CAREER: Developing Robust Longitudinal Indicators and Early Warnings of Cybercrime

Challenge:

- Is cybersecurity getting better or worse over time?
- How can we gather data to answer the question empirically for combating cybercrime?

Solution:

- Gather and analyze longitudinal data on defender efforts (e.g., time to remediate)
- Multiple datasets: web-based malware, business-email compromise, inferred losses from cyber insurance prices
- Identify evidence of target selection early

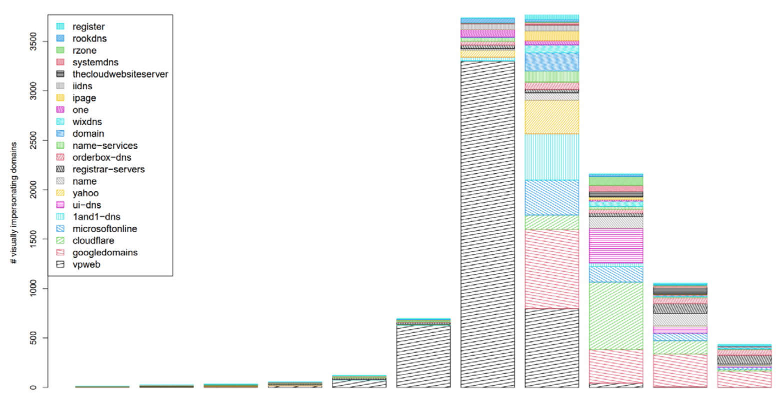
PI: Tyler Moore, Award: 1652610

Contact: tyler-moore@utulsa.edu

Compare Defender Efforts

HP	# URLs	Days to Clean	Recomp. Rate
1	87,486	31	1.77%
2	72,921	60	3.30%
3	40,112	128	1.24%
4	34,504	10	0.496%
5	32,720	69	2.65%
6	30,328	63	2.77%
7	30,100	20	4.46%
8	29,541	6	3.24%
9	21,957	223	0.587%
10	21,162	77	0.841%
Median for HPs >1K URLs		36	2.26%

Track Efforts Over Time



Scientific Impact:

- Advancing understanding of how to collect reliable cybercrime indicators
- Effort-based indicators could mitigate information asymmetries about defender performance

Broader Impact and Broader Participation:

- Improves understanding of what security data should be collected and how best to share it
- Business-email compromise (BEC) attacks are the most prevalent cyber threat facing businesses today
- This research suggests countermeasures that could greatly improve resilience to BEC attacks