



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



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

MITRE | ATT&CK Matrices Tactics Techniques Data Sources Mitigations Groups Software Resources Blog

Contribute Search

GROUPS

- Overview
- [admin@338](#)
- [Ajax Security Team](#)
- ALLANITE
- [Andariel](#)
- [APT-C-36](#)
- [APT1](#)
- [APT12](#)
- [APT16](#)
- [APT17](#)
- [APT18](#)
- [APT19](#)
- [APT28](#)
-

Groups

Groups are sets of related intrusion activity that are tracked by a common name in the security community. Analysts track clusters of activities using various analytic methodologies and terms such as threat groups, activity groups, threat actors, intrusion sets, and campaigns. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to any of the above designations for a cluster of adversary activity. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Groups" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness. We do not represent these names as exact overlaps and encourage analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used, and technique use for that Software is tracked separately on each Software page.

Groups: 133

ID	Name	Associated Groups	Description
G0018	admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic,

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

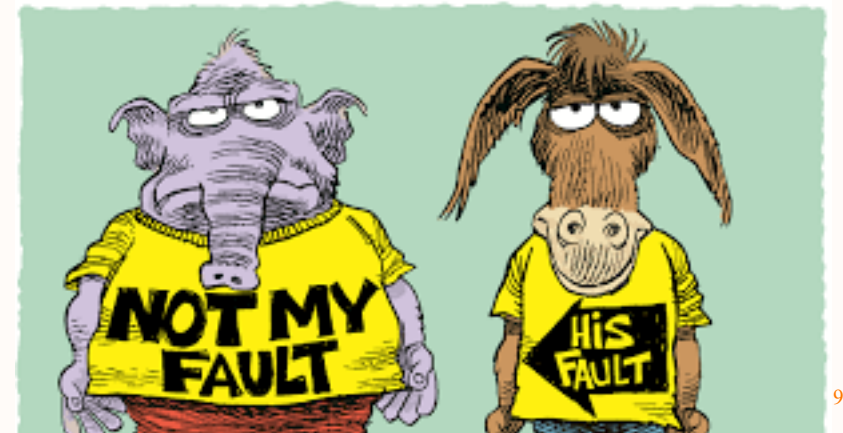
- Communication Gap– Statistically versus Deterministic sample detection
BOOSTING– learn and look at mistake, rinse and repeat- Take a Boosting approach
- Knowledge Gap /Graphs– Security knowledge required to understand different strains/ mutexs etc.
And make decisions
Seemingly inconsistent information– 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

**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
- Transparency of the process and better usability of the results





Avast