

Practical Incident Response & Threat Intelligence

Adli Wahid

Email: adli@apnic.net

Twitter: [@adliwahid](https://twitter.com/adliwahid)

Talking Points

Share observations & reflections of IR community :

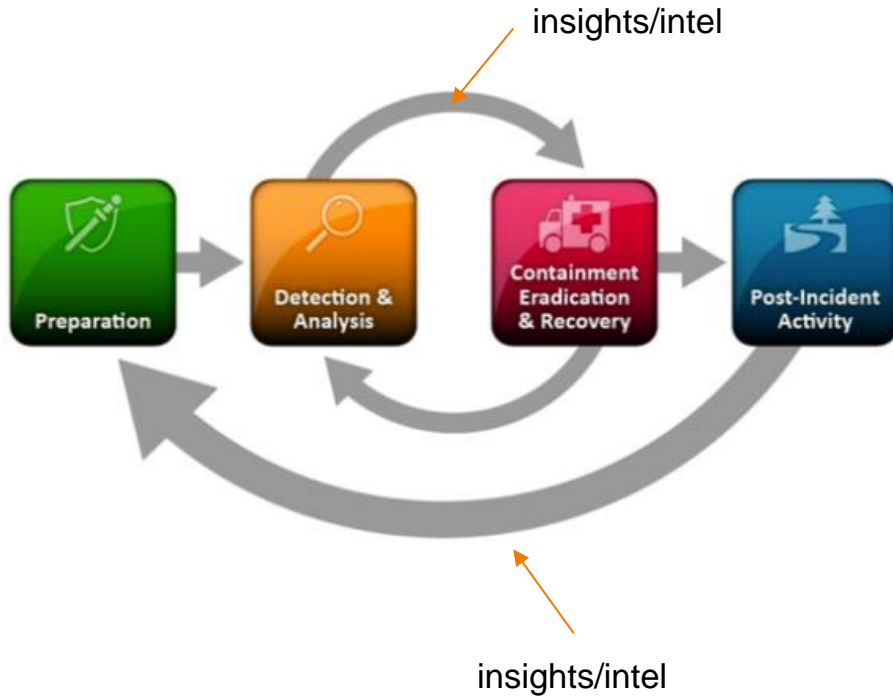
1. Incident Response in Practice
2. Cyber Threat Intelligence & Incident Response
3. Issues and Challenges
 - Consumer vs Contributor
 - Maturity
 - Actionability
4. Realities on cooperation and sharing

The Big Picture



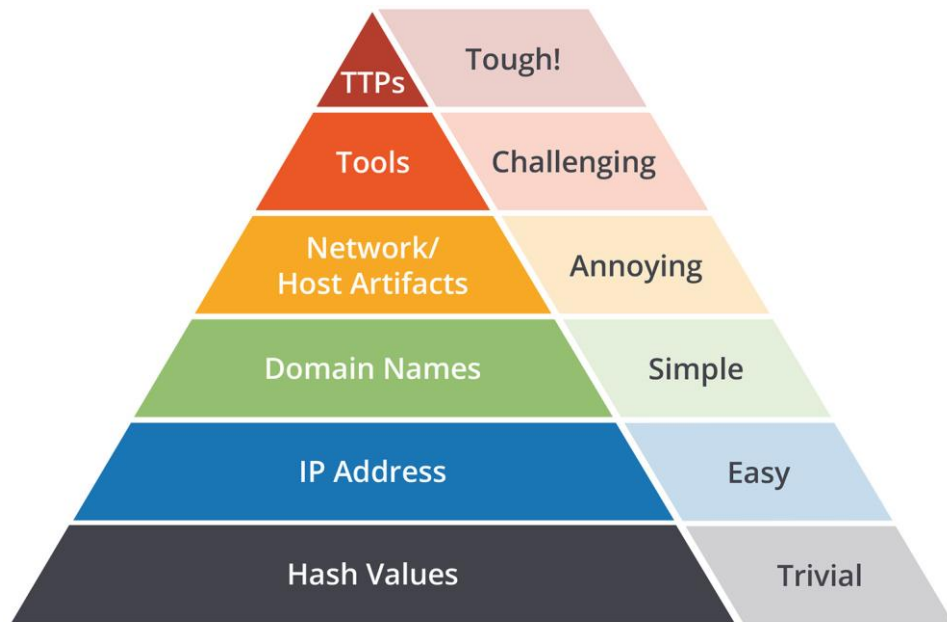
NIST Cybersecurity Framework 1.1

Incident Response in Practice



- Planning to deal with security incidents
- Understanding Threats and Risks
- Increase resilience
- Goldmine for insights (intelligence) from lessons learned (post-incident)

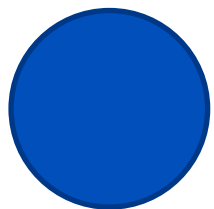
Cyber Threat Intelligence (CTI)



Source: David J. Bianco, personal blog

- Detection & Prevention
- Usefulness of intelligence and
- Difficulties of obtaining them
- The higher you get the more resources adversaries have to expend
- Amount of work to extract Indicators of Compromise (IOCs)
- TTPs = Tactics, Techniques and Procedures

Detecting or Preventing



Research
Analysis



1. IP address
2. Domain
Names (C&C)
3. File name
4. File Hash
5. Email Sample
6. etc



1. Anti Virus
2. IDS
3. Yara
4. Firewall
5. Proxy
6. EDR
7. Reports
8. Threat Hunting

Ransomware.exe

Not So Straight Forward

Wannacry

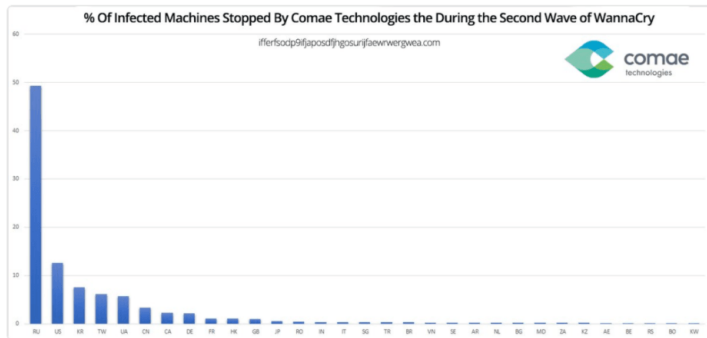


Matthieu Suiche ✓

@msuiche

Following

Since registering the 2nd killswitch yesterday, we stopped ~10K machines from spreading further - mainly from Russia. #WannaCry #OKLM



RETWEETS

146

LIKES

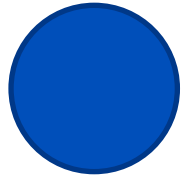
180



10:39 AM - 15 May 2017

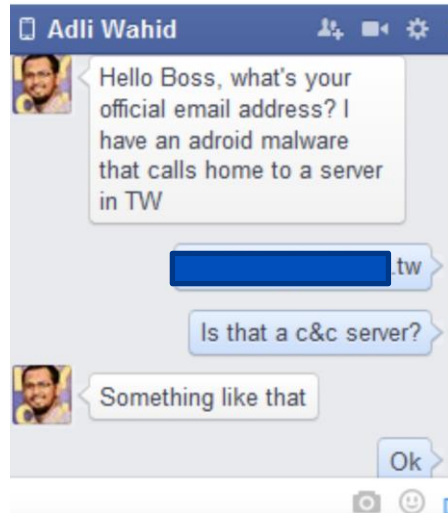
- Ransomware attack in May 2017
- Uses EternalBlue exploit leaked in April
- Targets Windows SMB, spread over the internet (worm)
- Domains:
 - `iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea[.]com`
 - `ifferfsodp9ifjaposdfjhgosurijfaewrwegwea[.]com`
- Kill switch:
 - Tries to connect to a website (domain hardcoded)
 - If connection works, exit
 - Else, encrypt
- Lessons Learned
 - Not just blocking
 - Quality of sharing / IOCs
 - Timeliness
 - Evolving Attack

Investigation (2014) – Android Botnet



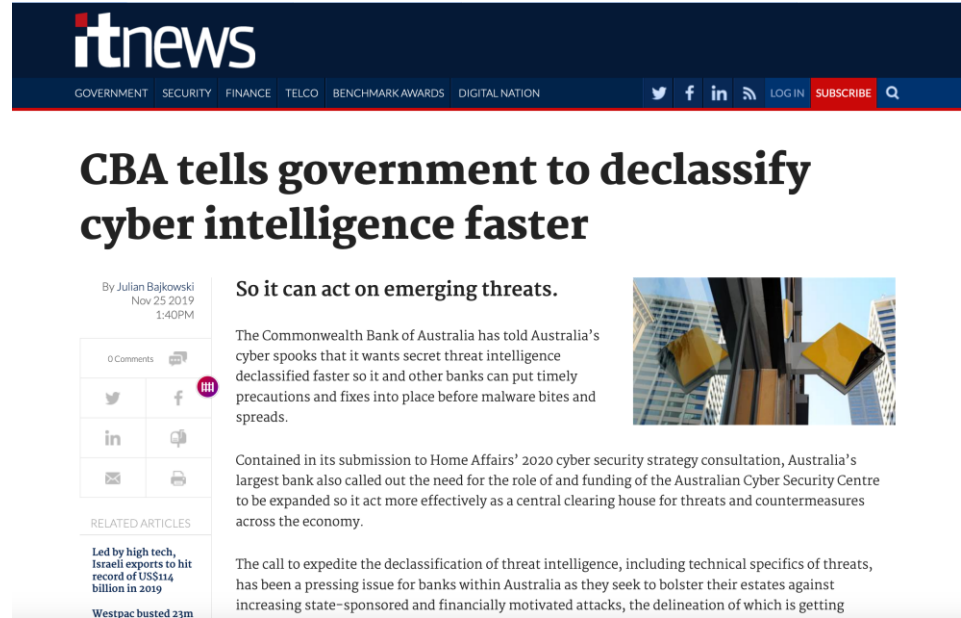
C & C in TW

Android.apk
(found in MY)



- Malware on Dropbox
- 3 Months Investigation (CERT & LEA & ISP)
- 44,506 IP addresses (bots) infected machine
- 4,324,440 NTD amount stolen from users in MY
- Attacker operating from IP outside of TW
- Personal information (phone book) & Phones compromised
- What's next?
- Lessons Learned
 - Share even the small data
 - Build trust before incident
 - Be practical in sharing but careful
 - Dilemma take down or investigate
 - Cross country – investigation & remediation

Collaboration?



The screenshot shows the top of an IT News article. The header includes the 'itnews' logo and navigation links for Government, Security, Finance, Telco, Benchmark Awards, and Digital Nation. Social media icons for Twitter, Facebook, LinkedIn, and RSS are also present, along with 'LOG IN', 'SUBSCRIBE', and a search icon.

CBA tells government to declassify cyber intelligence faster

By Julian Bajkowski
Nov 25 2019
1:40PM

0 Comments


Twitter Facebook LinkedIn Email Print

RELATED ARTICLES

- Led by high tech, Israeli exports to hit record of US\$11.4 billion in 2019
- Westpac busted 23m

So it can act on emerging threats.

The Commonwealth Bank of Australia has told Australia's cyber spooks that it wants secret threat intelligence declassified faster so it and other banks can put timely precautions and fixes into place before malware bites and spreads.



Contained in its submission to Home Affairs' 2020 cyber security strategy consultation, Australia's largest bank also called out the need for the role of and funding of the Australian Cyber Security Centre to be expanded so it act more effectively as a central clearing house for threats and countermeasures across the economy.

The call to expedite the declassification of threat intelligence, including technical specifics of threats, has been a pressing issue for banks within Australia as they seek to bolster their estates against increasing state-sponsored and financially motivated attacks, the delineation of which is getting


Ref: <https://www.itnews.com.au/news/cba-tells-government-to-declassify-cyber-intelligence-faster-534549>

UN NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE


1 INTERSTATE COOPERATION ON SECURITY



2 CONSIDER ALL RELEVANT INFORMATION



3 PREVENT MISUSE OF ICTs IN YOUR TERRITORY



4 COOPERATE TO STOP CRIME & TERRORISM



5 RESPECT HUMAN RIGHTS & PRIVACY



6 DO NOT DAMAGE CRITICAL INFRASTRUCTURE



7 PROTECT CRITICAL INFRASTRUCTURE




8 RESPOND TO REQUESTS FOR ASSISTANCE




9 ENSURE SUPPLY CHAIN SECURITY



10 REPORT ICT VULNERABILITIES



11 DO NO HARM TO EMERGENCY RESPONSE TEAMS



State of the Collaboration

Positives

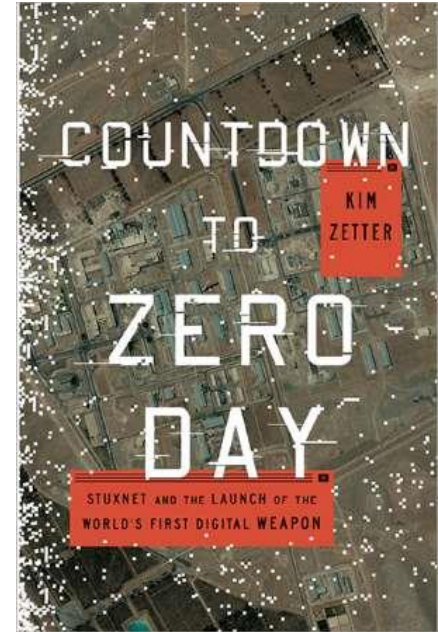
- Frameworks
 - STIX & TAXII
 - ATT&CK
- Tool
 - MISP by Circl.lu
 - Lots of development
- Expectations
 - Traffic Light Protocol (TLP)
 - Norms
- ISACs, Sector Based Sharing
 - FS-ISAC
- Share early
 - Validation by community

Could be Better

- Not ready to consume
 - Lack of process, automation, resources
- Consume only
 - Not ready to share
 - Stigma: “Should only share validated information”
- Creates gaps in quality
 - sector, regional, big picture
- Trust
 - Sharing with adversary or friend?
 - Exclusive club
- Lessons learned
 - All information is useful
 - MISP-Warninglist (false positives)
 - Sinkholes

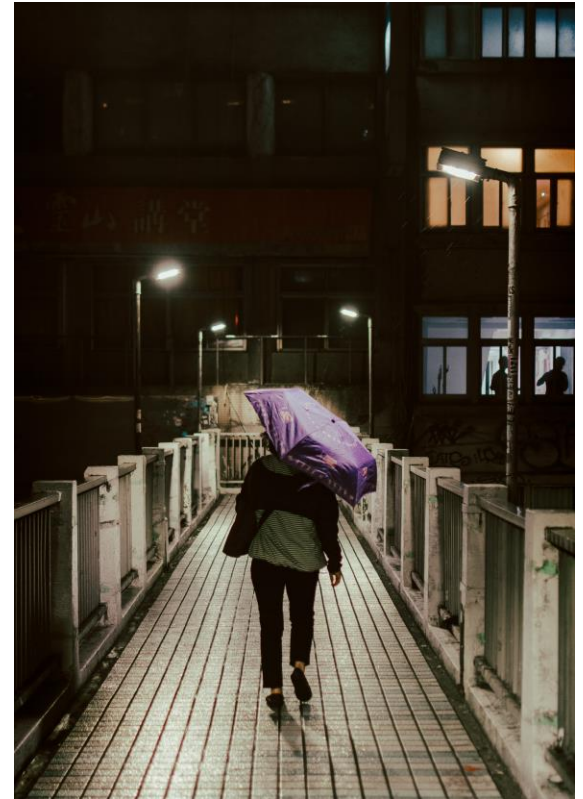
Legal & Political Challenges

- Security & Geo-politics
- Sanctions
 - Political Tool
- Realities
 - Security incident happens globally
 - An incident may start in one location, spread out (by accident or by design)
 - Daily affair for security community but somewhat invisible to many
 - Vulnerability exploited in a sanctioned economy maybe repurposed against another
- Implication
 - Illegal to collaborate / contact
 - Timeliness
 - Information Gathering /Quality of Data
 - Preventing / Mitigating attacks
- Example
 - Stuxnet (2010)
 - Discussion at the recent IGF in Berlin (Cybersecurity BPF & Session on Norms)



Conclusion

- Threat Intelligence
 - Enhance your IR plan/practice
 - Consume and contribute
 - Allocate resources, enhance process
- Learn More
 - MISP Summit
 - FIRST Cyber Threat Intel Summit
 - SANS CTI Summit
- Technical community – reach out & share feedback with other stakeholders (i.e. policy makers)
- Get involved
 - Security Track @ APRICOT & APNIC Conferences
 - Community HoneyNet Project



Let's Connect!

Adli Wahid

- Email: adli@apnic.net
- LinkedIn: Adli Wahid
- Twitter: [@adliwahid](https://twitter.com/adliwahid)