A different cup of TI?

The added value of commercial threat intelligence

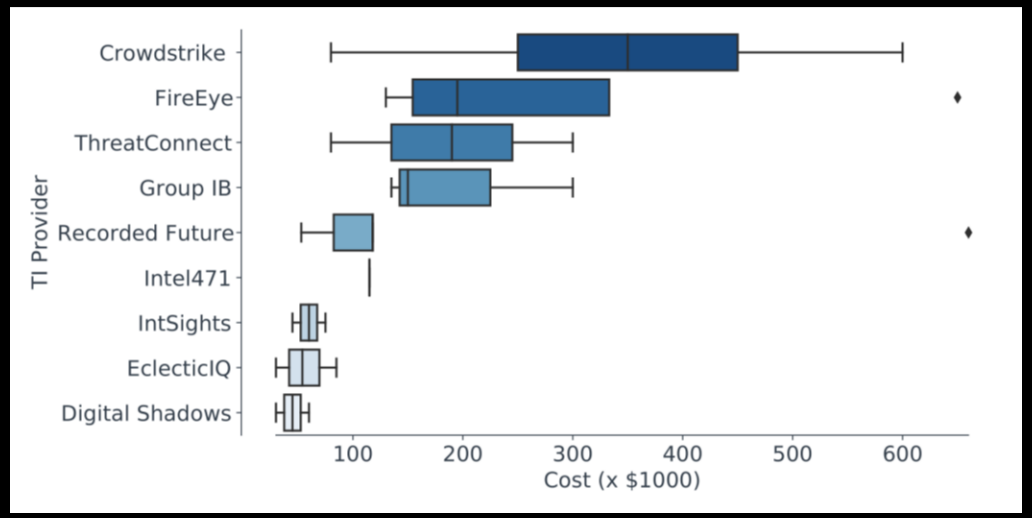
Xander Bouwman, Harm Griffioen, Jelle Egbers,
Christian Doerr, Bram Klievink, and Michel van Eeten

x.b.bouwman@tudelft.nl, @xbouwman

August 12, USENIX Security 2020

Still from *The Maltese Falcon (1941)*

Threat intelligence



Subscription fees of paid TI are prohibitively high for research.

Information on attacker behavior, used to adapt defenses to the threat landscape.

E.g., IPs, domains, hashes, reports.

Three types of external sources:

1. Open sources
2. Shared
3. **Paid, which we are the first to assess**

Questions

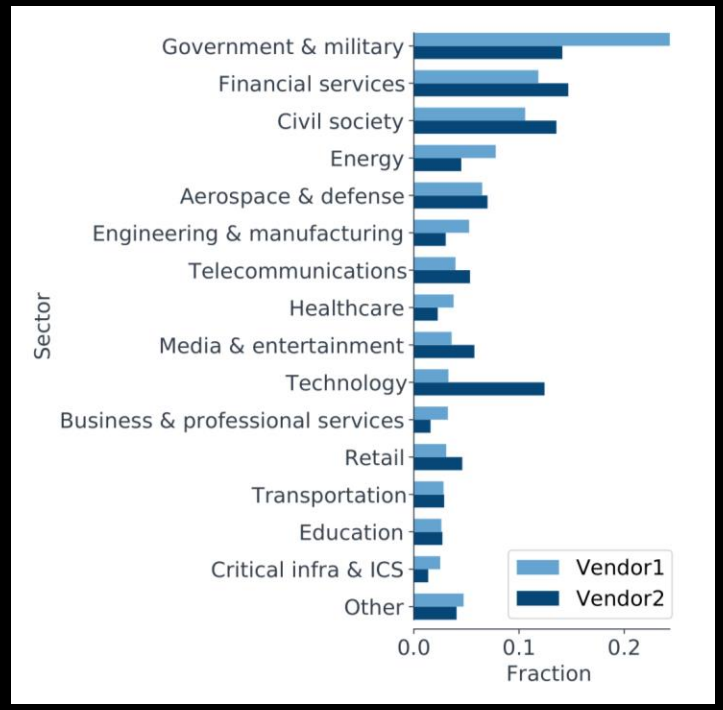
1. What do paid TI services consist of?
2. How is paid TI different from open TI?
3. How do customers use TI and perceive value?

Data

- Services of two leading TI vendors, reports and indicators *(6 years)*
- 6 open sources of TI *(1 month)*
- Interviews with 14 professionals who use paid TI

Method

- Relative comparison of feeds
- Grounded theory for interviews

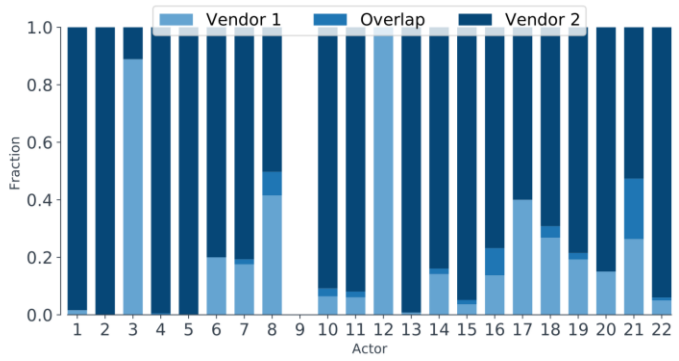


Targeted industries, as identified in the metadata of reports from two leading providers.

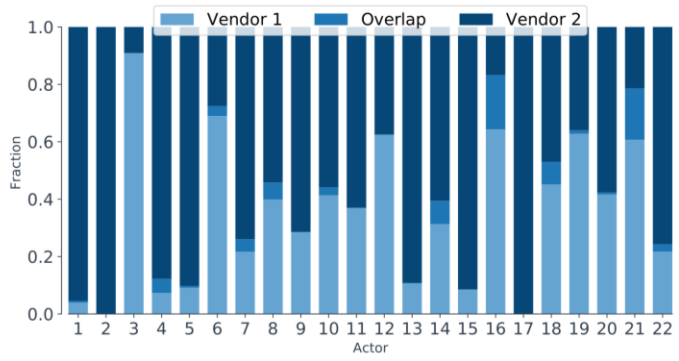
1 What do paid TI services consist of?

- **Threat reports** **71%**
- **Indicators of compromise** **71%**
- Requests for information 57%
- Portals 50%
- Platforms for data mining and aggregation of open sources 29%
- Custom alerts 14%

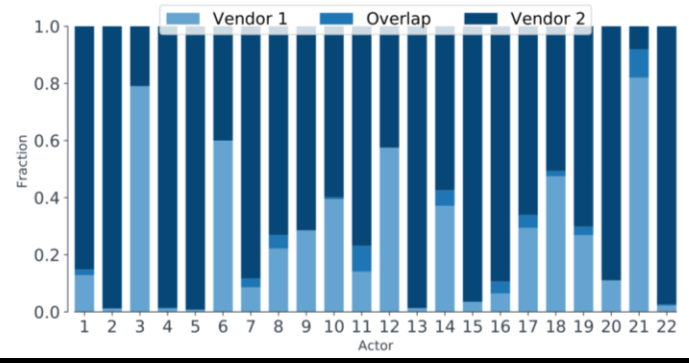
IPs



Domains



MD5s

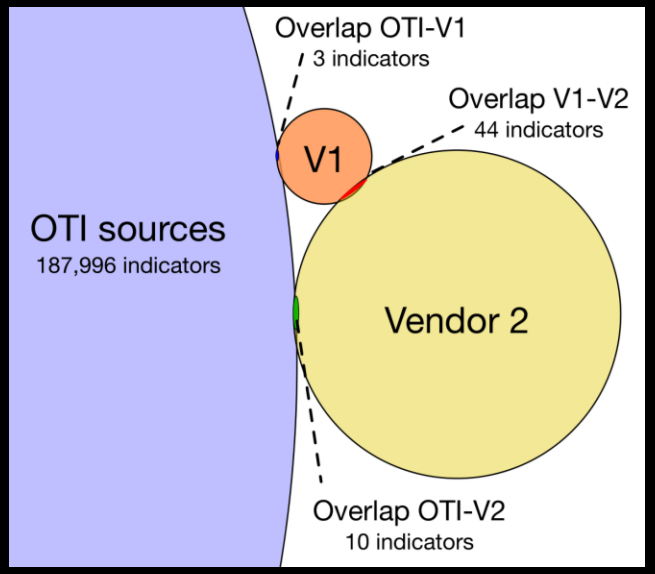


1 What do paid TI services consist of?

Indicator overlap 1.3-13%, depending on which vendor you take as denominator.

For specific threat actors tracked by both vendors no more than 2.5-4.0%, depending on type.

We find largely separate sets, which raises questions about coverage of vendors.



2 How is paid TI different from open TI?

Paid TI sources are smaller. Less than 1% overlap with 6 open source blocklists.

No evidence that paid sources are faster. Delay of one month both ways (small *n*).

Professionals describe paid sources as more comprehensive and ‘polished’.

TI VALUE PERCEPTIONS	Respondents *n=14*
Actionability	
Providing context	100%
Timeliness	50%
Comprehensiveness	50%
Suitable abstraction level	36%
Interpretability	21%
Visualized well	14%
Relevance	
Sectoral focus	64%
Geographic focus	50%
Coverage of relevant threats	50%
Ability to correct bias	14%
Confidence	
Automatability	79%
Confidence in vendor	71%
Original contribution	50%
Accuracy	43%
Selectiveness	29%
Affordability	21%

3 How do customers use TI and perceive value?

Customers want more curated feeds: they seem to be optimizing for the workflow of their analysts, not detection.

TI is mainly used for network detection, but we found also more surprising use cases.

Inductively gathered value perceptions.

Conclusions

- Between open and paid TI sources almost no overlap in indicators.
- Between two leading paid TI vendors 1.3-13% overlap in indicators.
- Even for specific threat actors, the vendors have 2.5-4.0% overlap.
- One-month delay in reporting (small *n*).

- Customers optimize for analyst time (low FP) rather than coverage (low FN).
- Identify interesting use cases of TI besides network detection.
- Costs of paid providers not a concern.
- Value understood through source. confidence, relevance, and actionability.

Still from *The Maltese Falcon (1941)*

Implications

"If you [the attacker] get detected on one machine, all of your offensive infrastructure has to be scrapped".
CCC 2019 talk of Vincenzo Iozzo, Senior Director at Crowdstrike

Customer behavior might better be explained by organizational factors.

Risk of 'market for lemons'.

A different cup of TI?

The added value of commercial threat intelligence

Xander Bouwman, Harm Griffioen, Jelle Egbers,
Christian Doerr, Bram Klievink, and Michel van Eeten

x.b.bouwman@tudelft.nl, @xbouwman

August 12, USENIX Security 2020