Crowdsourcing Intelligence:

Friend or Foe?!

Ryan Trost

WhoamI()

Ryan Trost

- Co-Founder, ThreatQuotient
- Security Operations Center (SOC) experience:
  - Spent the better part of my analyst career in a SOC
  - Managed several large (35+ analyst) DIB and USG SOCs
- Author of *"Practical Intrusion Analysis"* © 2009
- Developed a geospatial intrusion detection model
- Security Conference lectures include
  - DEFCON16, SANS, BlackHat 2014, ISACA ISRM, InfoSec World
- Chairman, Technical Advisory Board – Cyber Security AAS Collegiate program

Presentation Goal

Crowdsourcing intelligence has become mainstream over the past several years but is it:

helping teams defend against attacks?

OR

hurting teams by overwhelming them with false positives and intelligence gaps?

Crowdsourcing Threat Intelligence

Cyber deviants are known to share and re-use attack tactics, payloads, infrastructure…*shouldn't defenders share too?*

Pros:

- Improve defensive posture
- Build invaluable industry relationships
- Improve industry situational awareness
  - threat landscape
  - adversary targeting
  - etc.

"Sharing is caring!"

Cons:

- Trusting others
  - their analysis capabilities
  - making good decisions re: not submitting malware to OSINT repos
- Possible intelligence gaps
- Tools simply CANNOT keep up w/ volume!!
- Knowledge is power – sharing could quickly de-value Intel
  - Lifespan of OSINT vs. commercial vs. internal discovery

"Bad Intel LIVES forever!"

Sharing Efforts

- Industry/Vertical specific
  - DSIE
  - *-ISAC
- USG
  - Handful of USG reports (i.e. I&EW, TIPPR, FBI's JIB)
  - DIB Pilot *[more to come]*
- Vendor (fee & free)
  - Portal (i.e. IBM X-Force Exchange, Alienvault's OTX, Facebook ThreatExchange, etc.)
  - Subscription feed (i.e. iSight Partners, CrowdStrike, Verisign's iDefense, Intel471, etc.)
- Open Source Intelligence (OSINT)
  - Blacklists (200+ various sources)
  - Blogs
  - Whitepapers *("commercial flex")*
- Private Community

What is the Crowdsourcing Motivation?

- Industry/Vertical specific
- USG
  - Classified/FOUO
  - Green TLP
- Vendor
  - Free
  - Commercial
- OSINT
  - Blogs
  - Blacklists
- Private Community

What is the Crowdsourcing Motivation?

- Industry/Vertical specific
- USG
  - Classified/FOUO
  - Green TLP
- Vendor
  - Free
  - Commercial
- OSINT
  - Blogs
  - Blacklists
- Private Community

Contractual Obligation

Public do-gooder

psst…psst…3322.org is EVIL!

What is the Crowdsourcing Motivation?

- Industry/Vertical specific
- USG
  - Classified/FOUO
  - Green TLP
- Vendor
  - Free
  - Commercial
- OSINT
  - Blogs
  - Blacklists
- Private Community

Contractual Obligation

Public do-gooder

psst…psst…3322.org is EVIL!

What is the Crowdsourcing Motivation?

- Industry/Vertical specific
- USG
  - Classified/FOUO
  - Green TLP
- Vendor
  - Free
  - Commercial
- OSINT
  - Blogs
  - Blacklists
- Private Community

Contractual Obligation

Public do-gooder

psst…psst…3322.org is EVIL!

What is the Crowdsourcing Motivation?

- Industry/Vertical specific
- USG
  - Classified/FOUO
  - Green TLP
- Vendor
  - Free
  - Commercial
- OSINT
  - Blogs
  - Blacklists
- Private Community

Contractual Obligation

Public do-gooder

psst…psst…3322.org is EVIL!

IOC Volumes

There are over 200 OSINT blacklists that are published by defending do-gooders to help others…but WOW that's a LOT of indicators!!

Feed Name	Total Indicators	Avg/Month	Avg/Day	Nov-14	Dec-14	Jan-15	Feb-15	Mar-15	Apr-15	May-15	Jun-15	
www.dan.me.uk Tor Node List	267,198	33,400	1,113	19,681	33,623	34,205	28,454	29,486	26,329	26,423	25,940	
torstatus.blutmagie.de All Tor Nodes	256,667	32,083	1,069	18,993	35,520	32,072	26,766	27,945	24,975	24,951	24,576	
torstatus.blutmagie.de Exit Tor Nodes	28,071	3,509	117	2,710	3,883	3,860	3,175	3,213	2,638	2,742	2,371	
cydef.us Tor Exit Nodes	33,669	4,209	140	3,947	8,355	5,567	4,315	4,468	3,741	3,276	N/A	
blocklist.de (All)	1,318,766	164,846	5,495	87,056	115,586	103,244	88,277	141,617	159,149	130,063	160,241	
blocklist.de (SSH)	130,944	16,368	546	4,451	9,326	16,827	15,908	11,953	18,263	6,351	16,541	
blocklist.de (Mail)	460,133	57,517	1,917	46,329	31,147	31,683	33,559	50,402	48,993	68,818	64,190	
blocklist.de (Apache)	489,552	61,194	2,040	26,469	53,698	37,554	23,432	47,555	45,251	25,126	60,738	
blocklist.de (IMAP)	154,306	19,288	643	19,612	5,840	4,136	4,807	8,774	19,410	32,204	34,116	
blocklist.de (FTP)	93,706	11,713	390	2,935	4,725	1,611	1,160	6,559	18,720	12,782	10,454	
blocklist.de (Bots)	224,891	28,111	937	19,348	31,407	25,955	22,370	27,795	33,608	22,092	15,723	
blocklist.de (Brute Force Login)	446,203	55,775	1,859	12,066	47,795	36,194	22,285	43,152	40,999	21,118	58,043	
Alienvault OTX	1,561,011	195,126	6,504	157,095	173,863	169,462	150,989	223,326	199,855	143,622	175,571	
hpHosts	309,640	44,234	1,474	N/A	66,937	38,281	40,529	29,776	48,918	62,129	15,751	
COMMERCIAL FEED 1	4,843,657	691,951	23,065	N/A	313,289	388,173	651,648	560,729	457,709	584,407	632,737	
COMMERCIAL FEED 2	186,111	26,587	886	N/A	31,601	18,130	28,842	15,782	14,187	19,373	19,049	

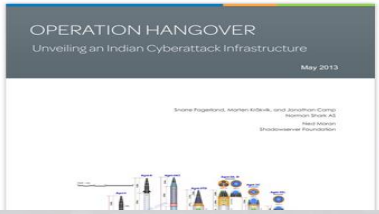
Crowdsourcing Mediums

- Documents (Google doc for collaboration)
- Email (listserv)
- Web
  - Portals
  - Blogs
- Social Media
- Feeds
  - CSV, XML, JSON, STIX/TAXII, etc.
- "Indirect Notification/Alerting"
  - DIB Pilot
- Bridge Calls
  - Usually Government
- In-Person
  - TechExchange
  - Conference [beer]

1-to-1

1-to-Many

Many-to-Many



STIX

- Developed by Mitre to answer the “machine-to-machine” sharing
  https://stix.mitre.org/
- Steady momentum over the past 2 years but still has some kinks
  - STIX is very robust, but....
    - For being a "structured" language it is very unstructured:
      - An indicator can appear in 4 different places:
        - » STIX -> Indicator
        - » CybOX -> Observable
        - » STIX -> Description
        - » STIX -> TTP
  - XML Bloat; file size increases exponentially when large organizations share verbose findings
- Recently transitioned over to OASIS, an open standard forum

DIB Pilot

- USG's attempt to "share" classified indicators to the Defense Industrial Base (DIB) through indirect means (via ISP)
  - DNS sinkholing
  - Email monitoring
- Mixed results based on who you ask
  - Negative reaction:
    - missed adversary attacks
    - very little information was provided to help investigations (Classified)
  - Positive reaction:
    - USG is SHARING!! (it took years for USG Legal and DIB Legal to come to an agreement around the effort)
- Results of the pilot DO NOT accurately reflect the mountainous hurdle this overcame

http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf

Mastering a Crowdsourcing Model

- Self-Reflection
  - "Threshold of pain"
    - Volume
    - IOC Type
    - Resources
  - Ability to streamline
- Which Source(s) do I trust?
- Find a company with similar:
  - Size
  - Capabilities
  - Adversaries
  - Budget
- Continually re-assess source(s)

Conclusion

Crowdsourcing intelligence is a powerful mechanism to augment existing efforts but it needs to be closely monitored OR it leads to intelligence gaps and ‘paralysis by analysis’.

QUESTIONS?

Ryan.Trost@threatq.com