VCAF: Expanding the ATT&CK Framework to Cover VERIS Threat Action Varieties

Alex Pinto – Security Data Scientist – Verizon - @alexcpsec
Gabe Bassett – Security Data Scientist – Verizon - @gdbassett

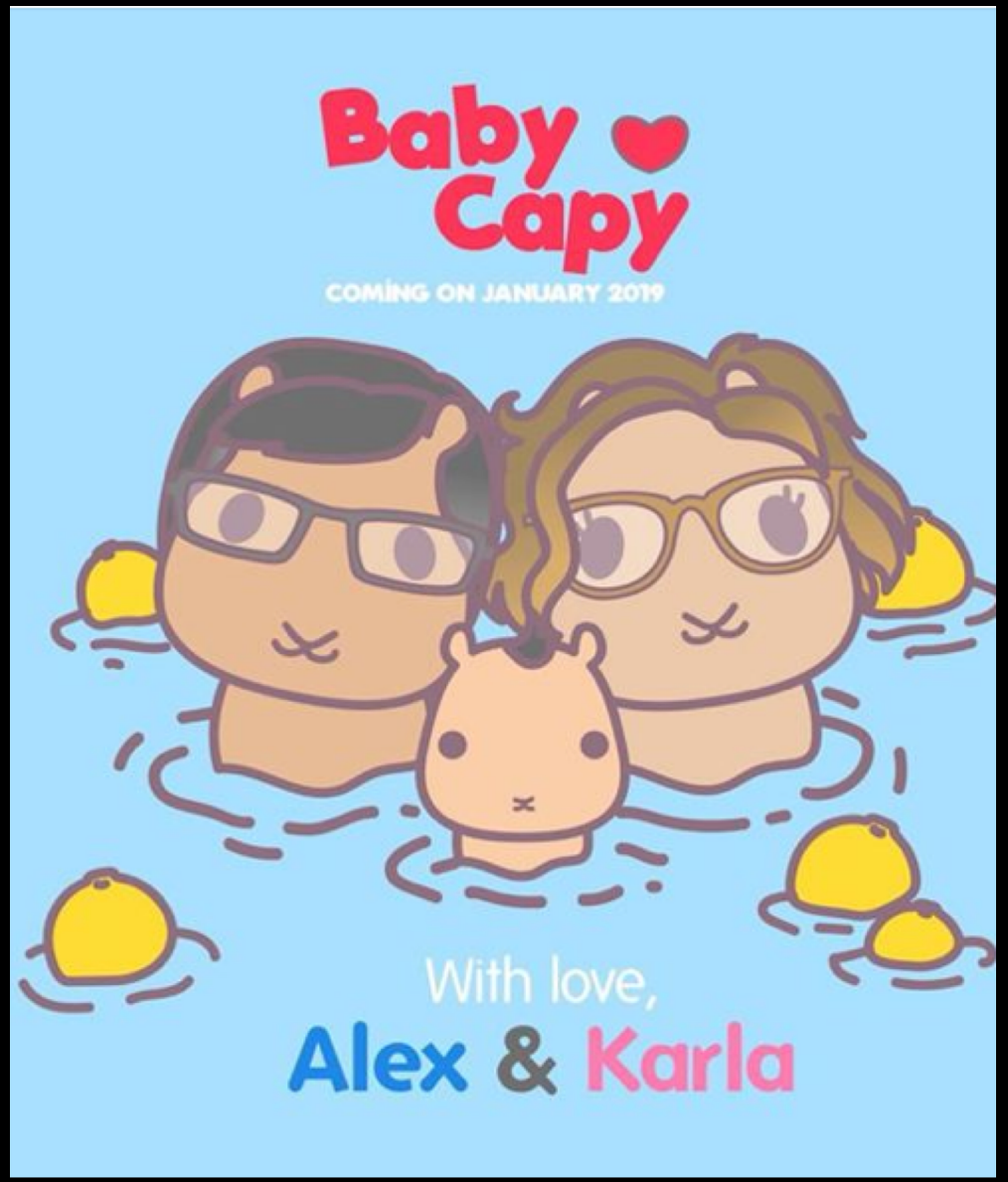
Your Humble Speakers

- Alex Pinto
  - Data-driven Capybara Enthusiast

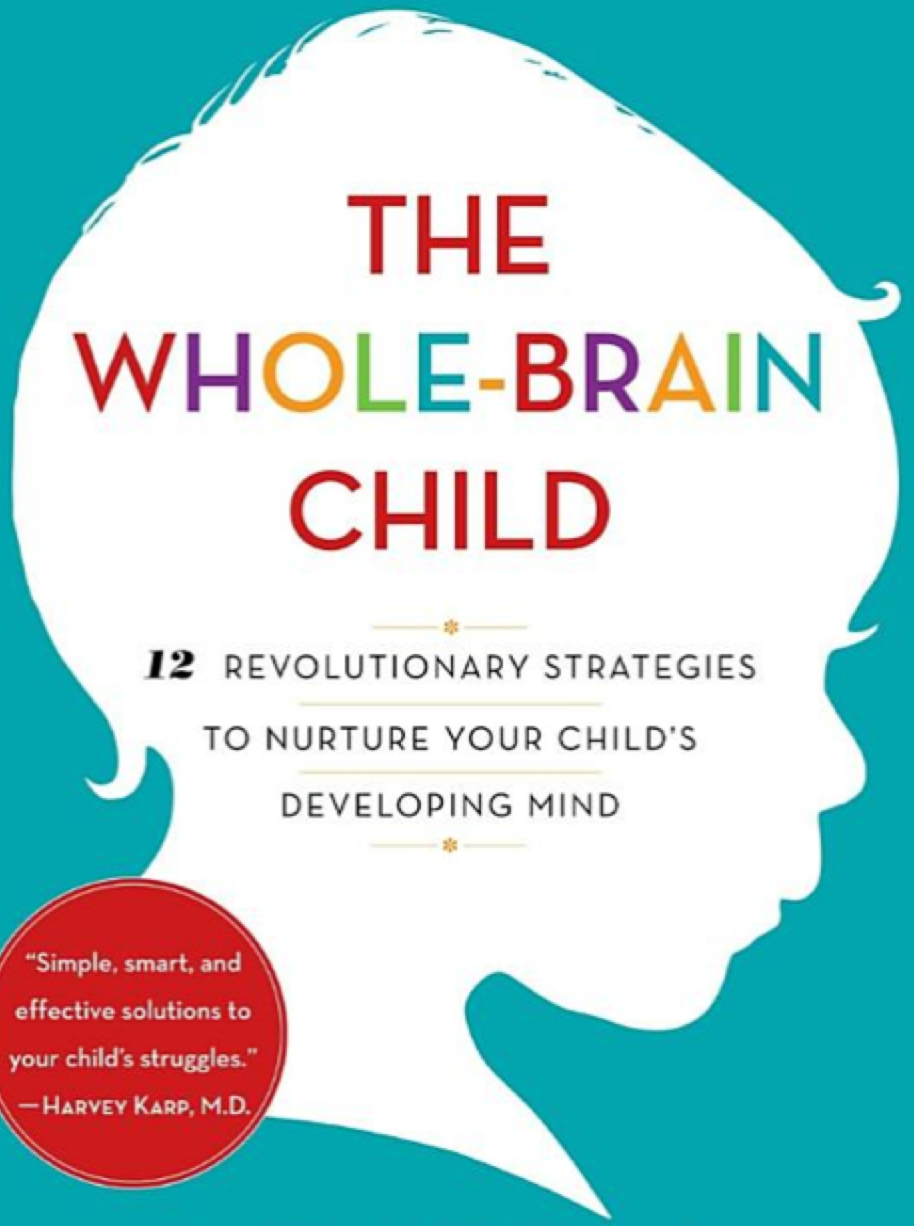
- Gabe Bassett
  - Voted most likely to create Skynet in HS


JUDGE


Gabe The Engineer
@gdbassett
Following
Adabelle Bassett born yesterday at 8:38pm.
7lb 2oz, 18in
5:33 AM - 6 Oct 2018
1 Retweet 88 Likes
25
1
88


Baby Capy
COMING ON JANUARY 2019
With love,
Alex & Karla

NEW YORK TIMES BESTSELLER



THE WHOLE-BRAIN CHILD

12 REVOLUTIONARY STRATEGIES TO NURTURE YOUR CHILD'S DEVELOPING MIND

"Simple, smart, and effective solutions to your child's struggles."
—HARVEY KARP, M.D.

DANIEL J. SIEGEL, M.D.,

“Assume compromise! Everybody is Owned all the time! Buy my products!!”

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

“Through adversary simulation we have determined that there are control deficiencies on your detection of Persistence techniques on MacOS and those should be remediated.”

53,000+ incidents

2,200~ breaches

1 very brave data cleansing and classifying team

(https://www.verizonenterprise.com/verizon-insights-lab/dbir/)

Breaches Over Time

Show

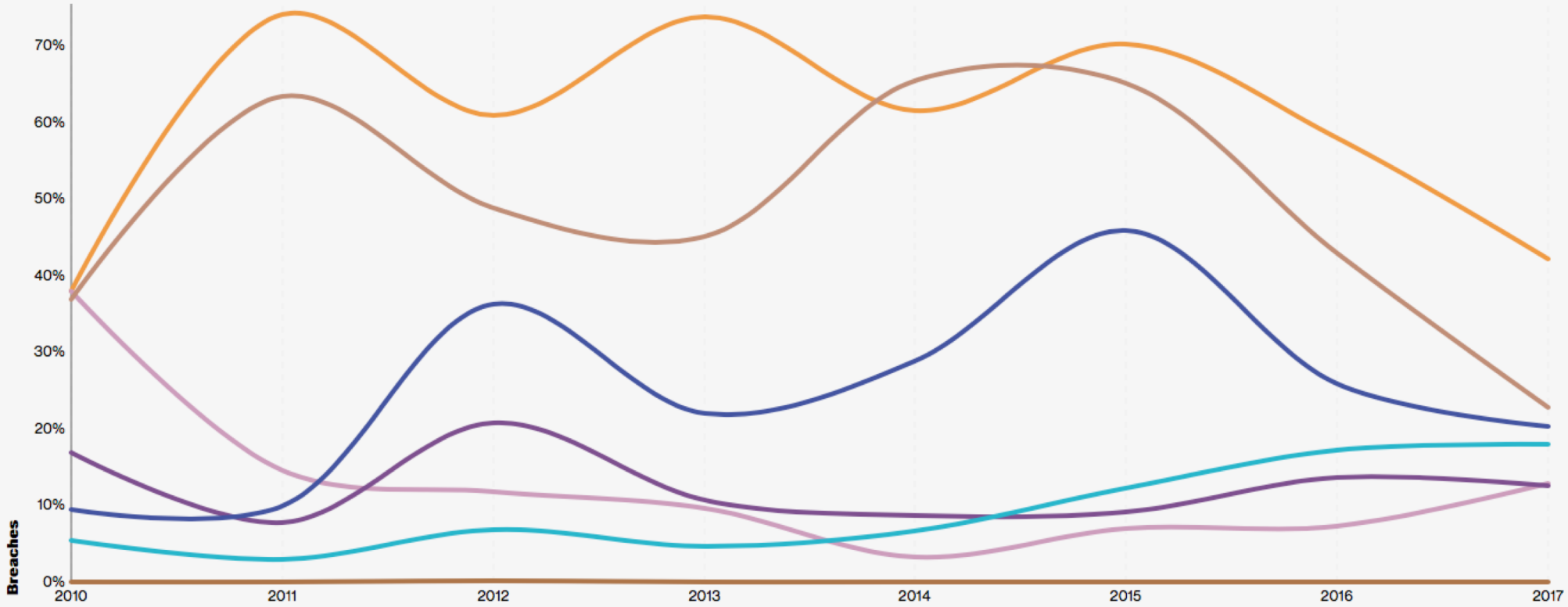
Actions | Actors | Assets | Attributes

Measure

Ratio | Value

- Hacking
- Physical
- Malware
- Misuse
- Social
- Error
- Environmental

Breach trends is a retrospective look over the last several years at various components of data breaches. Specifically, the threat actors involved and the actions they leveraged, along with the assets that were impacted, and the corresponding attributes compromised.



(http://www.verizonenterprise.com/verizon-insights-lab/dbir/tool/)

Motive Breakdown By Action Subcategory

Show

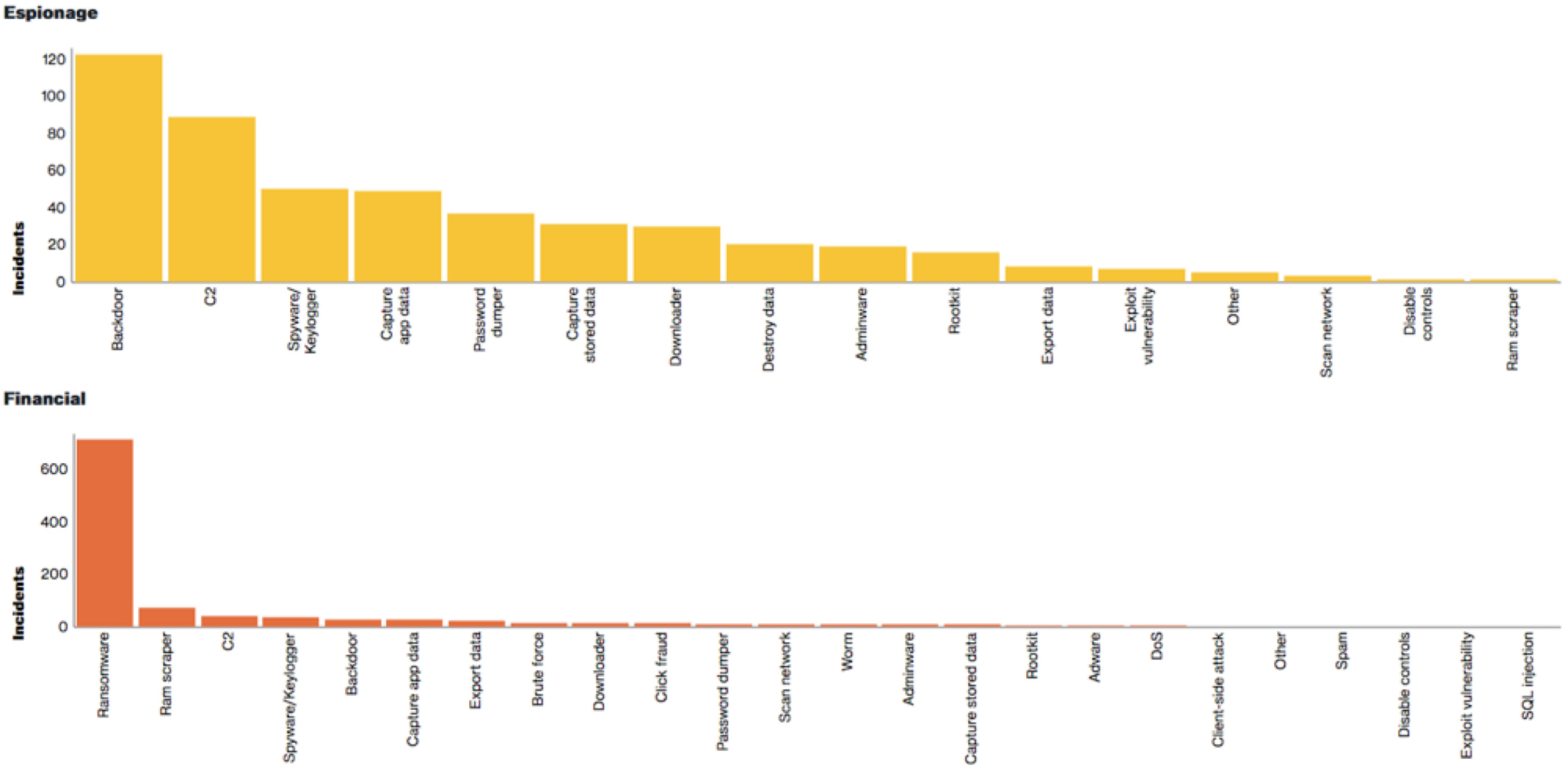
Variety | Vector

Incidents | Breaches

Action

Malware

Actors behave differently depending on their motivation. Understanding the factors that motivate the actors helps to determine the actions associated with them, and that knowledge can help you better tune your defenses.



(http://www.verizonenterprise.com/verizon-insights-lab/dbir/tool/)

(http://veriscommunity.net/)

VERIS

the vocabulary for event recording and incident sharing

- **Malware**
- Hacking
- Social
- Misuse
- Physical
- Error
- Environmental

ACTION.MALWARE.VARIETY

Adware: Adware

Backdoor: Backdoor (enable remote access)

Brute force: Brute force attack

Capture app data: Capture data from application or system process

Capture stored data: Capture data stored on system disk

Client-side attack: Client-side or browser attack (e.g., redirection, XSS, MitB)

Click fraud: Click fraud or Bitcoin mining

ACTION.HACKING.VARIETY

Abuse of functionality: Abuse of functionality

Brute force: Brute force or password guessing attacks

Buffer overflow: Buffer overflow

Cache poisoning: Cache poisoning

Session prediction: Credential or session prediction

CSRF: Cross-site request forgery

XSS: Cross-site scripting

Cryptanalysis: Cryptanalysis

ACTION.ENVIRONMENTAL.VARIETY

Deterioration: Deterioration and degradation

Earthquake: Earthquake

EMI: Electromagnetic interference (EMI)

ESD: Electrostatic discharge (ESD)

Temperature: Extreme temperature

Fire: Fire

Flood: Flood

Hazmat: Hazardous material

Humidity: Humidity

Hurricane: Hurricane

Ice: Ice and snow

Landslide: Landslide

Lightning: Lightning

Meteorite: Meteorite


Risk
TROOPS FOR CARDS
5
2
3
7
2
Risk
GEASE FIRE
Risk

Unstructured breach data

VERIS

Prioritized view of high level “threats” you and your industry are subjected to

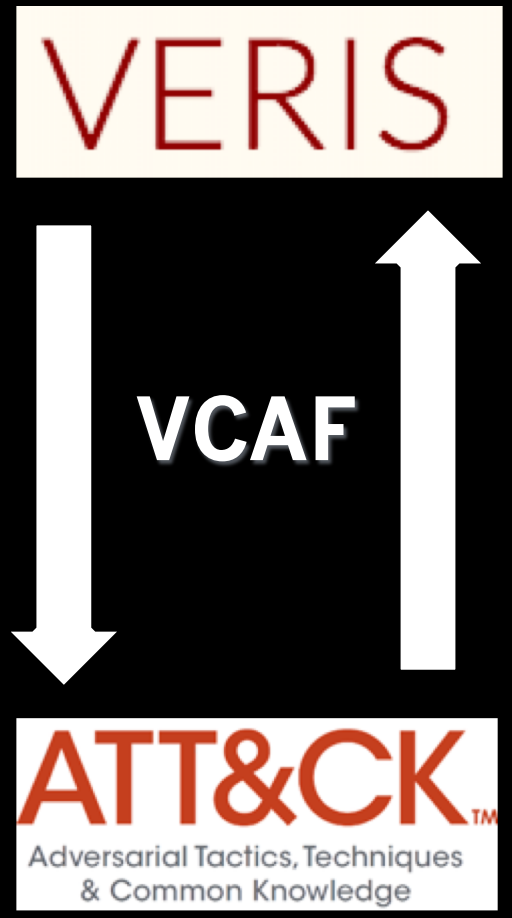
Network / EDR based telemetry analysis Attack Simulation

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

Atomic measurable control classification

☕ VCAF ☕
VERIS Common Attack Framework

Identify and quantify ATT&CK type techniques for more every-day type attacks



Connect the Strategic (VERIS) to the Tactical (ATT&CK)

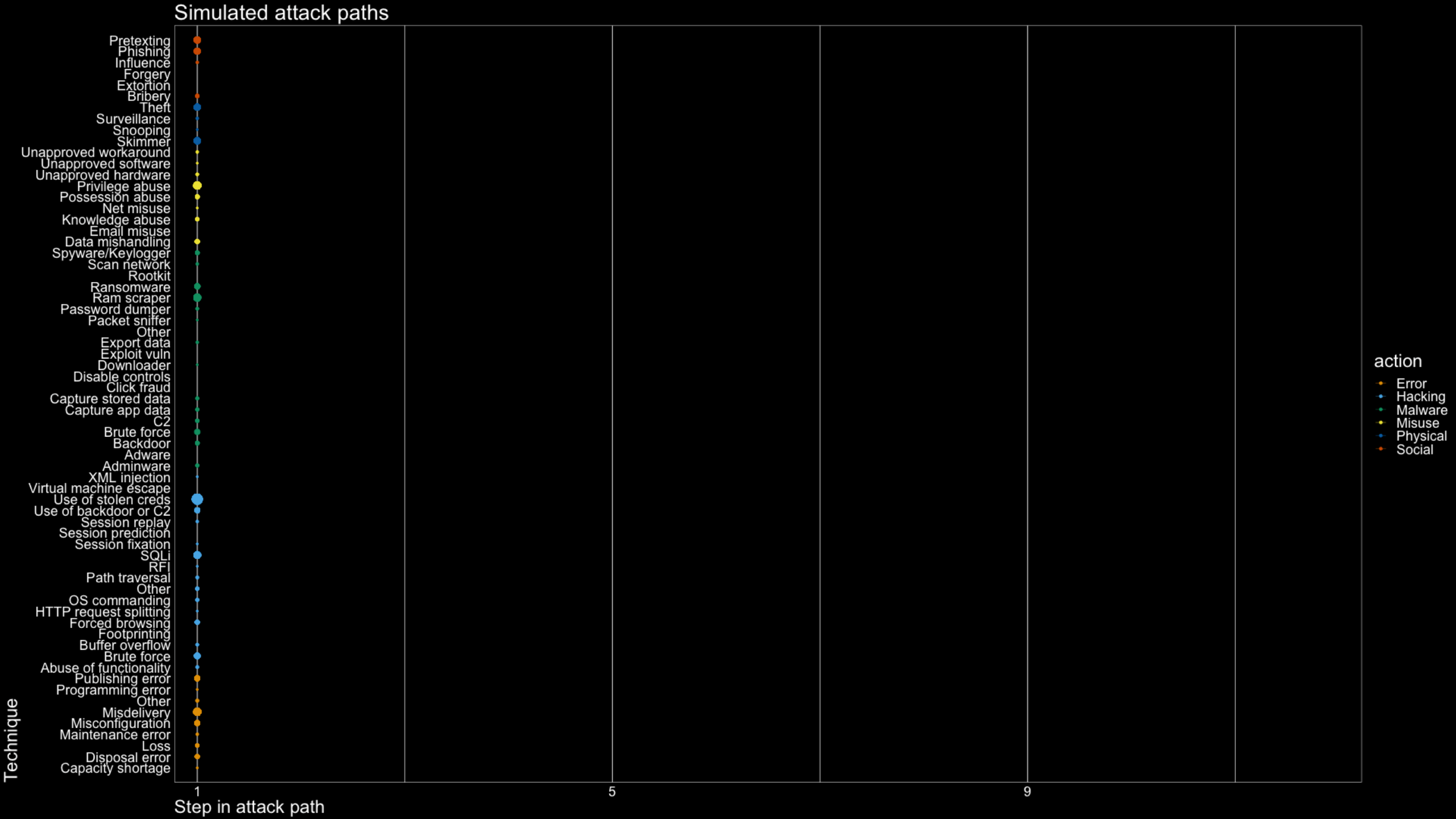
ATT&CK for the Average Joe

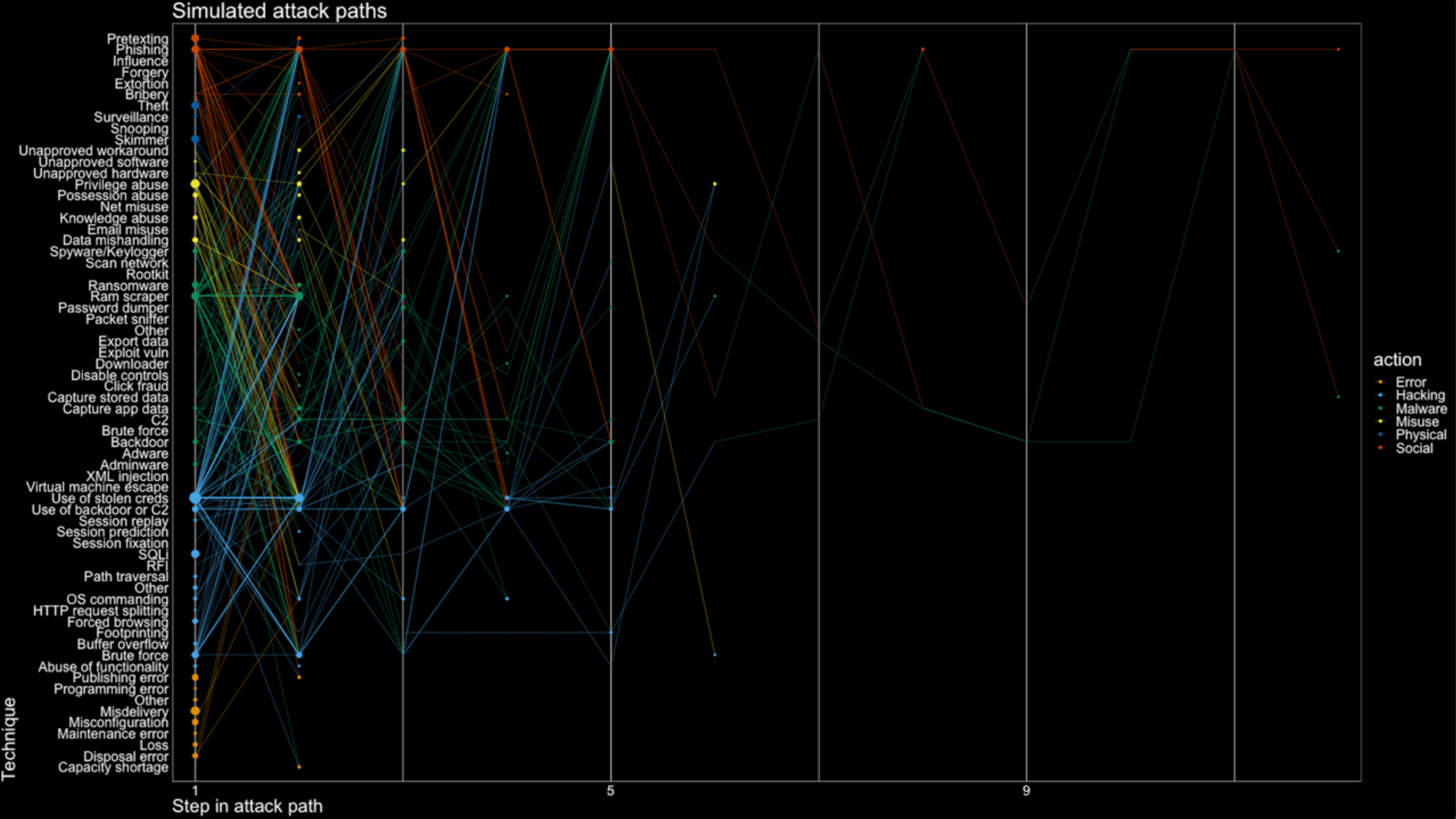
- ATT&CK is way too focused on “APT-level” threats.
- Ability to expand the taxonomy through specific popular TAVs to provide more granularity
- PRE-ATT&CK does cover a few of those:
  - Phishing <-> Phishing
  - Establish / Maintain Infra <-> part of “C2”

Strategic + Tactical

- Automatic collection of attack patterns allows us to use DBIR-like machinery from structured telemetry data.
- Pinpoint industry likelihood tied to VERIS + VCAF + ATT&CK can help direct prioritization of what controls / detective measure someone should do first.


DOUBL


Simulated attack paths
Pretexting
Phishing
Influence
Forgery
Extortion
Bribery
Theft
Surveillance
Snooping
Skimmer
Unapproved workaround
Unapproved software
Unapproved hardware
Privilege abuse
Possession abuse
Net misuse
Knowledge abuse
Email misuse
Data mishandling
Spyware/Keylogger
Scan network
Rootkit
Ransomware
Ram scraper
Password dumper
Packet sniffer
Other
Export data
Exploit vuln
Downloader
Disable controls
Click fraud
Capture stored data
Capture app data
C2
Brute force
Backdoor
Adware
Adminware
XML injection
Virtual machine escape
Use of stolen creds
Use of backdoor or C2
Session replay
Session prediction
Session fixation
SQLi
RFI
Path traversal
Other
OS commanding
HTTP request splitting
Forced browsing
Footprinting
Buffer overflow
Brute force
Abuse of functionality
Publishing error
Programming error
Other
Misdelivery
Misconfiguration
Maintenance error
Loss
Disposal error
Capacity shortage
Technique
1
5
9
Step in attack path
action
Error
Hacking
Malware
Misuse
Physical
Social

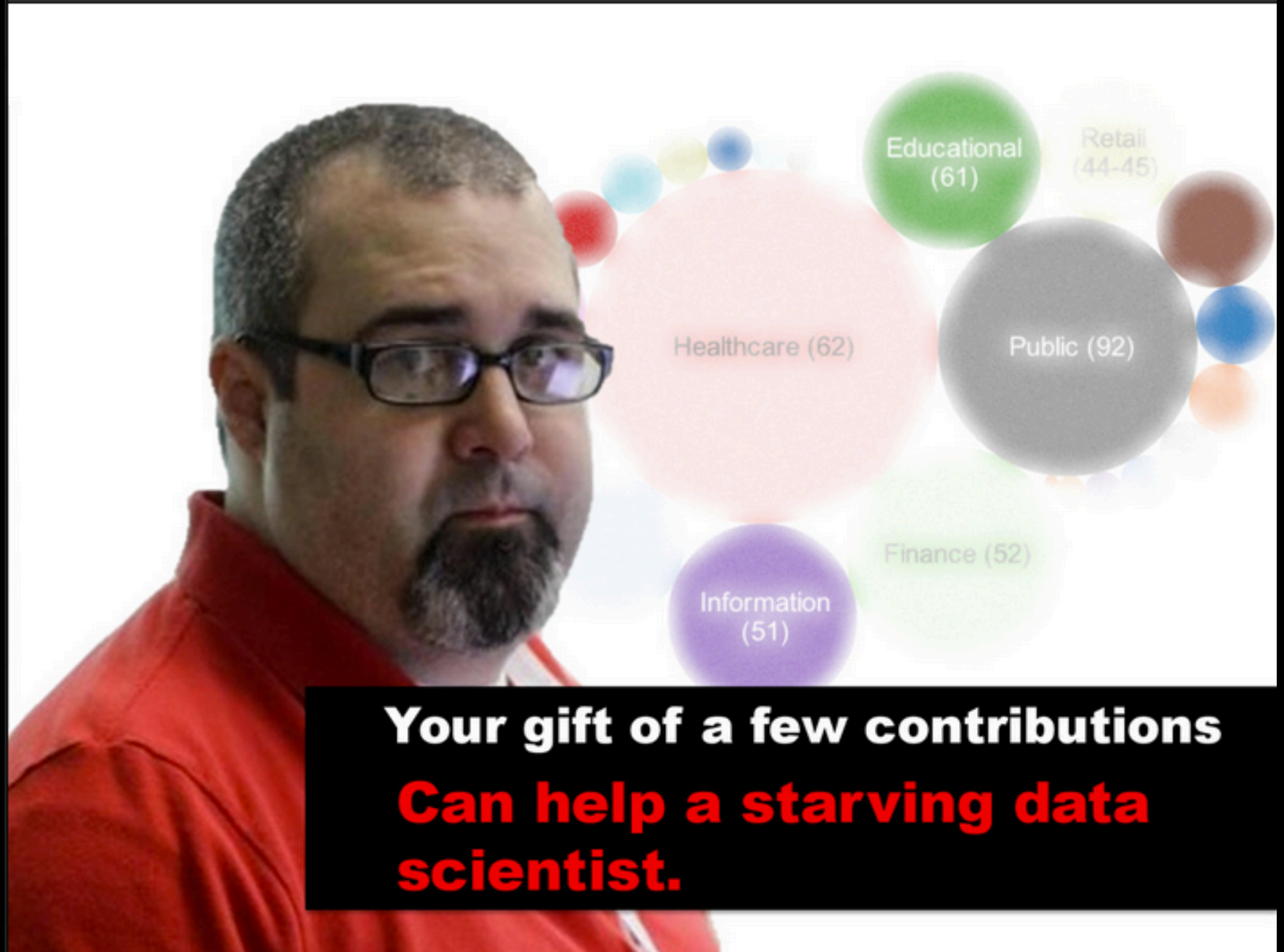

Simulated attack paths
Pretexting
Phishing
Influence
Forgery
Extortion
Bribery
Theft
Surveillance
Snooping
Skimmer
Unapproved workaround
Unapproved software
Unapproved hardware
Privilege abuse
Possession abuse
Net misuse
Knowledge abuse
Email misuse
Data mishandling
Spyware/Keylogger
Scan network
Rootkit
Ransomware
Ram scraper
Password dumper
Packet sniffer
Other
Export data
Exploit vuln
Downloader
Disable controls
Click fraud
Capture stored data
Capture app data
C2
Brute force
Backdoor
Adware
Adminware
XML injection
Virtual machine escape
Use of stolen creds
Use of backdoor or C2
Session replay
Session prediction
Session fixation
SQLi
RFI
Path traversal
Other
OS commanding
HTTP request splitting
Forced browsing
Footprinting
Buffer overflow
Brute force
Abuse of functionality
Publishing error
Programming error
Other
Misdelivery
Misconfiguration
Maintenance error
Loss
Disposal error
Capacity shortage
Technique
1
5
9
Step in attack path
action
Error
Hacking
Malware
Misuse
Physical
Social

Challenges

- Lot of mapping work to do. Not straight 1:1.
- Actual real live data from breaches to simulate and predict.
- Actual real live data from near-misses and continuous improvement of companies to help measure improvements in security posture.

How can I help?

- Contribute to the DBIR with anonymized granular-level data on breaches.
- We really don't care who the customer is. Really
- If we get enough data, we have the opportunity to publish and Appendix on this on next year's DBIR.


Educational (61)
Retail (44-45)
Healthcare (62)
Public (92)
Finance (52)
Information (51)
Your gift of a few contributions
Can help a starving data scientist.

verizon

Alex Pinto
alex.pinto@verizon.com
@alexcpsec

Gabe Bassett
gabriel.bassett@verizon.com
@gdbassett