# Applying STIX to Intelligence Teams

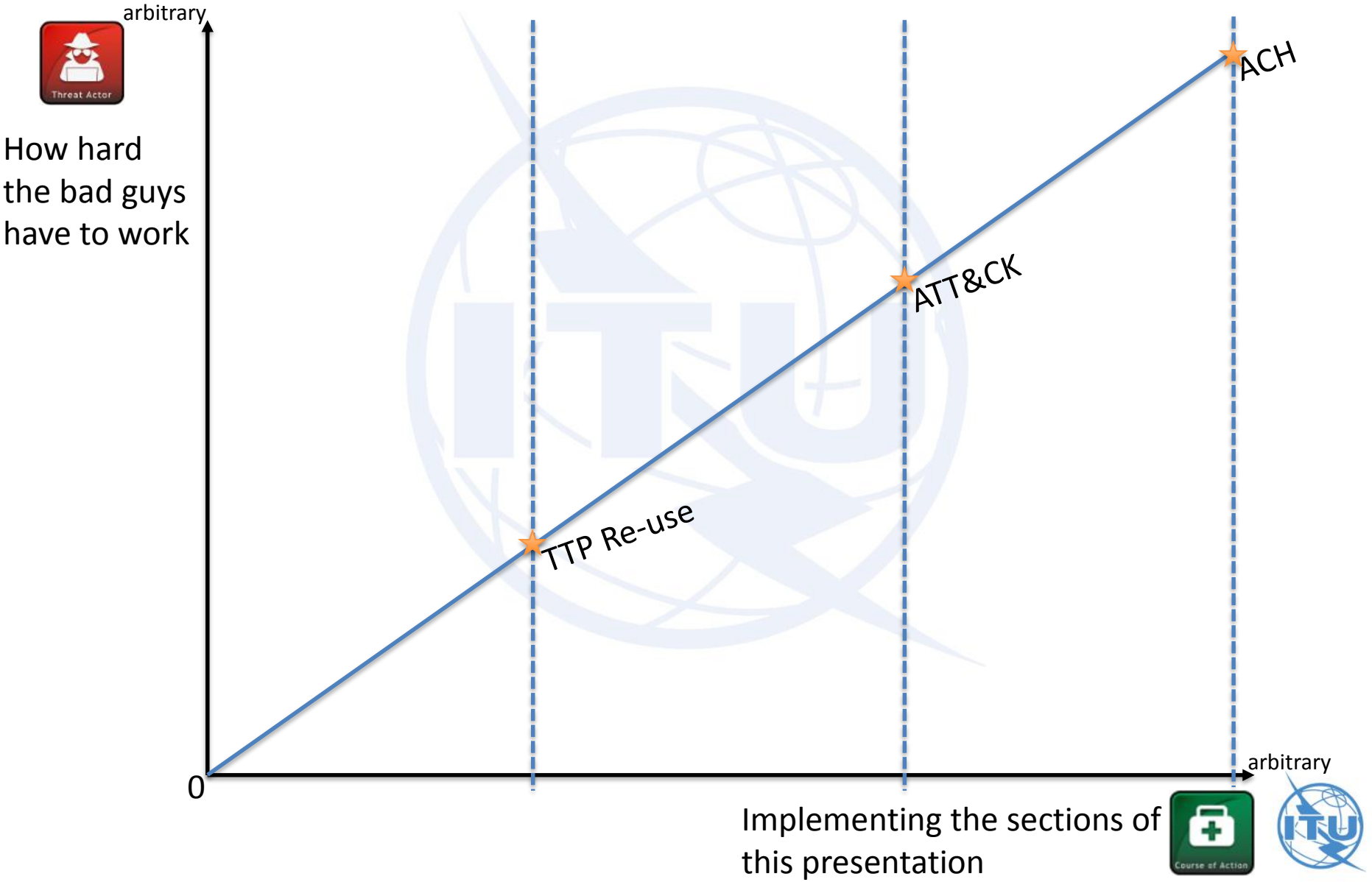
## A ransomware Case study

*Chris O'Brien, EclecticIQ*

# Applying STIX to Intelligence Teams

- Gandcrab – a Case Study
- Tracking TTP re-use in Ransomware attacks
- Mapping Ransomware functionality using Mitre ATT&CK
- Managing collaboration with ‘Analysis of Competing Hypotheses’

# Advanced CTI Techniques



# Gandcrab – A Case Study

## Ransom.GandCrab

Summary | Technical Description | Removal

**Discovered:** January 30
**Updated:** February 02, 2
**Type:** Trojan
**Infection Length:** Varies
**Systems Affected:** Win

When this Trojan is exec

- %AppData%\Microso

The Trojan then creates

- HKEY_CURRENT_U

Symantec

http://{host}/{word1}/{word2}/{fname}.{extension}

| {host} | {word1} | {word2} | {fname} (combination) | {extension} |
|---|---|---|---|---|
| *hardcoded list* | wp-content | images | im | jpg |
| | static | pictures | de | png |
| | content | image | ka | gif |
| | includes | graphic | | |
| | data | assets | | |
| | uploads | pics | | |
| | news | imgs | | |
| | | tmp | | |

Figure 2 Format of URLs connected to by GandCrab v4.1

Fortinet

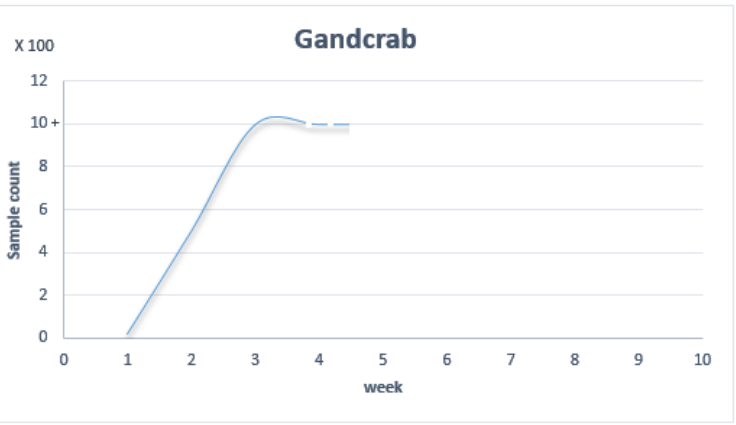



*Figure 1: Number of GandCrab samples by week*

Aconis

# Gandcrab – A Case Study

## GandCrab Ransomware Distributed by Exploit Kits, Appends GDCB Extension

### SUMMARY

Security experts have discovered a new ransomware strain called Malware: GandCrab that is targeting victims in the wild.

Key Findings:

- Malware Variant: GandCrab 2093f6 is currently being distributed through a malvertising campaign called Seamless campaign that then pushes the visitors to the RIG exploit kit
- Following the infection, GrandCrab encrypt the victim's files, appending the .GDCB extension to the encrypted file's name
- GrandCrab is the first ransomware to accept the DASH currency and the first to utilize the Namecoin powered .BIT tld
- Victims are encouraged to pay 1.5 Dash, currently equivalent to $1130 USD

### ANALYSIS

To date, there is no way to decrypt files encrypted by GandCrab for free.

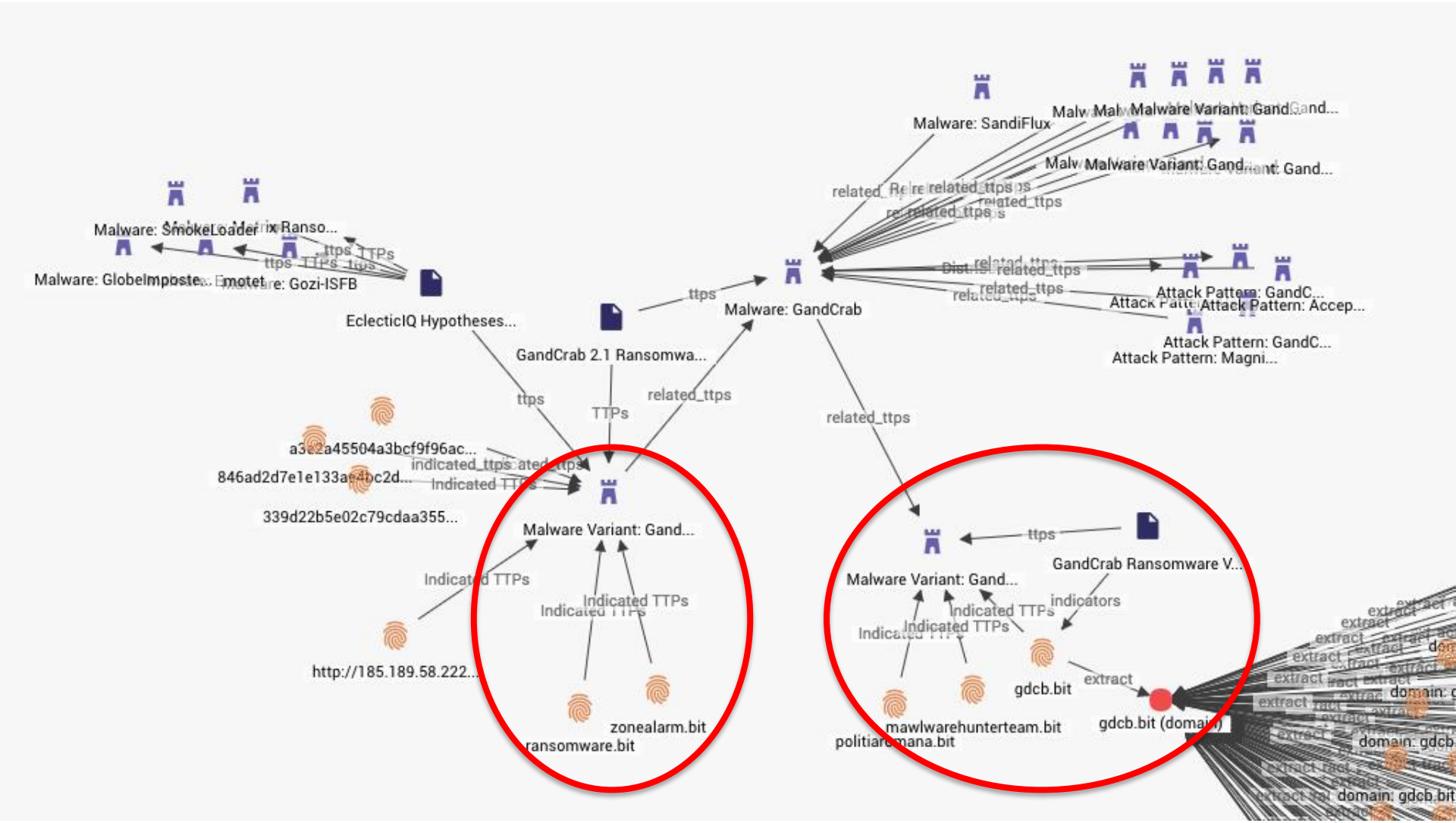
Victims are encouraged to pay 1.5 Dash (cryptocurrency), currently equivalent to ~$1130

GandCrab extortion note:

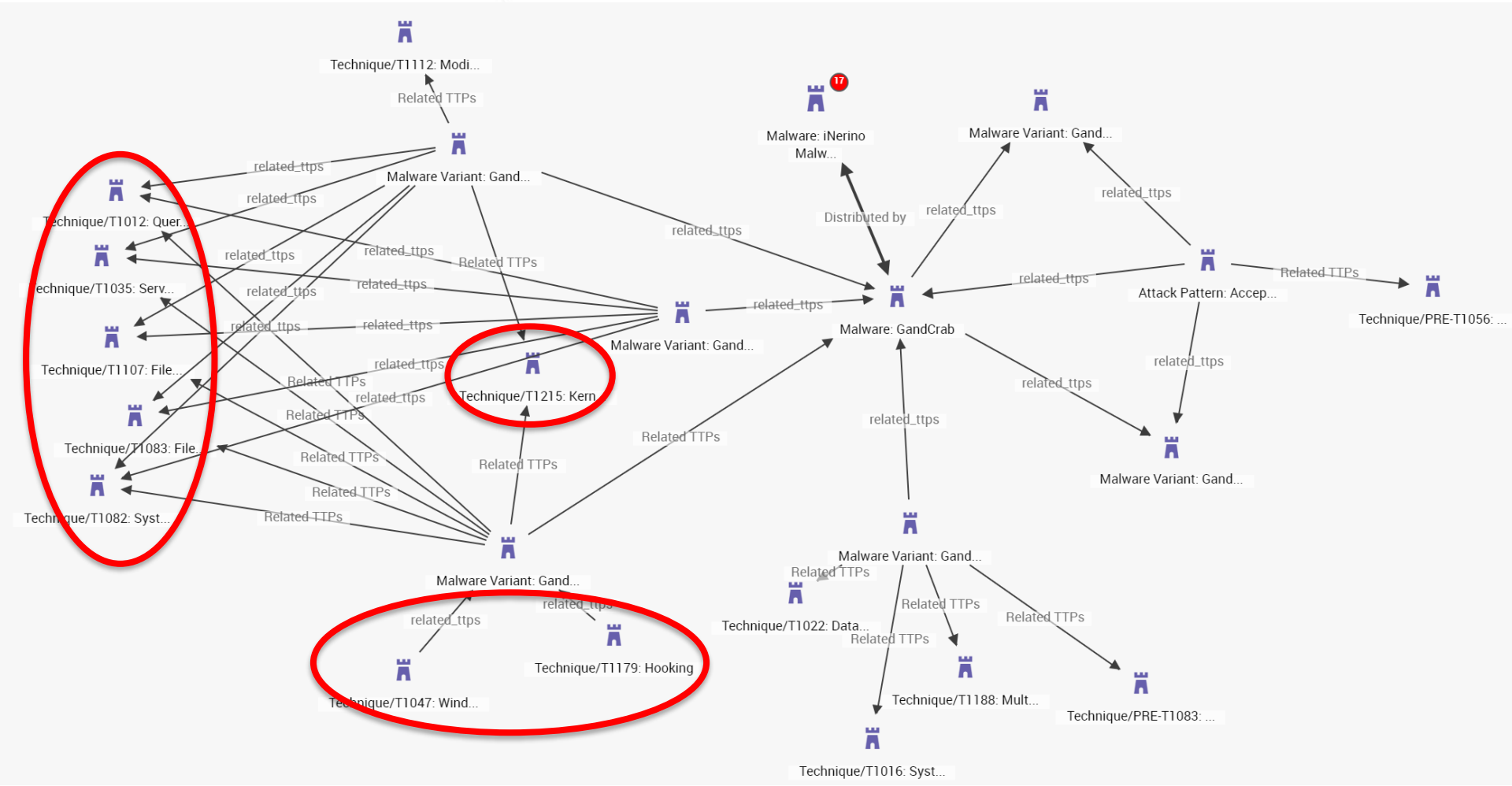
*---= GANDCRAB =---*

*Attention!*
*All your files documents, photos, databases and other important files are encrypted and have the extension: .GDCB*
*The only method of recovering files is to purchase a private key. It is on our server and only we can recover your*

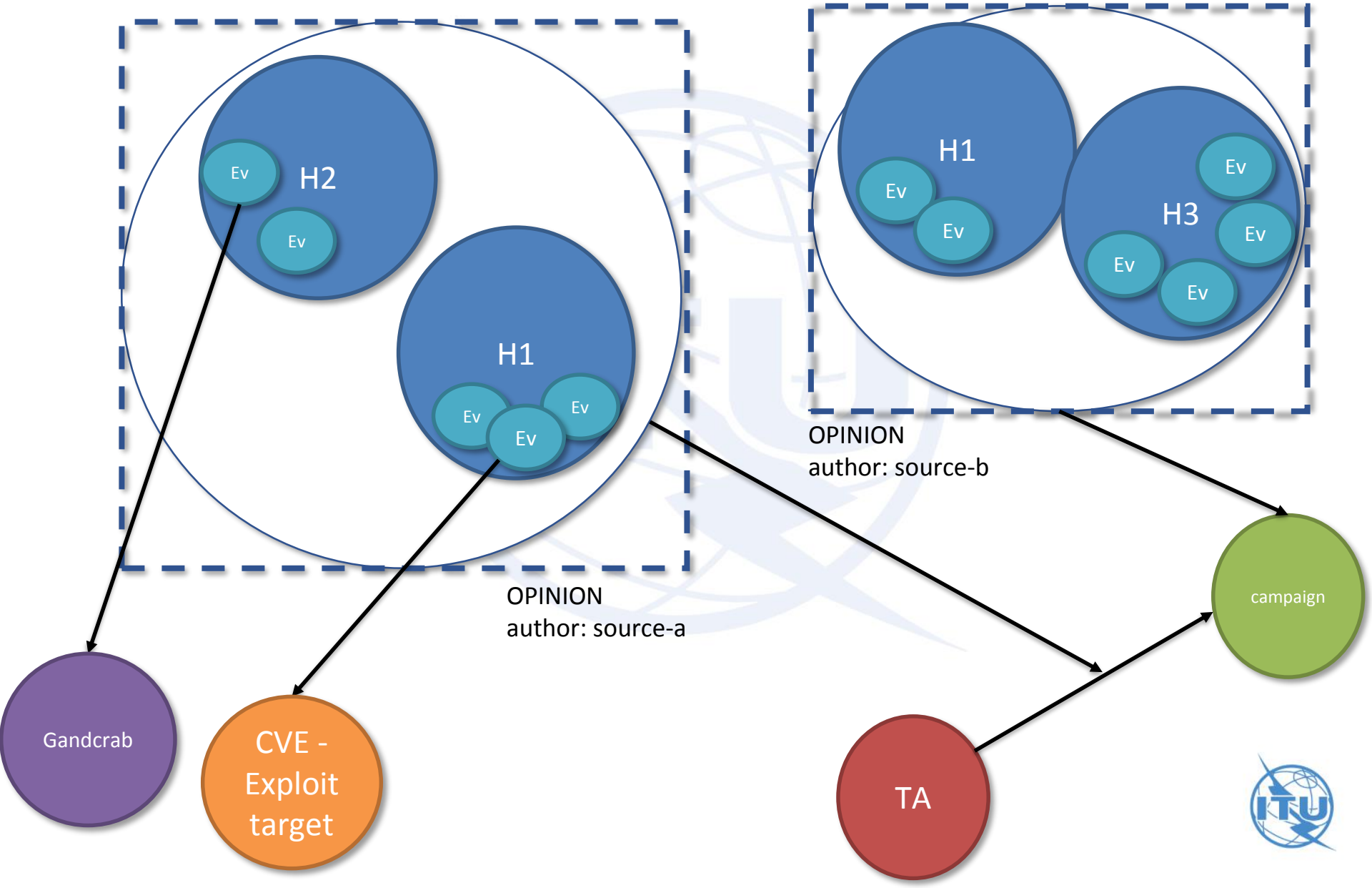
# TTP Re-Use


Malware: SandiFlux
Malware Variant: GandCrab...
Malware: SmokeLoader
Malware: GlobeImposter
motet
Malware: Gozi-ISFB
EclecticIQ Hypotheses...
GandCrab 2.1 Ransomwa...
Malware: GandCrab
Attack Pattern: GandC...
Attack Pattern: Accep...
Attack Pattern: GandC...
Attack Pattern: Magni...
ttps
TTPs
related_ttps
a3e2a45504a3bcf9f96ac...
846ad2d7e1e133ae4bc2d...
339d22b5e02c79cdaa355...
Malware Variant: Gand...
Indicated TTPs
http://185.189.58.222...
zonealarm.bit
ransomware.bit
GandCrab Ransomware V...
indicators
gdcb.bit
extract
mawlwarehunterteam.bit
politiaremana.bit
gdcb.bit (domain)
domain: gdcb.bit

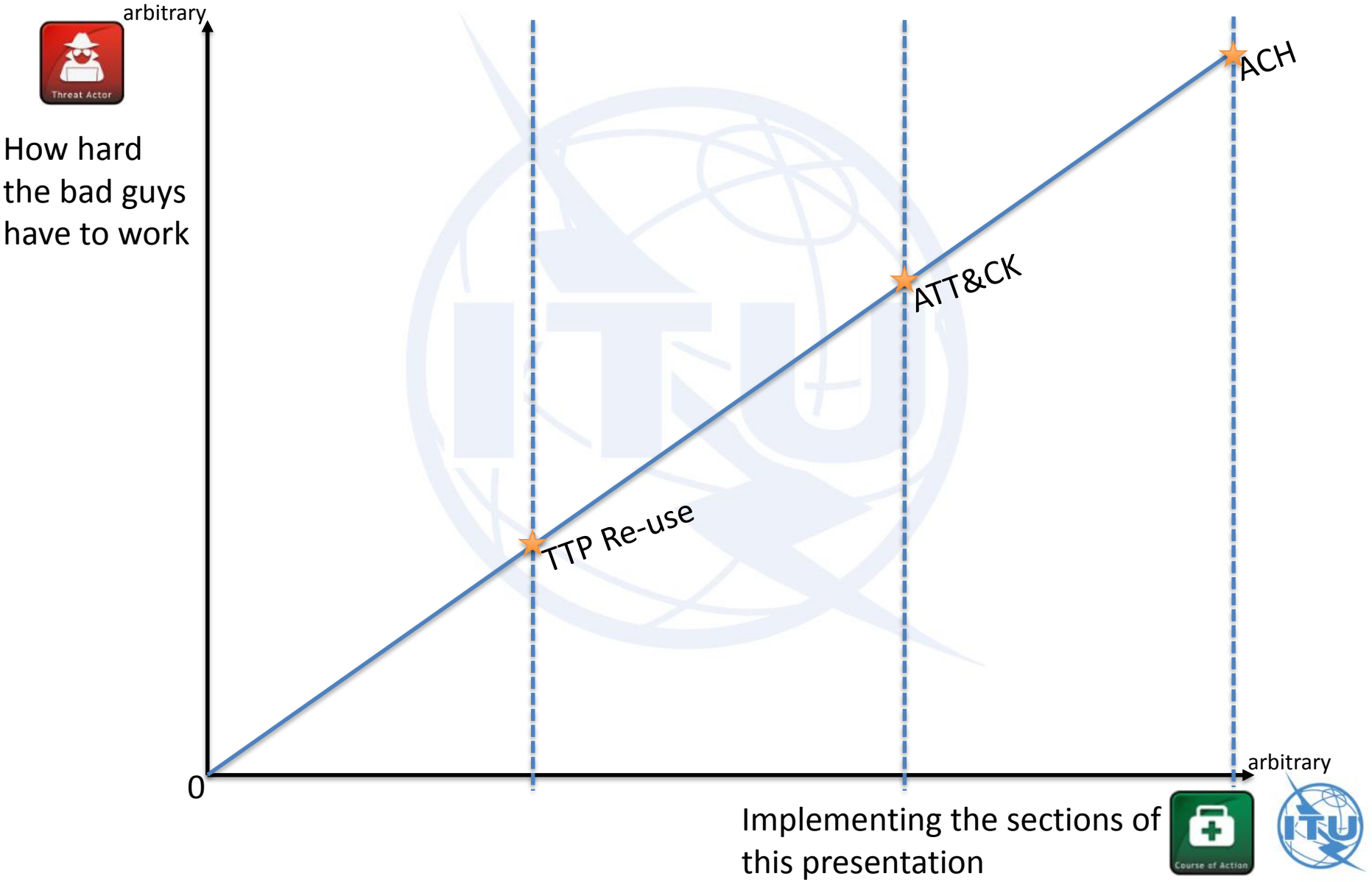
# Mitre ATT&CK Functionality Mapping



# Analysis of Competing Hypotheses



# Advanced CTI Techniques



# Thank you!

https://oasis-open.github.io/cti-documentation/