



Adaptive Malware Classification Using Bandit Feedback

Kyle Lemmons^{1*}, Rohan Mittal^{1*}, João Hespanha¹

1. UC Santa Barbara
*Equal contribution

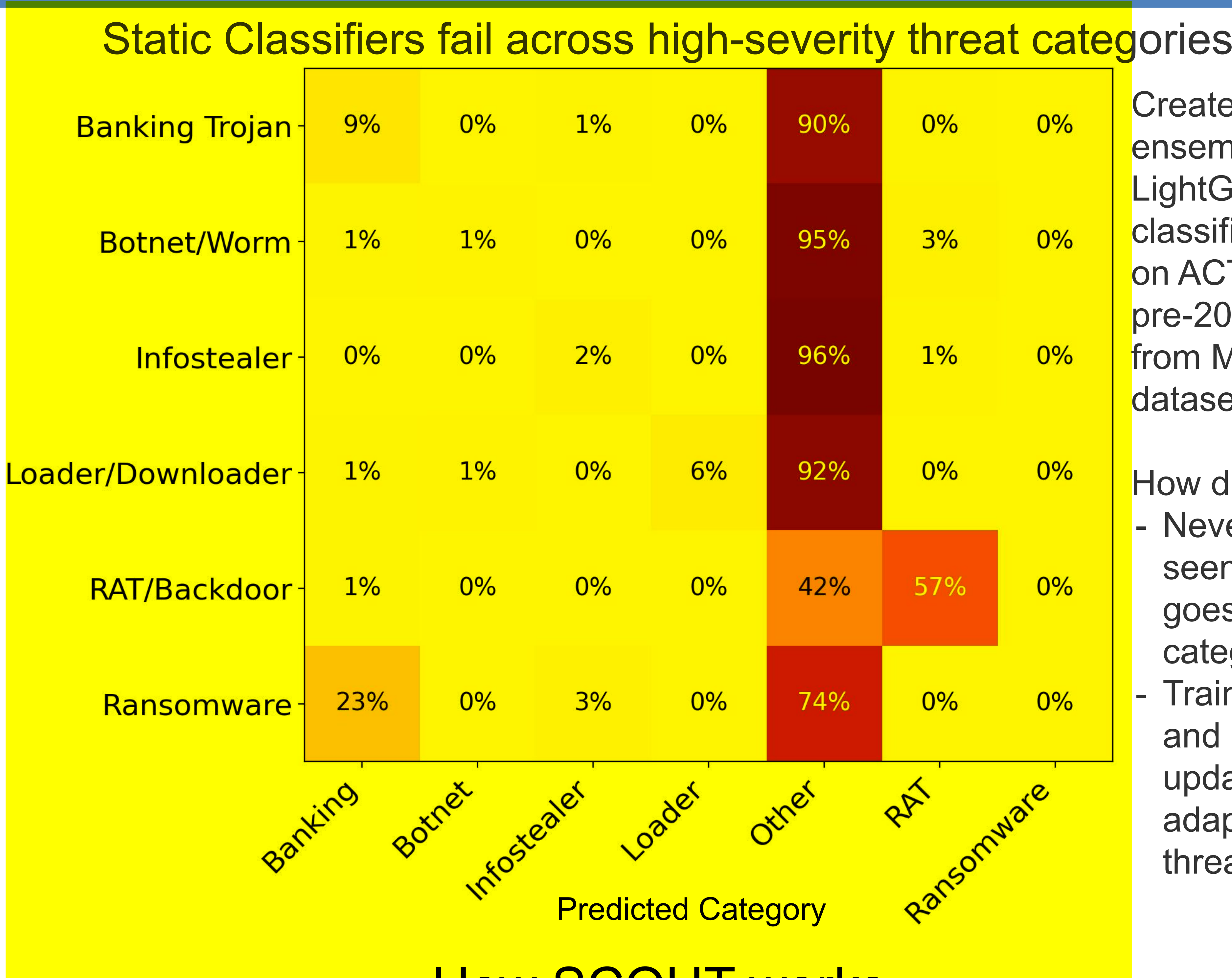
Background

- Antivirus systems flag malware by learning patterns from known threats, so attackers adapt, creating a cat-and-mouse game
- Bandit algorithms: updates itself automatically after every decision, only using the feedback it receives from the one choice it made.
- Aim: Build a bandit-driven system that adapts to evolving malware in a non-stationary environment

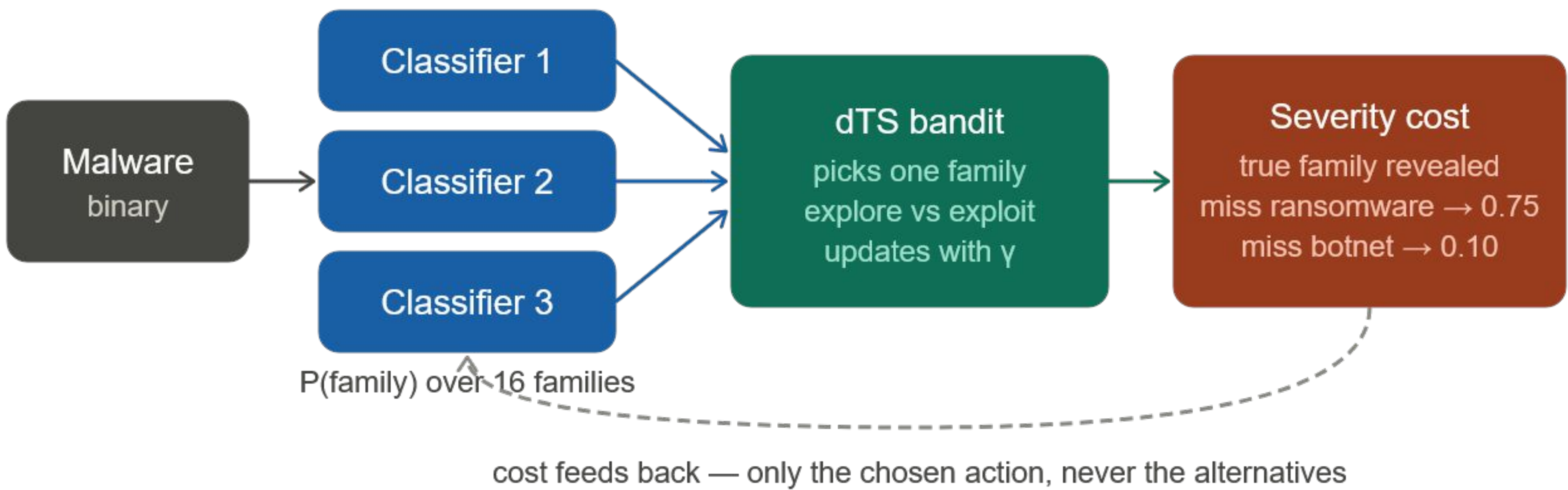
Approach

- Three classifiers analyze each malware binary and output a probability distribution over 16 malware families
- Bandit algorithm: SCOUT, built on discounted Thompson Sampling (dTS)
 - Chooses one of 16 malware families
 - Balances exploiting the best performing family vs exploring new families using a weighted probability distribution
 - Updates with γ (discount factor) to weigh recent vs old decisions

True Category



How SCOUT works



SCOUT = Severity-aware Classifier Orchestration Using Thompson-sampling; "dTS bandit" above refers to its core algorithm.

Conclusions

- Adaptive bandit learning outperforms static classifiers by ~22% while receiving less information
- Reduced severity-weighted cost by 47% compared to random guessing (0.158 vs 0.296)
- Cost spikes align with new malware families, simulating non-stationarity
- Future work: the bandit's action set isn't limited by what any one classifier can name and it could in principle learn to identify malware families no individual classifier was ever trained to recognize.

References

- [1] B. Anderson and J. P. Hespanha, "Boltzmann Learning of Contextual Games," *Proceedings of the IEEE Conference on Decision and Control (CDC)*, 2023.
- [2] R. Raj and S. Kalyani, "Taming Non-stationary Bandits: A Bayesian Approach," *arXiv preprint arXiv:1707.09727*, 2017.
- [3] Y. Russac, C. Vernade, and O. Cappé, "Weighted Linear Bandits for Non-Stationary Environments," *Advances in Neural Information Processing Systems (NeurIPS)*, 2019.

