When threat intel met DFIR

Who are we?

Thomas Chopitea

Coder, coder^{-1} & malware tamer @CERT Société Générale

CERT | SOCIETE GENERALE

Ronan Mouchoux

Intel analyst, OSINT hunter @CERT Sekoia

sekoia

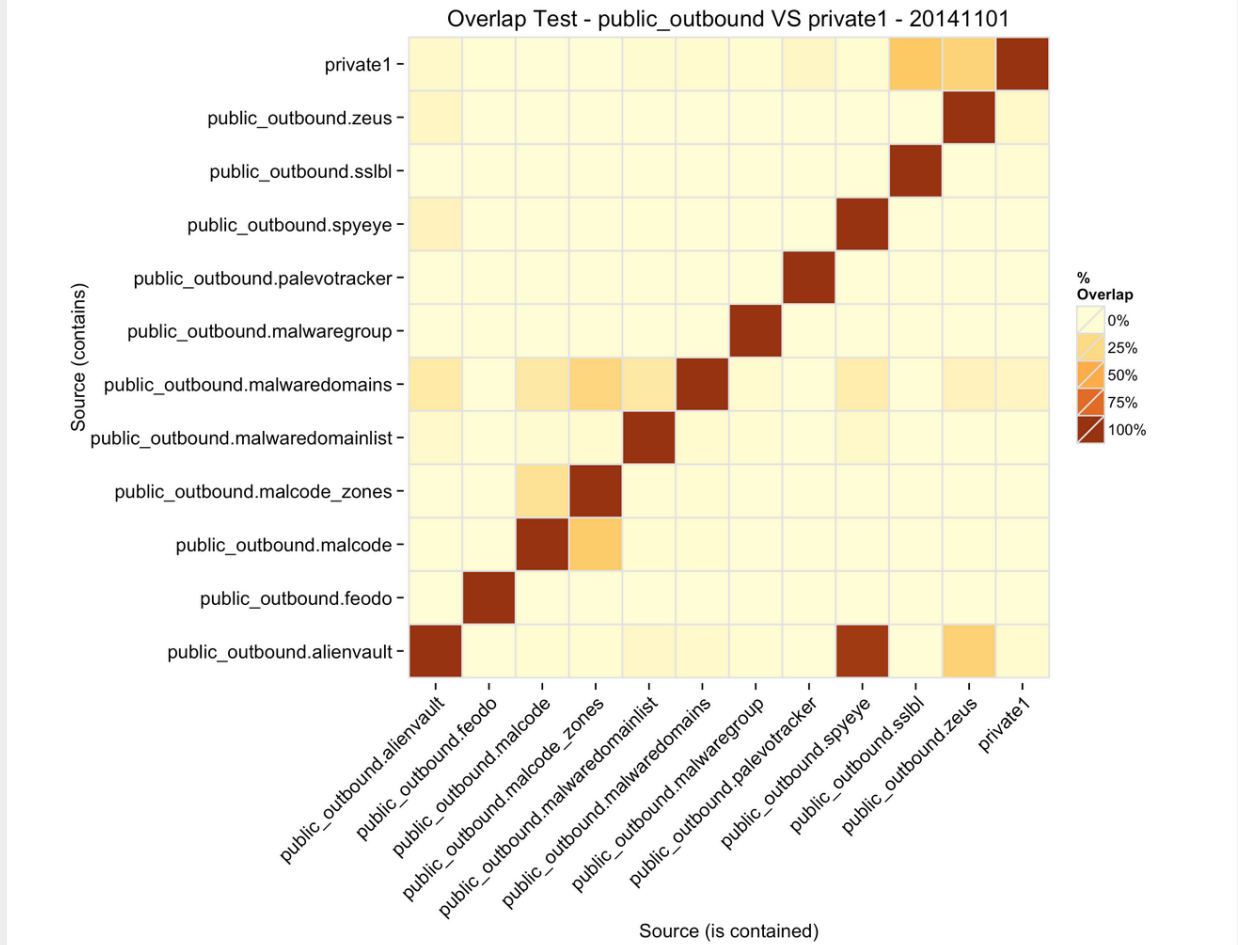

No Pandas, Bears, Foxes, Elephants or Kittens
...were harmed for this presentation.


Threat intel
in a (quite large) nutshell

Snakeoil warning

Feeds - Attribution - Military terms - Intelligence and espionage

Feeds



If you're blind, feed providers are one-eyed source

Attribution?

- Always nice to have a super-villian...
- Probably useless unless you have drones (Junaid Hussain)
- Probably useless unless you are LE (Su Bin, Dridex, etc.)

Still good to think in attacker groups

Military jargon 

- Guess who's had to deal with **adversaries** for a long time?
- US is leading Internet Research, makes us sound American

Intelligence != espionnage

Espionnage is **clandestine** information collection

Classified information is usually considered "better" than e.g. OSINT

Biais: Intelligence produced from espionnage is of **very high value**

What is Threat Intelligence?

Threat

`Risk = Vulnerability * Threat * Impact`

`Threat = Intent * Capability * Opportunity`

We like the term **"Threat Actor"**. May be any of:

- Cybercrime
- State-sponsored
- Hacktivism
- Insider
- Industry competition

Intelligence

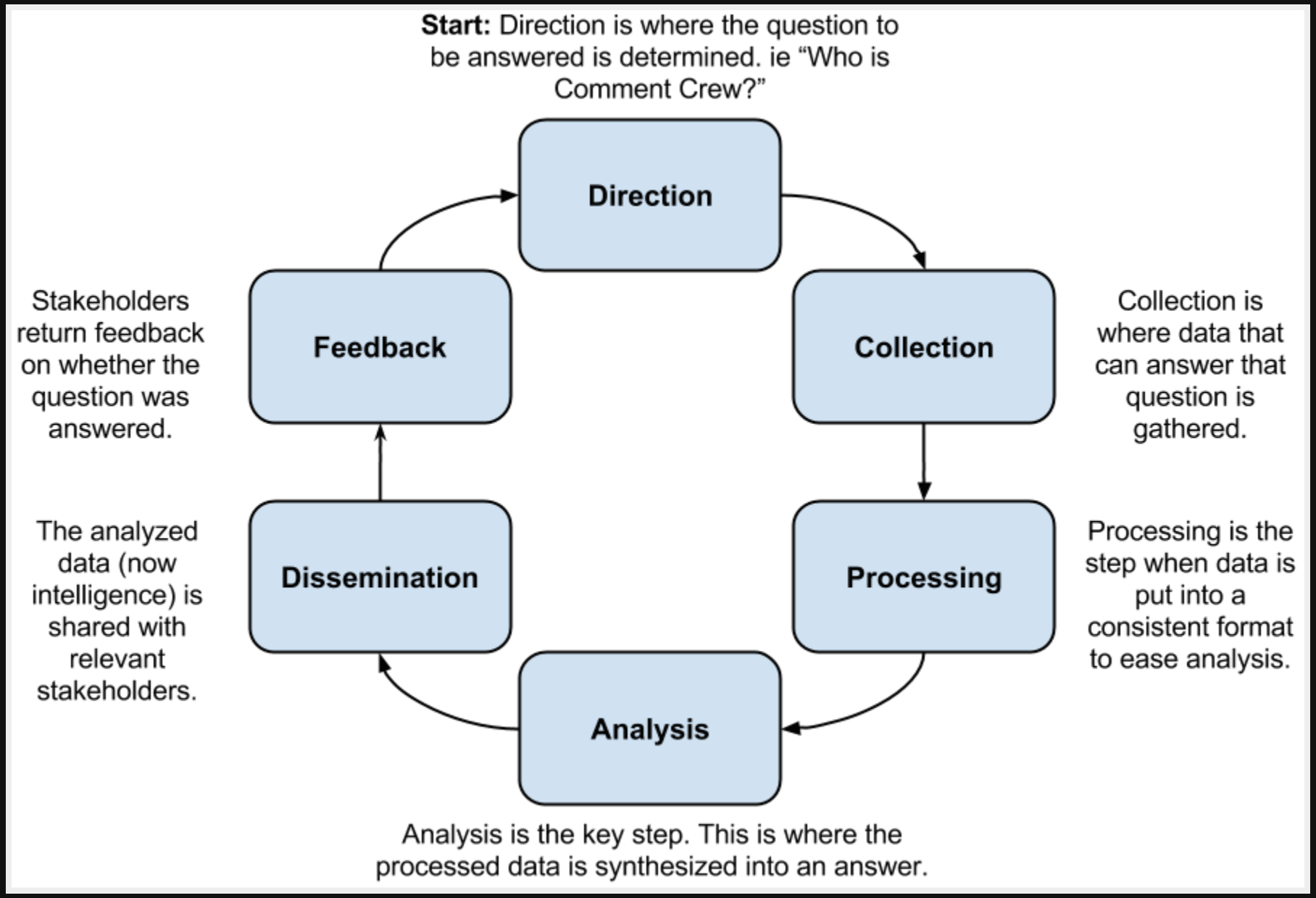
a.k.a. *Renseignement, ré-enseignement*

- Environment → Data → Information → Intelligence
- Intelligence is a **cyclic process**
- **Analysis** and **contextualization**
- Models help counter diversity with abstraction

"Actionable intel" 

Information	Intelligence
Raw, unfiltered feed	Processed, sorted info
Unevaluated when delivered	Evaluated and interpreted by trained analysts
Aggregated from virtually every source	Reliably aggregated and correlated for accuracy
May be true, false, misleading, incomplete, relevant or irrelevant	Accurate, timely, complete (as possible), assessed for relevancy
Not actionable	Actionable

BY DESIGN



The Intelligence Cycle courtesy of Scott Roberts

Intelligence is a product

It's not the fruit of a massive data ingestion but the product of a **particular analysis** in a **specific context**

Intelligence offers good countermeasures

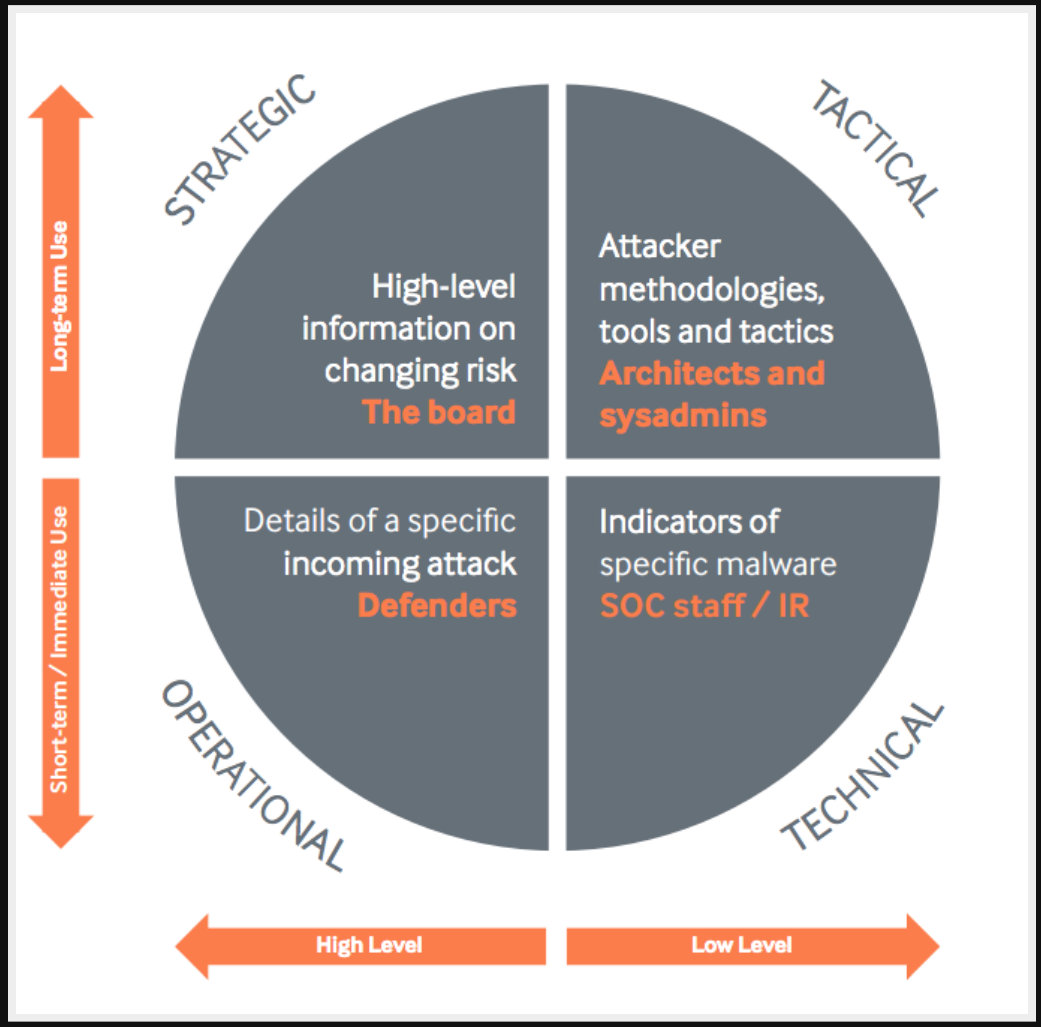
Threat	Countermeasure
resilient and perennial	long-term surveillance
organised, skilled, motivated	short-term reaction
stays under the radar, hides tracks	weak signal analysis, anticipation
adaptive to defender's response	discretion

Cyber Threat Intelligence

Actually means something 

Cyber	Area of interest / of collection
Threat	Subject of interest
Intelligence	Process

Types of threat intelligence



Strategic, tactical, operational, technical source

Strategic TI

- Target audience: **decision-makers**
- Focus on changing risks, high level topics:
  - Geopolitics
  - Foreign markets
  - Cultural background
- Vision timerame: **years**

Note: You may never have heard of this; could be explained by lack of maturity in orgs

Tactical TI

- Target audience: **architects & sysadmins**
- Focus on "TTPs":
  - Attacker *modus operandi*
  - Blue team / red team tools
  - Exfiltration / C2 methods
  - Persistence / stealth / deception mechanisms
- Vision timeframe: **weeks to a year**

Note: The most common form of threat intel (and **marketing** ) produced today; easy to obtain

Operational TI

- Target audience: **defenders**
- Focus on current & future attacks:
  - Who, what, when?
  - Early warning on incoming attacks
  - Social media activity
- Vision timeframe: **months, weeks, hours**

Note: Hard for private companies to obtain on advanced attackers; traditionnaly collected through HUMINT / SIGINT

Technical TI

a.k.a. Data 

- Target audience: **SOC, IR people**
- Focus on raw obersvables:
  - Indicators of compromise
  - Host and network artifacts
  - Yara, Snort, OpenIOC rules
- Vision timeframe: **hours to years**

Note: Man-hours are valuable. Technical TI is abundant. Processing should be as automated as possible.

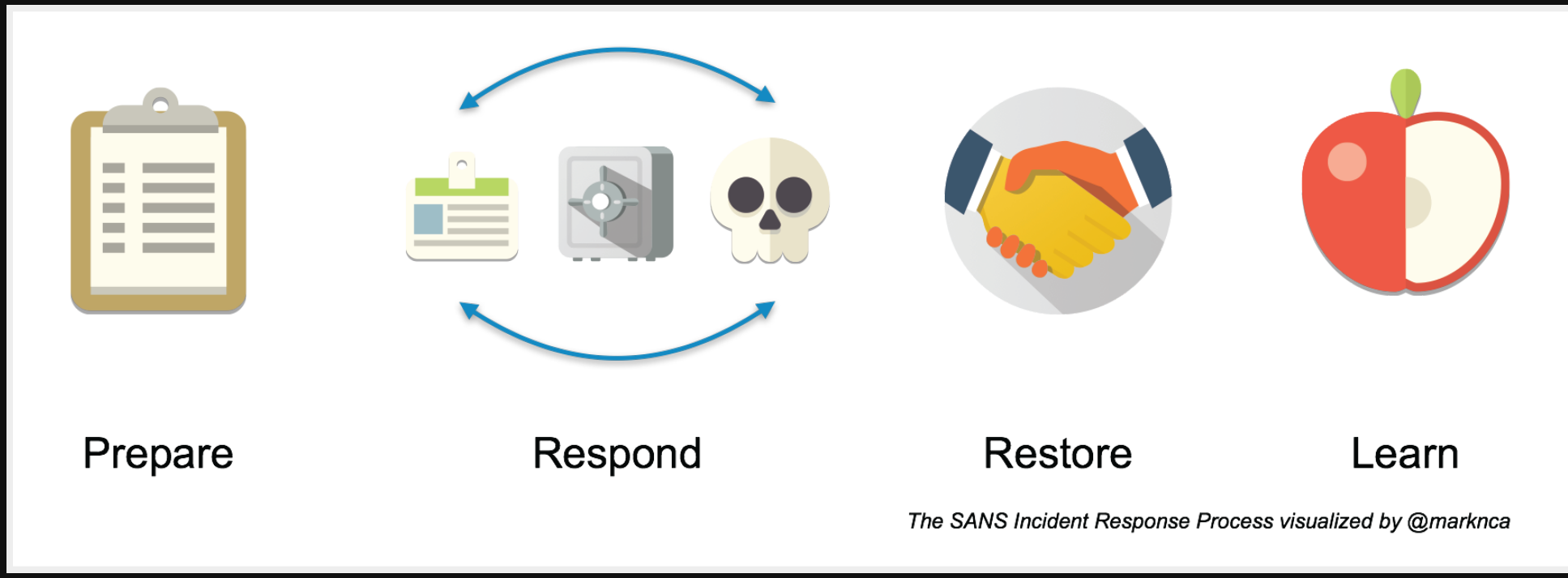
Weaponry

Strategic	Will feed SWOT, risk assessments, Porter Diamond model...
Tactical	Cyber Kill-chain, Diamond model, ACH
Operational	F3EAD, OODA Loop, Pyramid of Pain
Technical	Data stores / analysis: CIF, FIR, IntelMQ, MISP, Malcom, Maltego, Soltra...

That's all well and good, but...

What about DFIR in all of this?

IR process


Prepare
Respond
Restore
Learn
The SANS Incident Response Process visualized by @markn ca

Your typical DDoS

- **Hacktivists** (easy)
  - Can't keep their mouth shut (good **operational TI**!)
  - Plus, they rarely change TTPs → easily blocked
- **Organized crime** (medium)
  - Will use amplificators
  - Knowing which (tactical TI) makes upstream blocking easy
  - **Blackmail**: knowning TTPs allows you to scan your email servers for warnings

Weaponry: **MISP** (intel sharing)

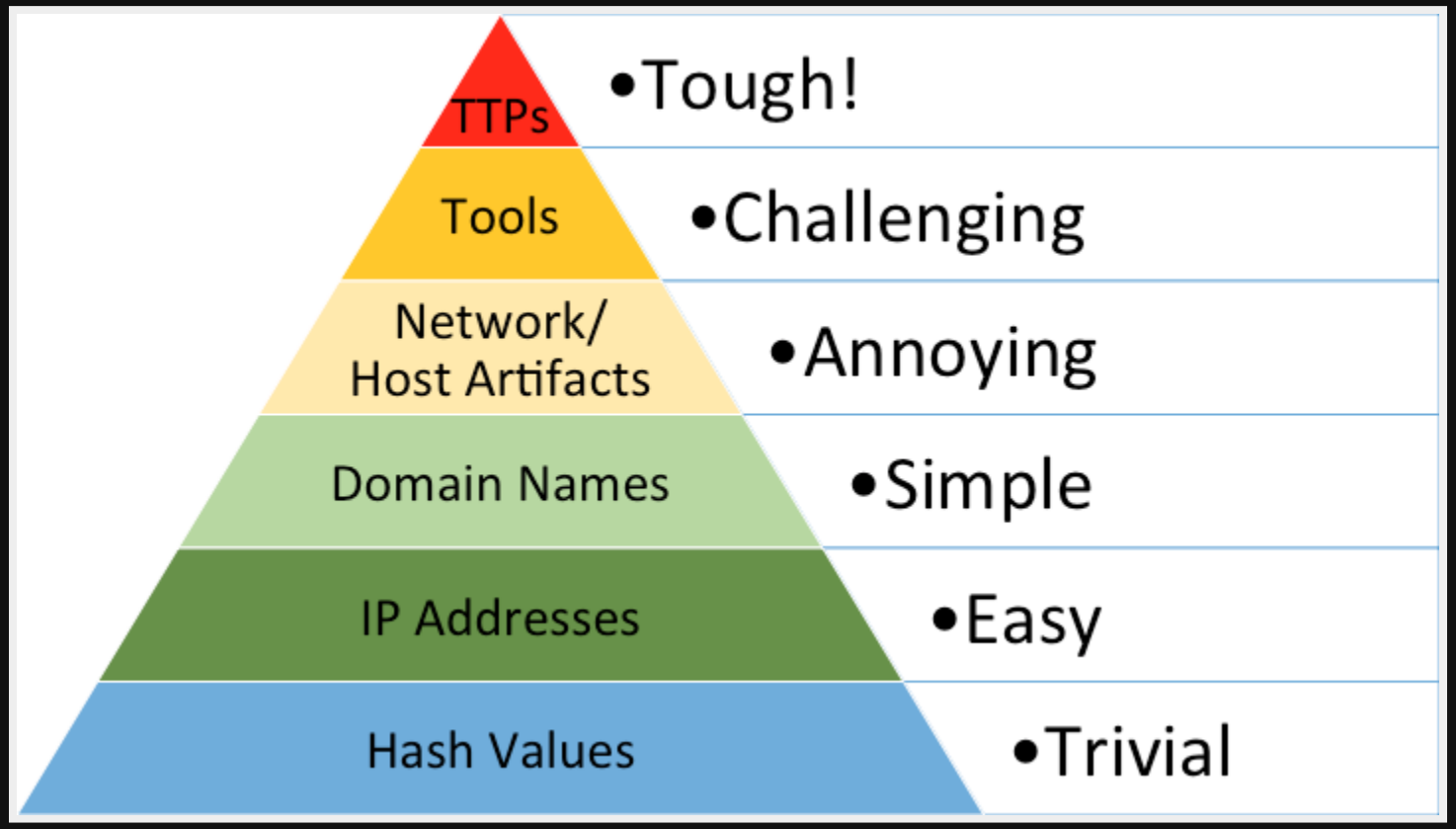
Weaponry: **MISP** (Intel sharing)

Cryptolocker

- Malware analysis → tactical intel report:
  - malware uses **time-based DGA** to determine C2
  - malware contacts C2 to retrieve key **before** encrypting
- Reverse DGA, block all domains for the next two years
- Keep monitoring samples for changes in DGA

That was fast...

"The pyramid of pain"



by David Bianco

Respond **quickly** to indicators, **deny** their use to the attacker

Cryptolocker

Lessons learned...

- Producing TI without anyone to consume it is **useless**
- Waiting for the key **before encrypting** is risky

New "locker" variants generate their own keys and start encrypting right away

Weaponry: **CIF**, **Malcom**, **IntelMQ** (aggregate & query)

"Hunting" for APTs

Use signatures, blacklists, activity patterns, intel, hunches, to **proactively** search for incidents

- **Target-centric**: focus on valuable resources, search around them
- **Actor-centric**: focus on actors, their TTPs, traces they might leave

aka **Hunting** aka **"proactive" DFIR** aka **intelligence driven IR**

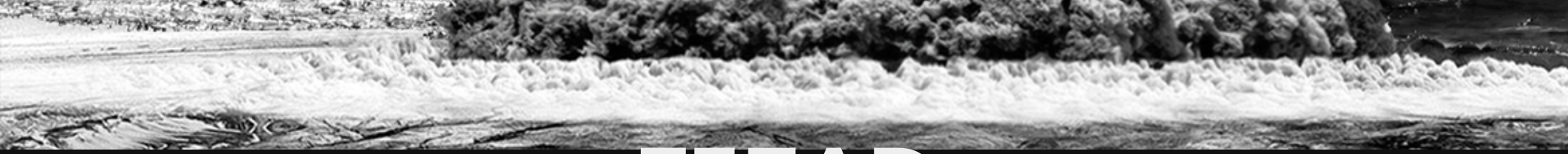
Warning: proving true-negatives is impossible

The hunt

Pre-incident

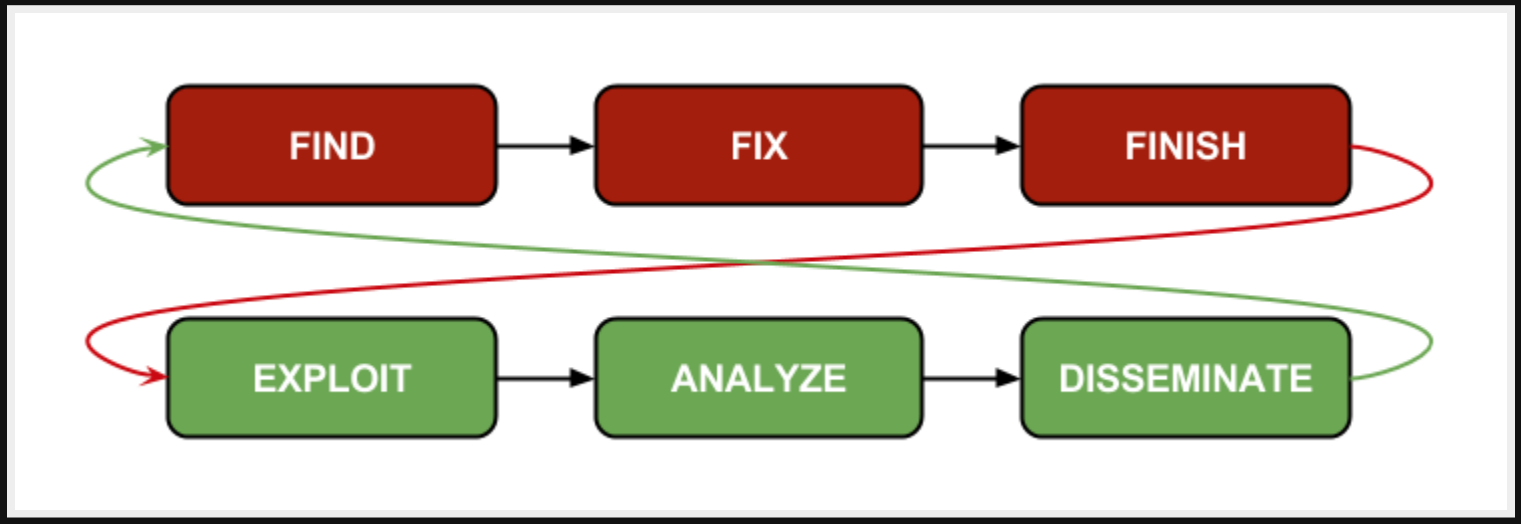
1. Gather intelligence on **external or internal attacks** (privately or publicly shared)
2. Disseminate: Leverage this intel on your network and endpoints (**Grr**, **OSQuery**)
3. **Match!** → Declare & handle incident


ZOMG APT!
Post-incident
1. Draw a picture of the attack (Cyber Kill-chain may help)
2. Produce new intel on the attack
3. Use this to identify new incidents
4. Repeat!
Note: Useful to have your TI and IR teams closely working together
Weaponry: FIR, MISP



F3EAD

A target-centric approach to intelligence analysis



Bridge between **operations** and **intelligence**

a.k.a. "Hunting"

Cyber Kill-chain?

Divides attacks into 7 KC phases

1. **Recon** - harvesting email addresses, etc.
2. **Weaponization** - Exploit + payload
3. **Delivery** - Malicious email, watering-hole, etc.
4. **Exploitation** - Exploiting vulnerable software & installing payload
5. **Installation** - Ensuring persistence
6. **Command & control** - channel for remote manipulation
7. **Act on objectives** - Lateral movement, data exfil

Cyber Kill-chain!

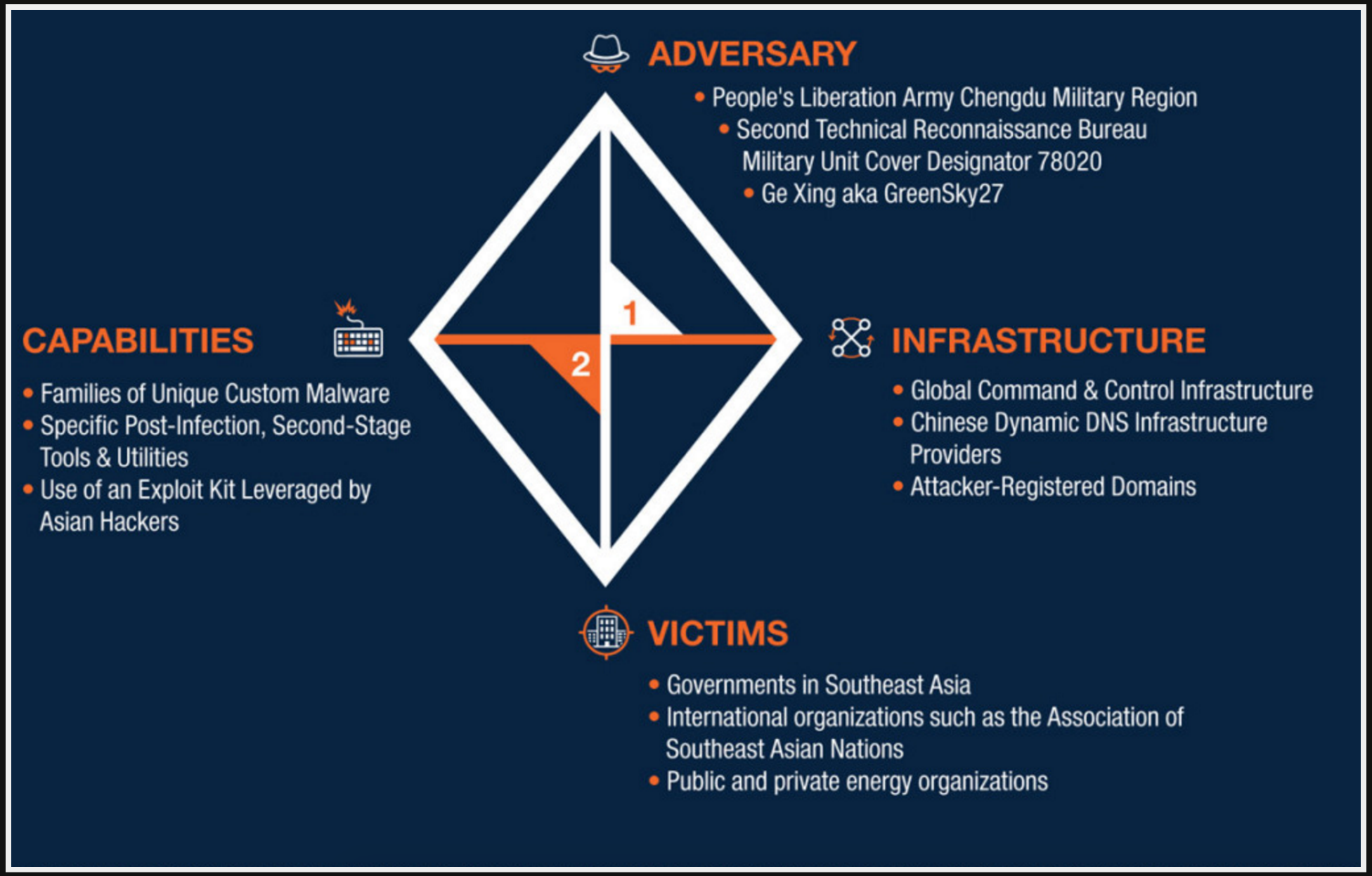
- Incidents may be **correlated** through similarities in their phases
- Correlation **does not imply** causation
- Can still give strong hints as to where to look next
- Useful to describe an incident (and countermeasures) to C-execs

but...

- Too **malware**-focused
- Can't act much on phases **1-2**

Diamond model

"ID" card for incident → campaign → attacker


ADVERSARY
• People's Liberation Army Chengdu Military Region
• Second Technical Reconnaissance Bureau Military Unit Cover Designator 78020
• Ge Xing aka GreenSky27
1
2
CAPABILITIES
• Families of Unique Custom Malware
• Specific Post-Infection, Second-Stage Tools & Utilities
• Use of an Exploit Kit Leveraged by Asian Hackers
INFRASTRUCTURE
• Global Command & Control Infrastructure
• Chinese Dynamic DNS Infrastructure Providers
• Attacker-Registered Domains
VICTIMS
• Governments in Southeast Asia
• International organizations such as the Association of Southeast Asian Nations
• Public and private energy organizations

ACH

Demo time!

Hardware courtesy of Paul Rascagnères

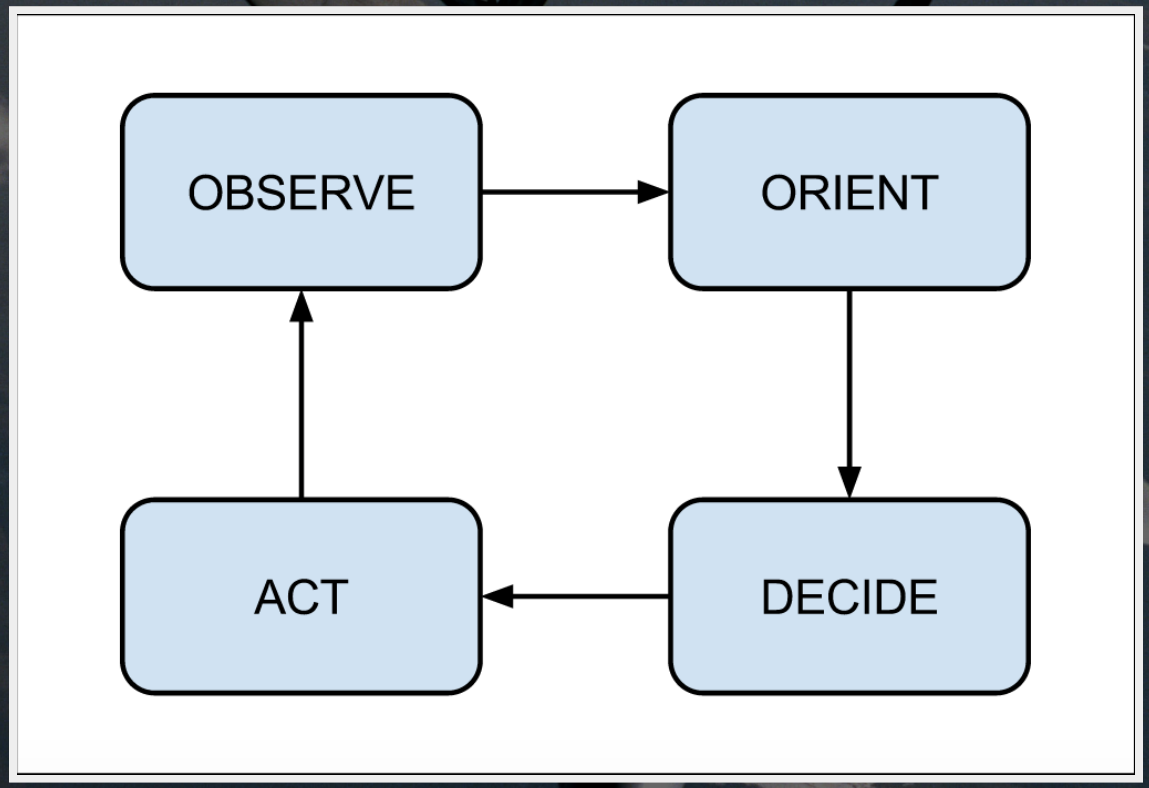
Dridex & Gootkit

Similar TTPs in delivery phase

- **Dridex** - Email delivery of **[stage1]** MS Office Doc with macros, which downloads additional code from pastebin **[stage2]**, which in turns downloads and executes binary from other server **[stage3]**
- **Gootkit** - Email delivery of **[stage1]** MS Office Doc with embedded binary, decoded, dumped and ran **[stage2]**
- Spam wave **every Tuesday** (before arrests). New wave → new sample, new pastebin URL, new macros, etc.

Relatively small OODA loop

OODA loop?



Goal is to get **inside** adversary's loop

Dridex & Gootkit

Response

1. Detect suspicious emails in corporate environment
2. **Dridex**: Extract & block pastebin URL → threat neutralized
3. **Both**: Use AV to block both macro and binary

Sometimes, intel sharing allowed us to block Dridex's **[stage2]** before it even started hitting

Dridex & Gootkit

Lessons learned

- The Kill Chain is helpful to illustrate **where malware-based** attacks are acted upon
- The Pyramid of Pain confirms it's easy for attackers to **change compromised indicators**

- **Sharing** & **dissemination** win! Use **MISP** to quickly share indicators
- We were probably **loosing the OODA race** since Dridex malspam did not slow down until the recent arrests...

Malware forensics

- TI can provide **quick-wins** when dealing with unknown malware
  - **ASEP A** corresponds to **malware M**
  - **Malware M** stores stolen **data in D**
  - Find A → find D!
- TI **without specialists** to consume it is **pretty useless**:
  - Knowing what crypto a threat is using may be useless without REs
  - In turn, REs can also provide **extra intel**!

- Weaponry: **OpenIOC**, **Malcom**, **Viper** (storage)

Managing Threat Intel

As tough as it sounds

We're not mature

but lots of stuff is going on

- **MISP** - Event-based indicator sharing
- **FIR** - Incident management platform + indicator correlation
- **CRITS** - Platform to store threat-related information

- **Malcom** - Correlation of network traffic with maliciousness feeds
- **CIF** - Query indicators + variety of output formats

- **Grr**, **osquery** - Endpoint hunting

What's nice about "standards"...

- **MITRE** - STIX, TAXII, CybOX, MAEC
- **IETF** - IODEF
- **Mandiant** - OpenIOC
- **Yara** rules - just rocks
- **VERIS**

Remember dissemination?

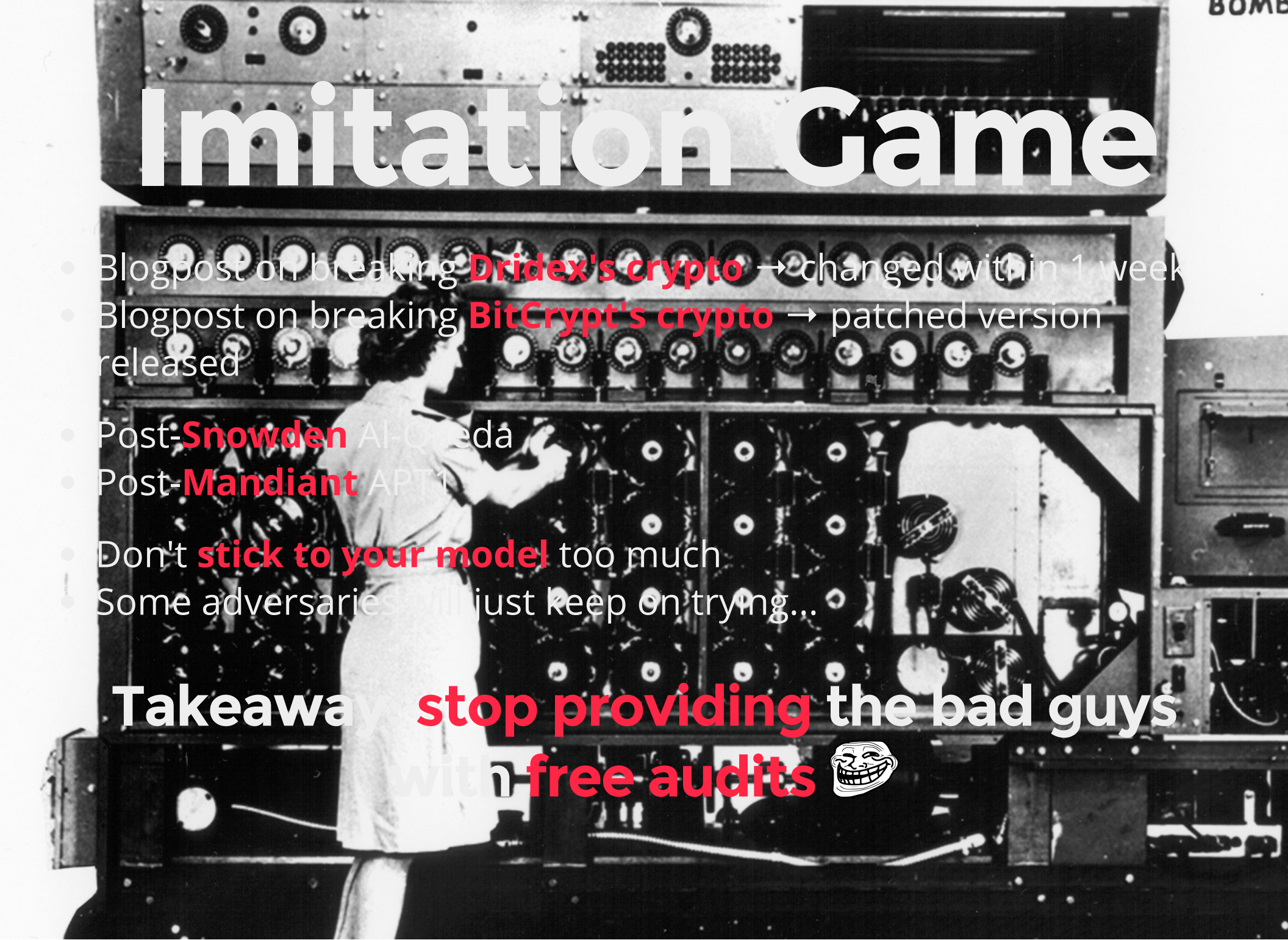
Sharing is caring

- **TLP**: *de facto* exchange protocol
- Solves part of the problem (issues with large orgs, several trust groups)
- Plus, we like automation and TLP is **hard to (safely) automate**

Oversharing

- Discrete vs. Secretive
- Don't trust everyone, don't distrust everyone

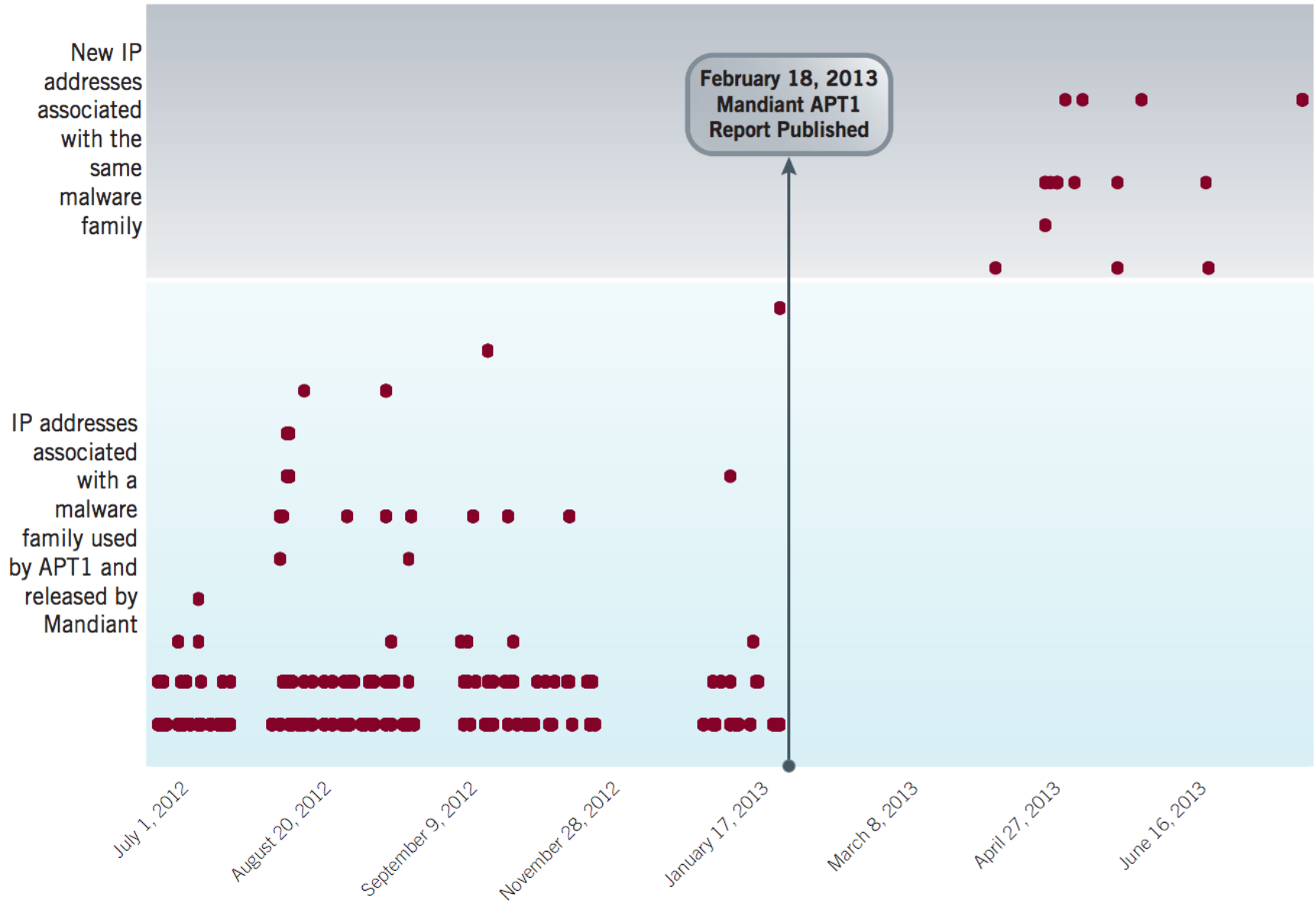
Imitation Game



- Blogpost on breaking **Dridex's crypto** → changed within 1 week
- Blogpost on breaking **BitCrypt's crypto** → patched version released
- Post-**Snowden** Al-Qaeda
- Post-**Mandiant** APT1
- Don't **stick to your model** too much
- Some adversaries will just keep on trying...

Takeaway: stop providing the bad guys with free audits

FIGURE 10: APT1'S INFRASTRUCTURE CHANGES FOLLOWING RELEASE OF MANDIANT REPORT



APT1 Changes to IP Addresses Used by One Malware Family

Conclusion

TI is closely related to traditional intelligence (duh)

Models help but have limitations

The quality of your TI directly influences the quality of your response

Tools to store, analyse, and share intelligence exist, but there's room for improvement

What next?

Less IOCs

Patternless attacks?

Cybercrime will keep industrializing

IA-based malware?