Building a Business Case for Cyberthreat Information Sharing

HKCERT Information Security Summit
Hong Kong
September 4, 2018

IT ISAC

IT-ISAC Overview

- Founded in 2000 to facilitate information sharing among industry competitors. Office in Manassas, VA, USA.
- Global membership from a diverse set of companies that produce, use, and leverage IT products and services for core business operations.
- Not for profit corporation comprised of corporate members and managed by the Board of Directors.
- A collaborative forum, not just a threat feed.
- Not part of any government agency, entity or department.

IT ISAC

What is our Mission?

Grow a diverse community of companies that leverage information technology and have in common a commitment to cyber-security; to serve as a force multiplier that enables collaboration and sharing of relevant, actionable cyber threat information and effective security policies and practices for the benefit of all.

(emphasis added)

The Information Sharing Challenge

- Sharing sensitive information is not part of most corporate cultures
  - Risks of sharing are understood, value of sharing is less understood
  - Lawyers are risk adverse
- Developing and implementing trusted frameworks is resource intensive
  - How many lawyers does it take to create an NDA?
  - How do you train people on what is in the NDA?
  - Who do I engage with?
- The amount of information available is almost limitless
  - What information do I share?
  - I already have too much information—why do I need more?

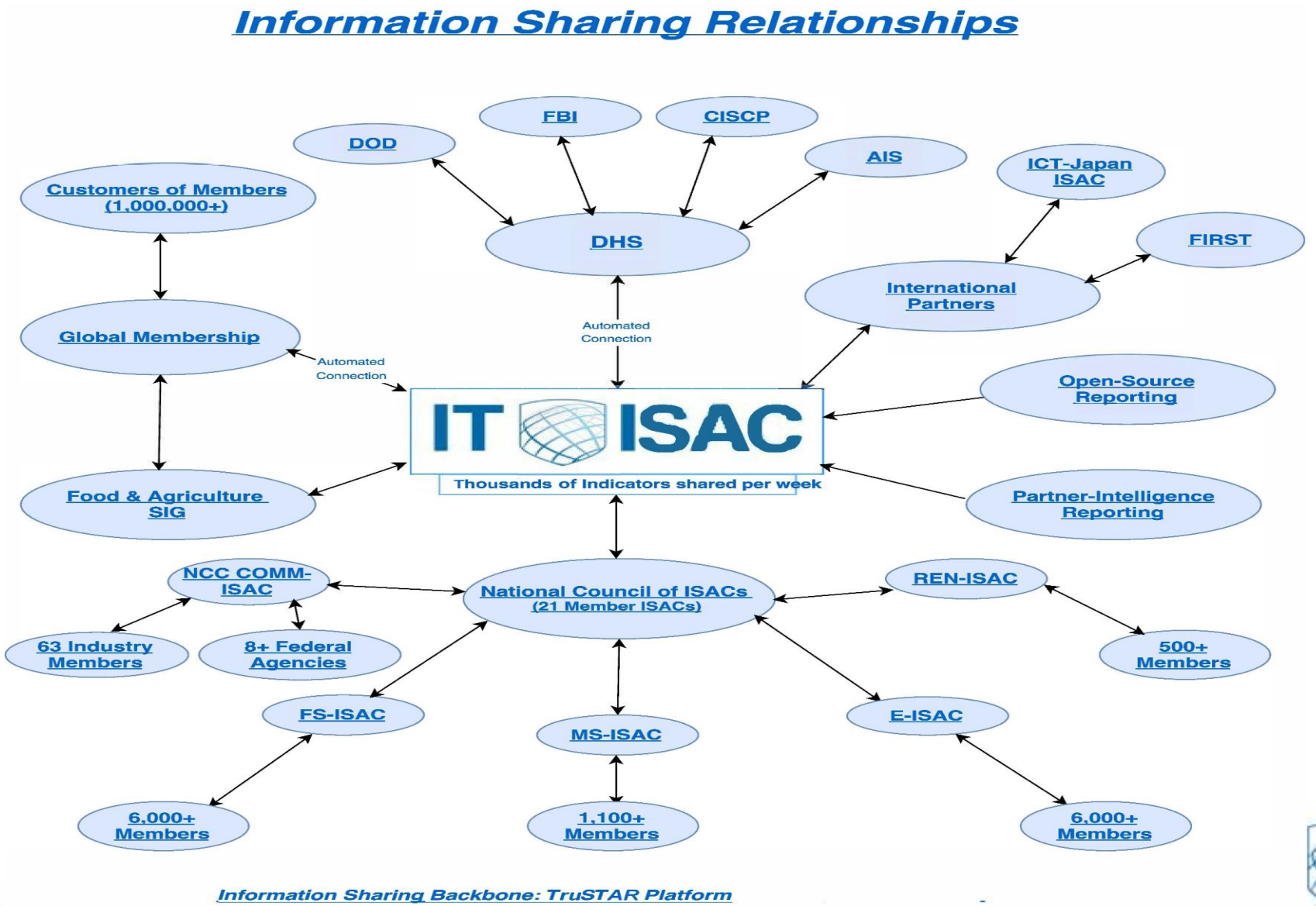
IT ISAC

The Business Case for Sharing

- Sharing is a risk management activity
  - Information sharing is a tool to achieving enhanced situational awareness
  - You get (and provide) early warnings by sharing
- Collaboration amortizes the cost of defense
  - By sharing with others you learn from others
  - Identify actors and threats you may not have been tracking
  - You help your suppliers, partners and competitors secure their enterprises
- Entering and era of increased risk of cyber regulations
  - Demonstrate to stakeholders corporate commitment to protecting its brand, assets, customers, employee and IP
  - Act voluntarily or accept regulatory mandates

IT ISAC

Strength in Numbers



ISAC

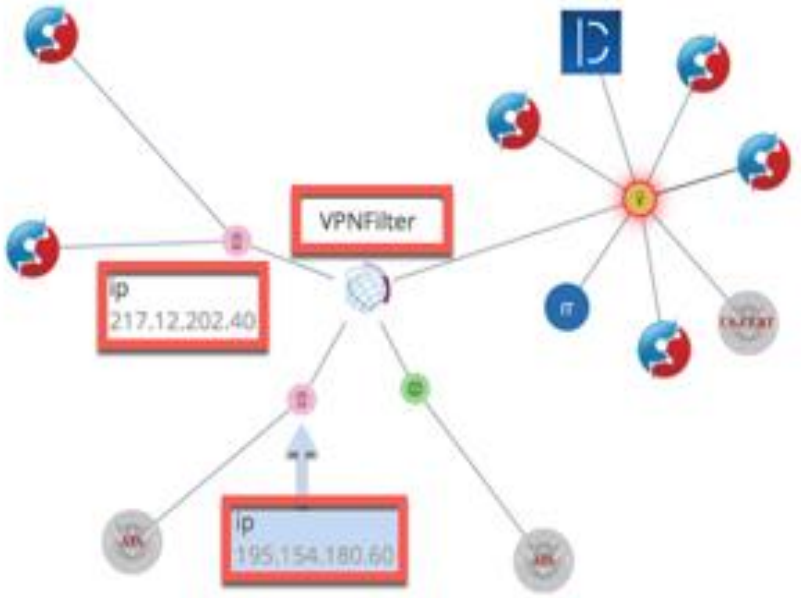
Benefits of Sharing with Competitors

Turn the competitor into a partner!

- The threats to your businesses are shared. A shared threat is an opportunity for joint defense.
- They are seeing the same attacks you are seeing. Learn from each other.
- You are both monitoring different actors. Pool resources for mutual benefit.
- If an actor successfully takes down your competitor, they can come after your company next.

IT ISAC

The more we share. . .



VPNFilter

Content | IOCs (54)

Known C2 Domains and IPs

ASSOCIATED WITH THE 1ST STAGE

photobucket[.]com/user/nikkireed11/library

[redacted]

photobucket[.]com/user/bob7301/library

toknowall[.]com

ASSOCIATED WITH THE 2ND STAGE

91.121.109[.]209

217.12.202[.]40

94.242.222[.]68

82.118.242[.]124

46.151.209[.]33

217.79.179[.]14

91.214.203[.]144

95.211.198[.]231

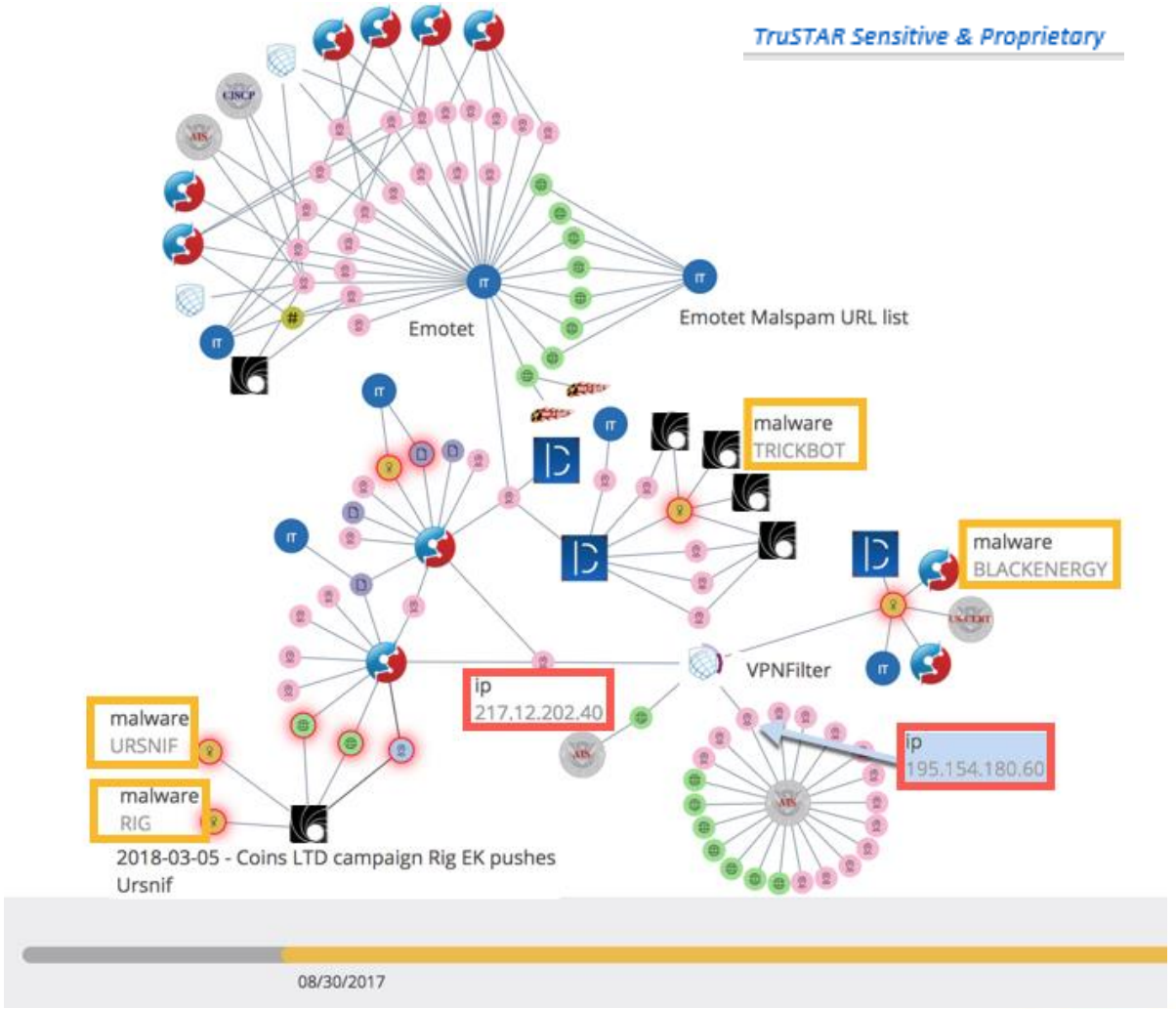
195.154.180[.]60

08/30/2017 — 05/25/2018

IT ISAC

The more we see

- Pivot to Atomic IOCs
  - 195.154.180.60
  - ROI: 21 IOCs
- Pivot to Contextual IOCs
  - 217.12.202.40
  - ROI: 208 IOCs
  - 2nd Hop: 349
- Associated Malware
  - Ursnif
  - Trickbot
  - Emotet
  - Rig EK
- Campaign
  - Coins LTD



Sharing Aides Analysis

- Customized analysis through TIPs
  - Members can hunt based on their specific needs
- IT-ISAC provides trending analysis
  - Trending Malware
  - Threat actors/campaigns trends we're seeing
  - Active vulnerability exploitation
- Incident analysis
  - Research and truth detecting
- Collaborative analysis
  - Consulting with partners in National Council of ISACs
  - Discussions with and among ISAC members

IT ISAC

How to Share

- Automation vastly increases the scale of information that can be shared
  - Companies control what precisely what they share
  - Easier to share without attribution
- Secure platforms
  - Manually intensive but still effective
- Meetings, secure chat, and lists
  - Builds trust by promoting collaboration and personal connections
- Through trusted third party
  - Enables submissions without attribution

IT ISAC

Case Study: Petya/Not Petya—July 2017

- Active engagement with members and partners
- Hosted out of cycle Technical Committee meeting with members
  - Captured and shared with members:
  - Payload Sample
  - Open Source Summary Reporting on a daily basis
  - Methods of Spreading
  - What Happens Once Affected
  - Mitigation and Defensive Measures
  - C2 Payment Servers
  - Confirmed VirusTotal Files
  - IOCS: File Hashes & IPs

IT ISAC

Phantom Squad- Sept. 2017

Hello, [redacted]

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Phantom Squad

Your network will be DDoS-ed starting Sept 30st 2017 if you don't pay protection fee - 0.2 Bitcoin @ 15BMLAkAVoUDDdzrBnX8Wh6RGjHsuVL3GF.

If you don't pay by Sept 30st 2017, attack will start, yours service going down permanently price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

This is not a joke.

<http://autolampen-moser.de/js/mage/adminhtml/sales/aw.php?A6jXCJqLAp3fwnf0%2F7AgnX3S9zK0P9OjKEKmYTWeNu7P0c1qqO8LEQB08g%2Bx7CNqF%2BdS75PpweQc0T1uCm3zOgK30UwRuOHcbreHx5NMyYfEiStWbwKG2VZInmMrwGBZIVofw4YRXtPKCNqGhKgoEA%3D%3D>

IT ISAC

Value to the Company that Shared

- We discovered there had been no open-source reporting about this so reached out to the IT-ISAC and partner ISACs.

- Other IT-ISAC members and our partners reported back, within minutes and informed us they saw the same malicious email and it was a hoax.

- We captured and shared with members:
  - IP Addresses
  - Bitcoin Wallet Addresses
  - Advice on What To Do

IT ISAC

Golden Niagara/Gold Lowell- February 2018

- Member reaches out to us asking for information on “Golden Niagara”
- Confirm the actual actor is Gold Lowell—Sam Sam Ransomeware that was actively impacting some cities and states in the U.S.
- Received and shared threat reports that contained IoC’s.
- Value—company saw indicators associated with an active, ongoing attack that was impacting other organizations. By collaborating with the IT-ISAC, we were able to confirm the actor and provide indicators associated with the active campaign.

IT ISAC

Heartbleed March 2018

- Member shares with us a suspicious IP. Not sure what it is.
- We share it with members and partners who confirm the IP is a malicious IP known to be used in the an attack exploiting the Heartbleed vulnerability.
- Value—Member company can now look for other indicators on their network associated with Heartbleed exploitation and take protective action.

IT ISAC

What's Next

- Enhanced Automation
  - OASIS is doing great and important work on STIX/TAXII standards
- Moving Beyond Indicators
  - How to collaborate on common security challenges
  - Joint analytical products with members and partners
- Coordination
  - How do we turn individual initiatives into a common capability?
  - How do we automate sharing within the ISAC Community?

IT ISAC

In Sum . . .

Sharing adds value by:

- Building trusted relationships that can amortize the cost of security
- Providing enhanced situational awareness
- Increasing analytical capacity
- Increasing the overall level of security throughout the larger community
- Demonstrating corporate commitment to voluntary industry leadership

IT ISAC

Promote a Culture of Sharing

- Create a business case that demonstrates how sharing adds value to the company.
- Establish policies and authorities that detail who can share what.
- Identify trusted partners build relationships with them.
- Deploy/leverage automated capabilities that make sharing less resource intensive.
- Empower analysts to engage and collaborate with their peers.
- The “bad guys” are not your competitors but are the people attacking your network.
- The threat actors are sharing and so must network defenders.

IT ISAC

Thank You!

Scott C. Algeier

Executive Director, IT-ISAC

+1 703-385-4969

salgeier@it-isac.org

@ITISAC