RISKsec

Decrease your risk • Increase your security

Disrupting the attack lifecycle: how do attackers behave?

Kelly Shortridge

Detection Product Manager, BAE Systems Applied Intelligence

SC MEDIA

THE CYBERSECURITY SOURCE

haymarket

RISKsec
Decrease your risk Increase your security

As an industry, the narrative often omits that attackers are human

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

Human brains are optimized for speedy decision-making to aid survival

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

Attackers are just like us – they aren't perfectly rational thinking machines

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

"Attackers will take the least-cost path through an attack graph from their start node to their goal node"[1]

=

Attackers optimize for least cost and least risk to get to their end goal

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

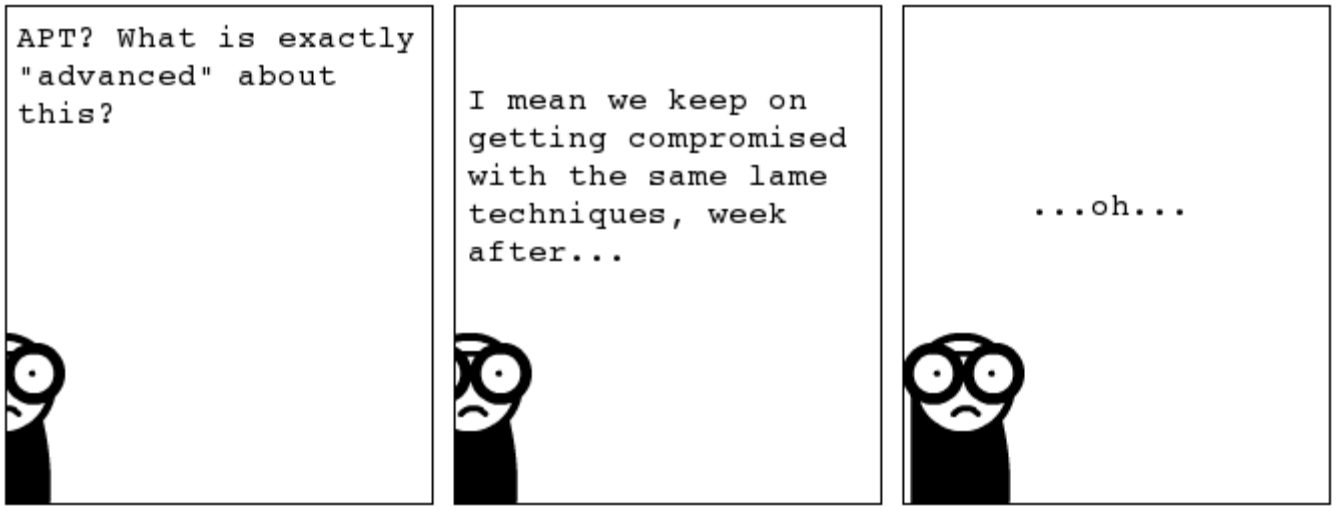
1. Dino Dai Zovi, "Attacker Math 101"

Attacker preferences: Fantasy

Opting for fancy, “advanced” footwork every time against defenders

Attacker preferences: Reality

Kicking between the defender's legs, because it works


APT? What is exactly "advanced" about this?
I mean we keep on getting compromised with the same lame techniques, week after...
...oh...

RISKsec
Decrease your risk Increase your security

What are biases?

- People are “bad” at evaluating inputs into decisions
- They’re also “bad” at evaluating potential outcomes of decisions
- People take mental shortcuts in decision-making
- Famous biases: Dunning-Kruger, confirmation bias, short-termism, illusion of control

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

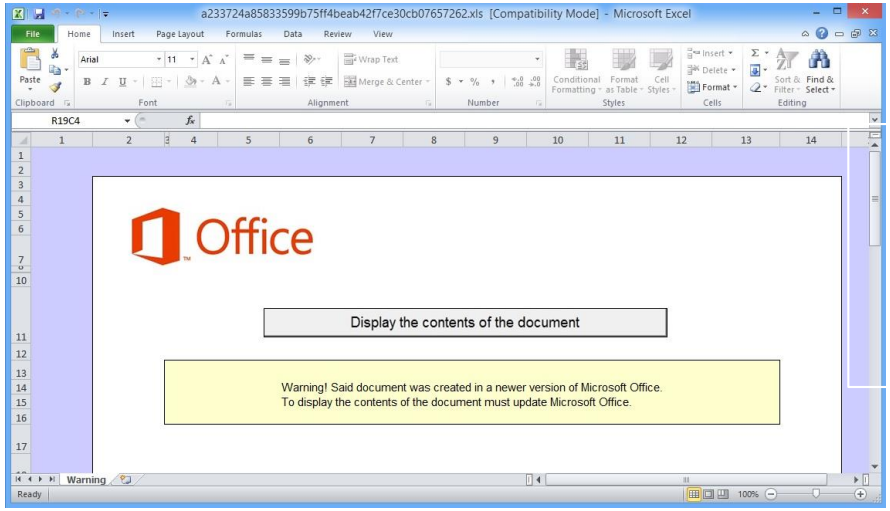
RISKsec
Decrease your risk Increase your security

Attacker biases

- Risk averse – feel losses 3x as much as defenders
- Focus on probabilistic vs. absolute outcomes (likelihood of success, not just final value of success)
- Quickly incorporate new data into their model of effective methods
- Avoid hard targets unless necessary, prefer low-hanging fruit
- Prefer repeatable / repackageble attacks

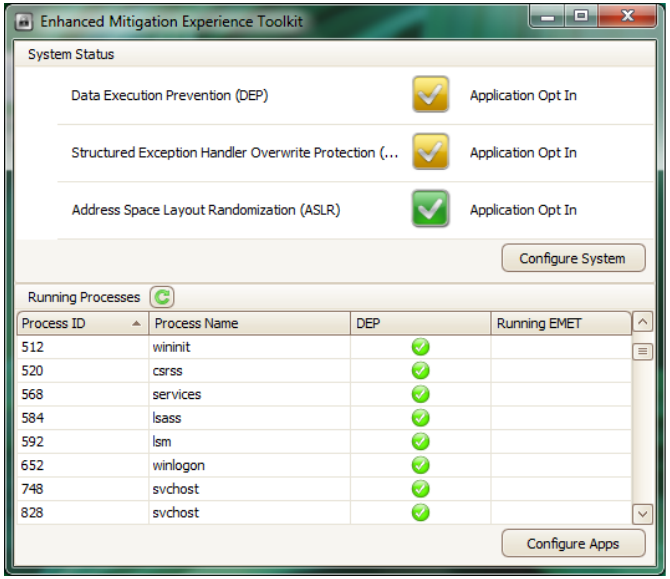
SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

For background, see my presentation “The Art of Explanation: Behavioral models of infosec”



Malicious macros are the tasty, low-hanging fruit for attackers…

…not 0day exploits that bypass ASLR / DEP



RISKsec
Decrease your risk Increase your security

Attacker ROI

- Attackers care about ROI, regardless of goals
- Malware spammers – keeps ROI high via low costs, “spray and pray” approach
- Criminal groups – keeps ROI high via targeting higher-value assets, despite more costly approach
- U.S. APT – keeps ROI high via longer-term persistence, despite very high costs of attack (reliability is pricey)
- Comrade Bear APT – keeps ROI high via “plausible deniability” approach (reliability is less important)

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

For background, see my presentation “The Art of Explanation: Behavioral models of infosec”

RISKsec
Decrease your risk Increase your security

Leveraging these biases

Raising the cost and uncertainty of attack decreases the likelihood of attack across spectrum of attackers

1. Eliminate low-hanging fruit
2. Drive strategy with data
3. Erode information advantage

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

Playing games

Humans either “think” or “learn” when playing games

- Thinking = modeling how opponents are likely to respond
- Learning = predicting how players will act based on prior rounds
- Defenders should therefore disrupt how attackers think and learn

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

First: questions to ask

- “How do you think our adversary chooses their delivery method?”
- “What countermeasures do they anticipate?”
- “Which of our assets will attackers want?”
- “How will attackers bypass our security investments?”
- “What are the cost / resources required for attackers to get to our assets?”

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

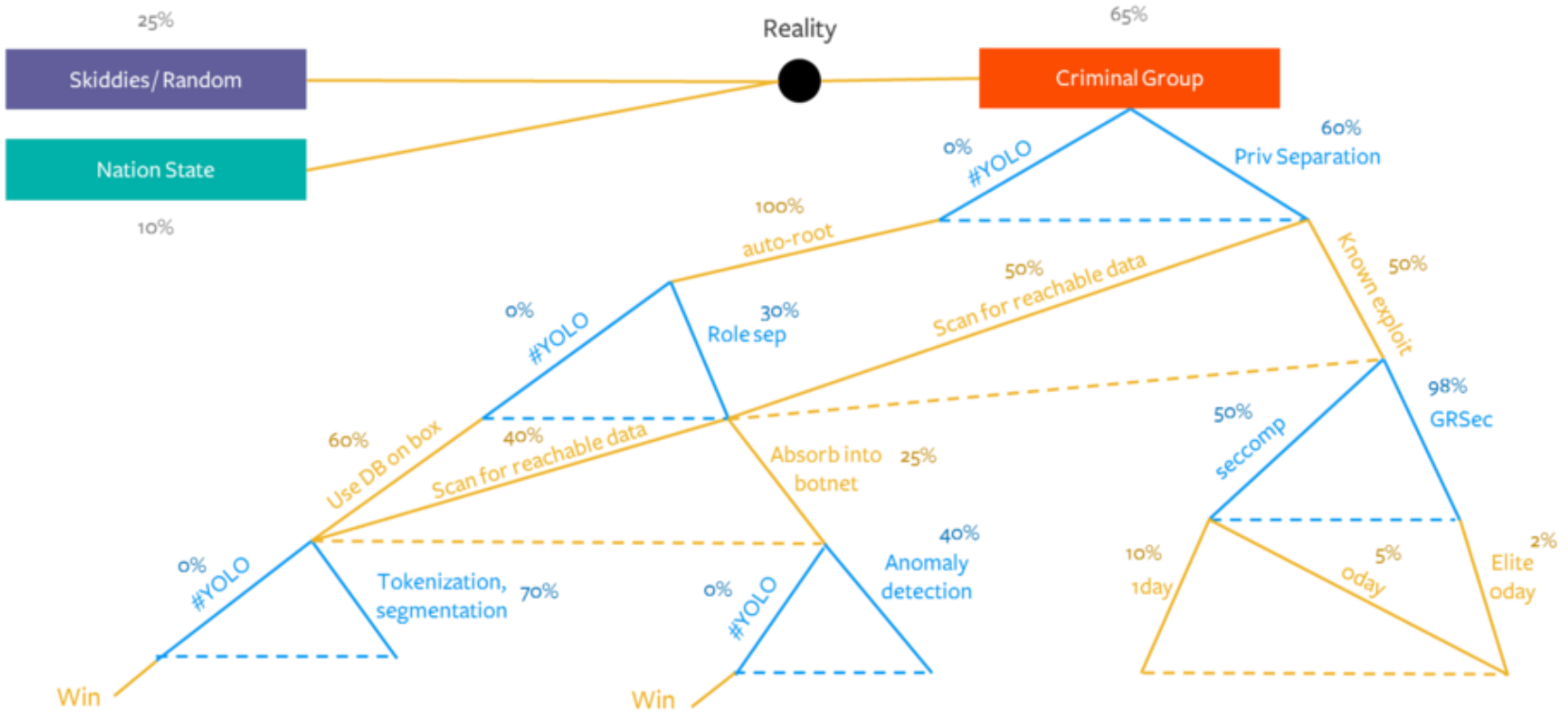
Decision trees

Diagram likely attack paths with estimated probabilities

- Creates an auditable picture of why you chose certain tools
- Easy to update after an incident or when threat intel comes out on a relevant attack group
- Keeps you honest with tangible metrics – deters self-justification
- Hedge against “additive only” approach – decisions are revisited
- Mitigates “doubling down” effect by showing exactly where assumptions failed

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

Example decision tree



RISKsec
Decrease your risk Increase your security

Selecting tools

- Start with tools that eliminate low-hanging fruit
  - Requires both criminals and APTs to up their game
  - Two-factor authentication (ideally app vs SMS)
  - Role separation, privilege separation, other basics
  - IT asset management
- Build up from stopping “lowest-common-denominator” attacks
  - Don’t spring for anti-APT if you don’t have 2FA yet
  - Cover the basics, or more “advanced” tooling is worthless
  - Like having laser tripwires without a lock on your door

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

Towards data-driven

- Optimize for tools that add *actionable* data
  - Detect across kill-chain, not just block at disparate sections
  - Canaries / honeytokens to track attacker movements
  - IT asset management to understand own environment
- Not all data is created equal
  - Ensure that you aren't generating more noise than signal
  - What data actually helps you determine whether your strategy is working?

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

Visibility

Your advantage is understanding the local environment.

Adding visibility into attacker actions creates superior strategic options.

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

But first…

Attackers will cultivate data on your network (assets, flows, topology), application footprint, and employees (roles, access levels, relationships) to craft their attack

…do you even have this level of data to craft your defense?

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

A harsh truth

You must fully and continuously understand your own environment before you can attempt fancier strategies

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

Attacker data

- Human brains learn on a trial and error basis
- Collect data on:
  - Chain of decisions across attacker lifecycle (not just a singular event, e.g. spearphishing email)
  - Time between decisions (recon to delivery, delivery to exploit, etc.)
  - How attackers react to actions / paths being blocked (a form of A/B testing)
  - Scans or other indicators of attackers searching for security measures

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

Using the data

- Filling in decision trees
  - Visualize attacker “stories” to begin assigning probabilities and formulating counter-strategies
- Model tracing
  - Track attacker activity via “A/B testing” to determine how they select actions (how much learning rate plays into decisions)
  - With enough data, can start predicting next moves
- Disrupt learning
  - Use honeytokens / canaries to give attackers false information and throw off their learning process

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

Terraforming

- Attacker data helps visualize likely attacker paths
- Determine which is the hardest path for attackers to get to their goal
- Develop strategies to force attackers to harder paths
- Easiest start = eliminating easiest paths

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

Dynamism

- Maintaining a static environment is super helpful to attackers (keeps recon evergreen)
- Difficult to keep perfect, up-to-date idea of attacker playbook – better to make that playbook obsolete
- Falsifying information is an underutilized strategy
- For more advanced defensive teams, try things like fluctuating infrastructure
  - Netflix's Chaos Monkey as an example

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

Conclusion

- Attackers are human
- Attackers won't be "advanced" unless necessary
- Necessary = when cost of attack is higher
- Goal = raise cost of attack & create uncertainty
- Eliminate low-hanging fruit
- Collect data on yourself & attackers
- Erode offense's information advantage

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket

RISKsec
Decrease your risk Increase your security

Q&A

- kelly@greywire.net
- Twitter: @swagitda_
- LinkedIn: /kellyshortridge

SC MEDIA
THE CYBERSECURITY SOURCE
haymarket