27th ANNUAL
FIRST CONFERENCE BERLIN
14 - 19 JUNE 2015

UNIFIED SECURITY:
IMPROVING THE FUTURE

Best Practices in a Small Cyber Threat Intelligence Program

Katherine Gagnon, CISSP, GCIH, GCPM
Information Security Officer
World Bank Group

Intro to World Bank intel team

- Participate with peers outside WBG to exchange threat information
  - Financials
  - International Orgs
  - Threat Researchers
  - Service Providers
- Consume relevant information to protect WBG resources
- Protect WBG reputation
- Awareness: security operations & IR teams, management, users, other technical teams, etc.

Multi-stakeholder Engagement

Indicators of Compromise

- IP Address
- URL
- FQDN
- User Agent
- Email: Subjects, Senders, Attachments, etc.

….and more…..

Consuming all that data

- It is ***critical*** to understand the business to triage IOCs – what really could have an impact and what resources are important to protect from threats?
- It is also critical to have a clear picture of the corporate infrastructure to consider, if a protective measure is to be implemented against a specific threat, what can be applied and where.
- ***Agility is <u>key</u>*** – intel information has a short shelf life, so action needs to be taken in a timely manner.

Staff

- Team Lead: Manage relationships, triage incoming information
- Processor: Execute searches, add IOCs to block/watch lists, create tickets for SOC
- Malware Analyst: Escalation for processor, analyze malware, produce malware reports

~~~~~~

- SOC: Conduct investigations when searches result in hits


~~~~~~

It isn’t only about consumption

- Contribute to intel community and share threat data – you might get something back that will assist your investigation
- Vendor relationships
- Takedowns
- Infection Notifications
- Law Enforcement

Next step …. Build/Buy a “TIP”

- Automated processing of indicator feeds from one or more of: IODEF, OpenIOC, STIX, etc and other commercial feeds in the future
- Ability to populate manually based on IOCs we collect from non-automated methods, plus internally generated intel, and then process
- All IOCs (manual & automated) will be tagged based on a number of criteria: targeted vs not, source of intel, confidence, sinkhole status, TLP, reputation, AV coverage, and many more -- ideally the system would automate the *entire* scoring process, including doing look-ups for reputation, AV coverage, etc.
- The tagging will combine to create a "score" which will determine the other activities to occur. e.g. Which SIEM lists to add IOC to, push to firewall block, how long to include in active block list (days, weeks, months, etc) then move to in-active, request BrightCloud recategorization, submit a request to email admins to delete a known-infected message from user inboxes, request email admins quarantine, etc.
- Maintain a searchable malware repository with complete indicators and analysis, ideally with a API to engage with FireEye

Enrichment, automation and depreciation

By-products of intel program can help in other ways

- Vendor introductions
- Informal Solution “References”
- Best Practices collaboration with others
- Awareness

Other takeaways

- Intel specific for targeted attacks aren’t likely to come from tactical threat information
- Be sure you have a reliable process to consume and leverage threat data before subscribing to a commercial threat feed
- Relationships are key!