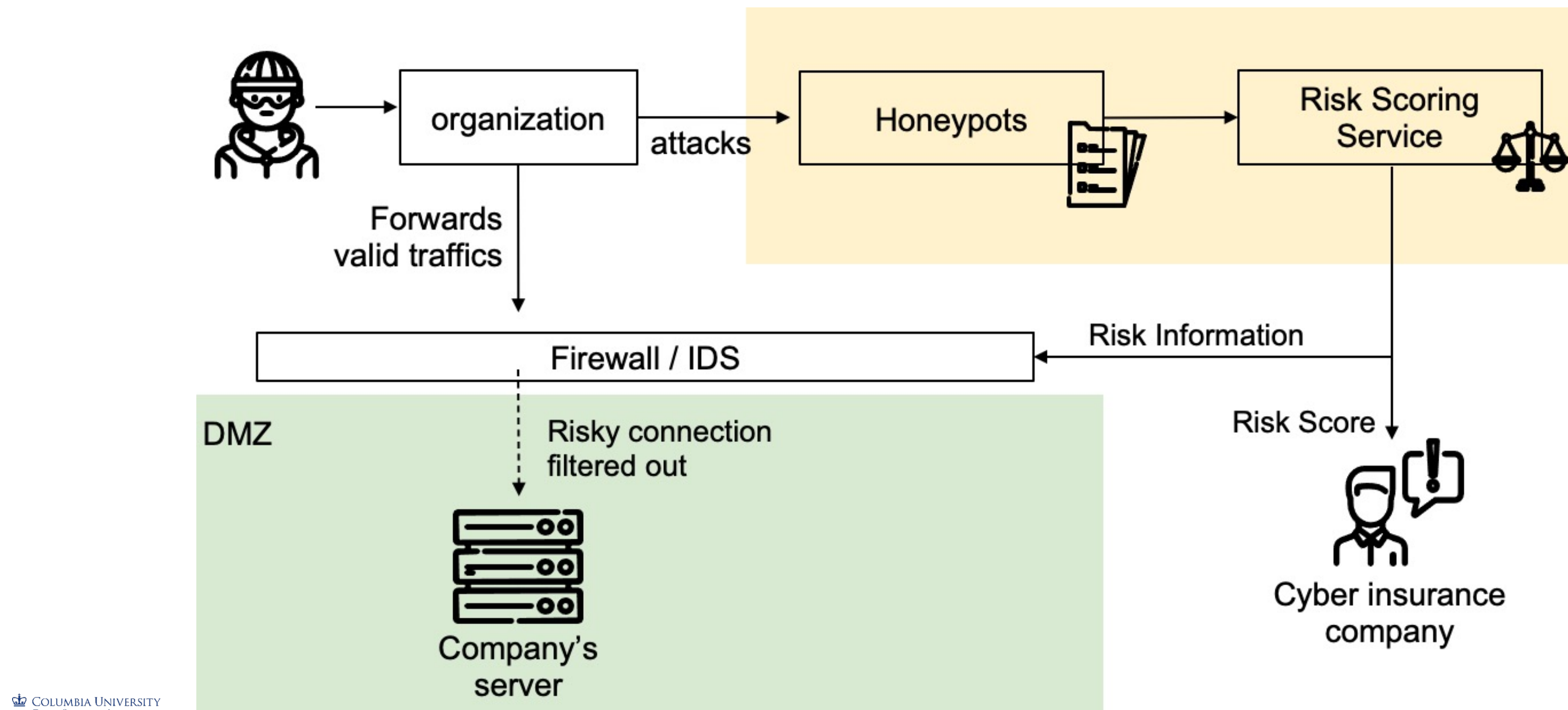


Figure 1. The flow of the enterprise cyber risk scoring

Network Architecture

The honeypots are placed in three crucial positions of the Columbia Network.

- (1) Open to internet and interacts with all connections.
- (2) Standard Zone blocks connections to certain ports that Columbia security standard defines as unnecessary / unsecure.
- (3) Redirected connection from the "load balancer" of CS department's enterprise zone.

This setup helps in detecting skillful attackers and flaws in enterprise's IDS/IPS systems.

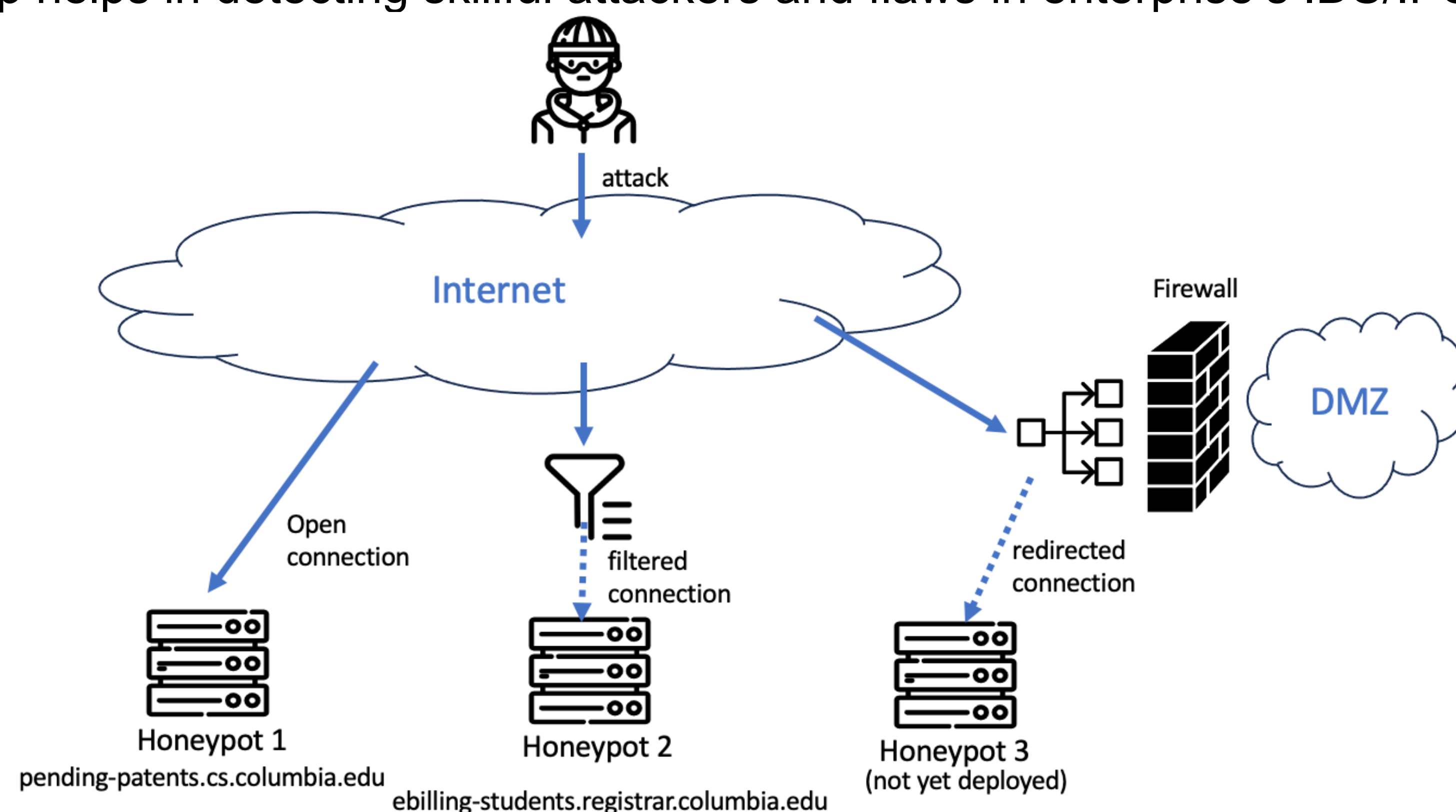


Figure 2. Honeypot locations in the network.

Attacks and Patterns

We monitored HTTP requests, TLS/SSL exchanges, DNS queries, SMTP connections. Each attack is a sequence of actions and each action is categorized as through Suricata IDS categorization system.

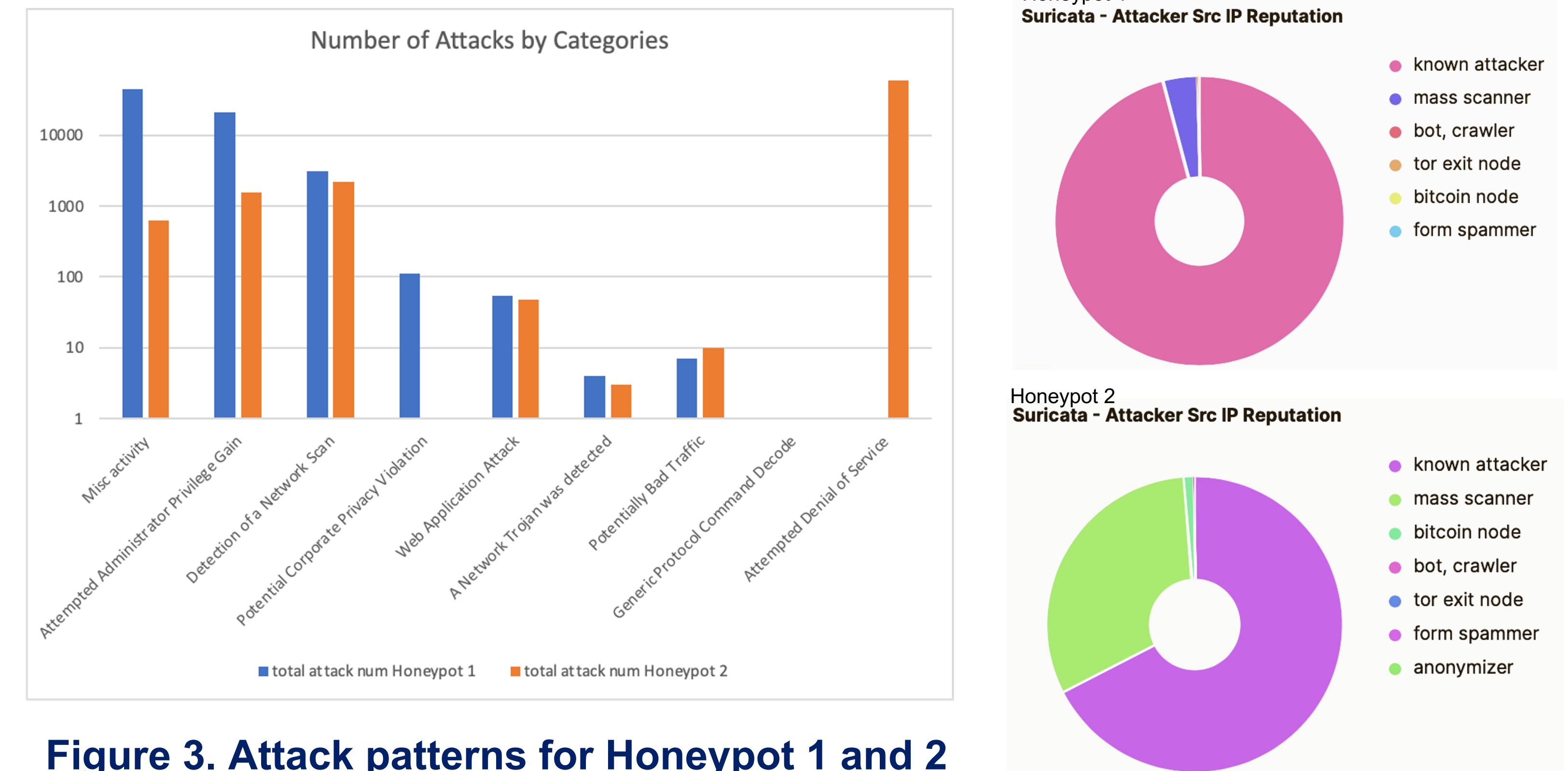


Figure 3. Attack patterns for Honeypot 1 and 2

Risk Scoring

Suricata IDS has 1:1 risk scoring for each incoming attacks based on the category. The table below shows sum of the risk scores by category of the attack.

Category	Sum Risk		Normalized (sum risk/incident count)	
	honeypot 1	honeypot 2	honeypot 1	honeypot 2
Attempted Administrator Privilege Gain	83256	6188	45.95%	3.23%
Potential Corporate Privacy Violation	339	0	0.19%	0.00%
Web Application Attack	220	192	0.12%	0.10%
A Network Trojan was detected	16	12	0.01%	0.01%
Attempted Denial of Service	0	179730	0.00%	93.68%
Potentially Bad Traffic	21	30	0.01%	0.02%
Misc activity	90920	1274	50.18%	0.66%
Detection of a Network Scan	6310	4426	3.48%	2.31%
Generic Protocol Command Decode	2	0	0.00%	0.00%
SUM	181177	191852		

Table 1. Sum of risk scores by attack categories

Red: high severity, yellow: medium severity, green: low severity

Future Work

- Filter out the background radiation of insignificant attacks such as mass scanner.
- Create a method of risk scoring system based on the payload of attack rather than 1:1 scoring system based on the attack category.

References

- Bove, Davide. "Using Honeypots to Detect and Analyze Attack Patterns on Cloud Infrastructures." Security Research Group Department of Computer Science Friedrich-Alexander University Erlangen-Nürnberg (2018).
- Salles-Loustau, Gabriel, et al. "Characterizing attackers and attacks: An empirical study." 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing. IEEE, 2011.