Avast

virus BULLETIN

What If?

From crazy ideas to more reasonable approaches to improve daily TI practice.

(No TI staff were harmed during the making of this presentation!)

Jaya Baloo
CISO AVAST

CYBER THREAT ALLIANCE

Lift our overall abilities ?

LEVEL UP

- Not an effort of one but of many
- The example of community - CERT / First IRC
- Emergency response Ukraine– rapid sharing and collaboration
- Rapid response vs IP concerns – sharing is the key, and being first lends advantage
- Joint up lift – share better data together – consolidation AV market –consequences /

Had more samples

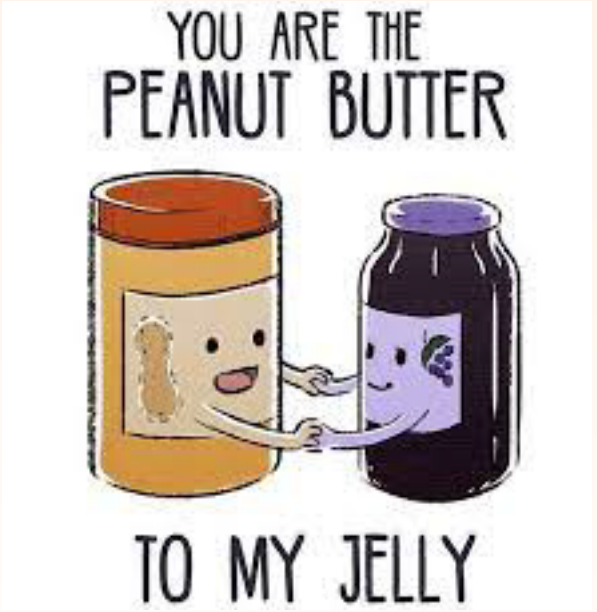
DAMN ESET (pronunciation matters)

- NCSCs – doesn't have malware res. / analyst
- Open platform submitting samples
- Triage **AND** feedback - incl. eta

Could Collaborate easier

Stronger together

- Amazing what you can achieve when no one cares who gets credit
- Not just technical
- Marketing & PR
- Open aegis // CTA
- WERKSPOT - // Dividing work – supply & demand



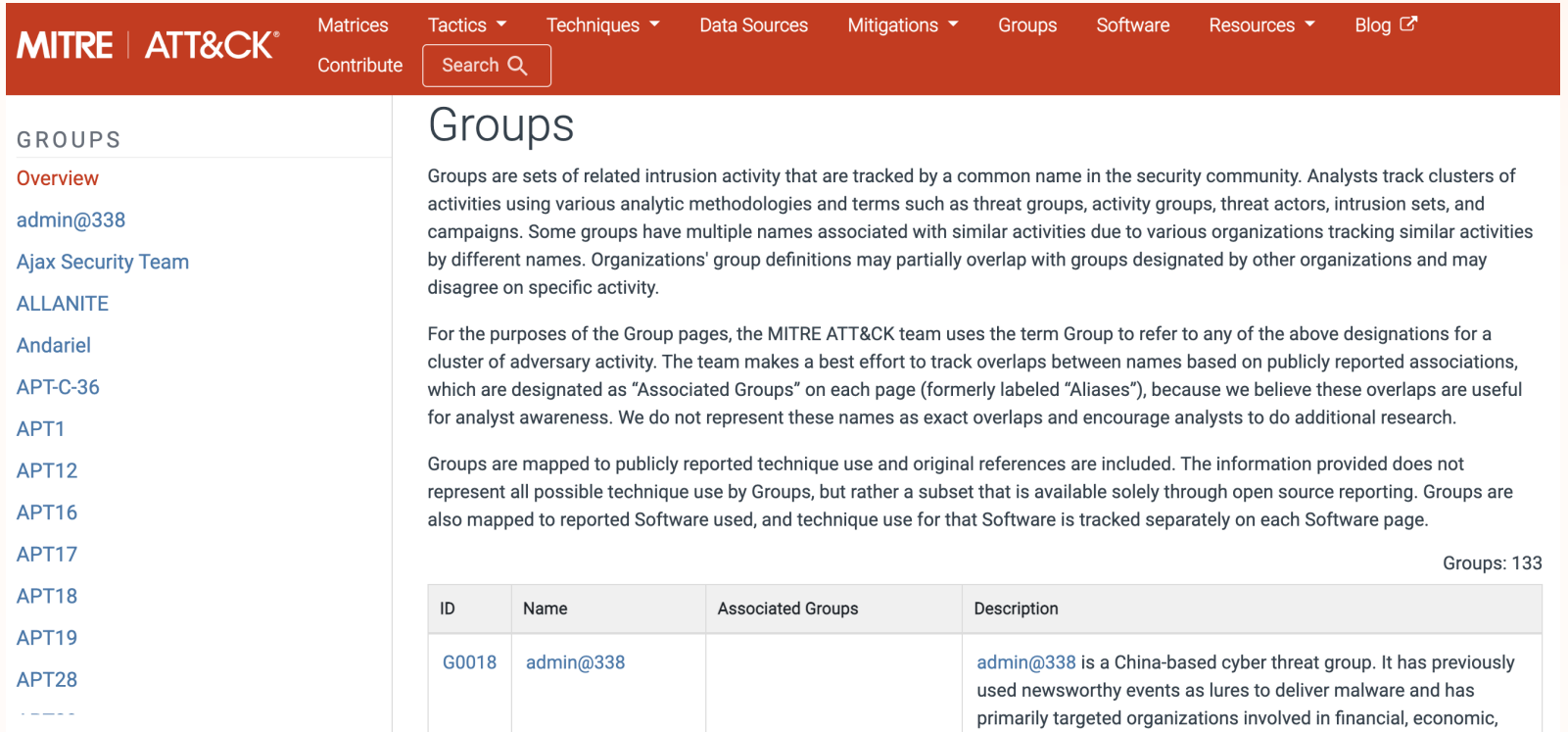
Could Automate IOCs/ TTPs

Automate all the things!

- AUTOMATE IOC HITS – and report for enrichment
- AND TAKE TTPS (DLL SIDE LOADING) as threat hunting objectives

Could agree on threat actor/ campaign naming

- SO OLD– I know
- AKA all the things– historically
- Agree on Mitre naming convention and add any new reports to existing groups or request new. Right now – Best Effort from Mitre
- Confidence level for new IOCs and TTPs



Organizing the data

Drowning in data...

- We are now not able to use all the data we have from our sensors and products -> We have more data than we are processing
- Easy query data / connections ?
- Quickly compare samples – at scale ? (Not just SSDEEP)
- Sometimes we are missing context but are we missing context because of volume or pipeline?
  - If volume -> maybe ML is here to help to cherry pick what is interesting
  - Use it to cherry pick anomalies from huge volume of unclassified data then researcher needs to validate

Improve collaboration between AI /Malware research teams

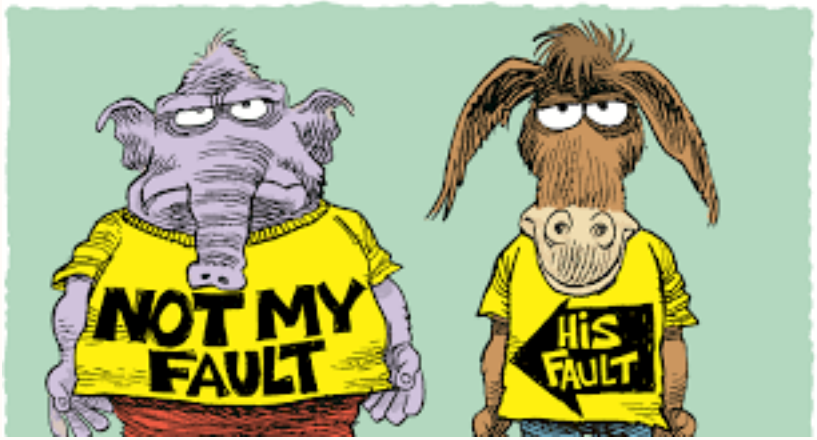
- Communication Gap– Statistically versus Deterministic sample detection
  BOOSTING– learn and look at mistake, rinse and repeat- Take a Boosting approach

- Knowledge Gap /Graphs– Security knowledge required to understand different strains/ mutexs etc. And make decisions
  Seemingly inconsistent information – hard to encode constraints – ie / also predicting times and sequence and ordering
- Explainability – understand why certain outputs are achieved from a certain model – better to move to a contract mechanism – where you know how to predict behavior 99% of the time

Andrew Gardner on Efficacy– ‘’ We’re just not measuring what matters. Our focus is on efficacy when we need to go beyond it with enrichment, context, and cost. ’

Context building with OSINT easier

- Context
- Structural use of OSINT/ Directed Hunting
- OSINT & MALWARE RESEARCH teams



Improve investigation basis – tooling and structural availability

WITH THE POWER OF
TEAM CYMRU™
PURE SIGNAL™

VICE

MOTHERBOARD
TECH BY VICE

Revealed: US Military Bought Mass Monitoring Tool That Includes Internet Browsing, Email Data

The “Augury” platform includes highly sensitive network data that Team Cymru, a private company, is selling to the military. “It’s everything.

Disruption requires democratization

- Better cross border collaboration
- Law Enforcement Relationship building
- Transparancy of the process and better usability of the results


Avast