Update on AbuseHelper

Christian Van Heurck - CERT.be
Agenda

• Description of the intended setup

• Lessons learned

• Our idea right now

• Discussions
Overview of the 1st installation: AH rules the world

- ShadowServer C&C
- CleanMX
- AbusIX
- Automatic Internal Feeds
- Manual Feeds
- 3rd party providers

Sources → Whois → Other experts → Reporting & Archiving

- CRM
- Cache
- Events Archive

RT-IR
Mail digests
...
Expected goals (1)

- Fully automated handling of automated reporting
  - Google AS information
  - SPAM reporting
  - C&C notifications
  - ...
- Fully automated time delimited sources
  - e.g. Rustock
Expected goals (2)

- Integrate (future) internal sources
  - IDS/IPS logs
  - HoneyPot
  - HoneySpider
  - Team Cymru
Main goal: let the bots do the work!

- Do all the repetitive job until the creation of the ticket
  - CSIRT only contacts the people
  - CSIRT safeguards manpower for added value tasks
- From a theoretical and technical point of view: it works!
But...

- We want:
  - 100% confidence that no information is lost
  - Full archive of all the incidents in a central place (how long?)
  - A place to query information for visualisation purposes
Some AbuseHelper issues

- Learning curve!
  - Learning AbuseHelper requires Python programming skills
    - The code is the documentation 😞
  - Flow centric architecture
    - How to handle unexpected custom queries?
  - « Too » new technologies
    - How will MangoDB, RIS, ... evolve (long term)?
Moving to a mix of technologies

- In AbuseHelper we trust!

- We want to try to mix well known and proven technologies with promising one (AH is promising)!

- We need to deliver something, taking too many risks at once might mean failure and end of funding 😞
New AbuseHelper layout

ShadowServer C&C
CleanMX
AbusIX
...
Automatic Internal Feeds
Manual Feeds

Sources → Whois → Other experts → Reporting & Archiving

3rd party providers

CRM → Cache → Short term archive
Long term archive

RT-IR

MyCERT portal (visualisation project)
Hierarchical events database

- Goals:
  - Persistent storage, reliability and monitoring of AbuseHelper
  - Easy of data manipulation for presentations purposes
  - Creating a database for research, own investigations and statistics
Database schema overview
Future: AbuseHelper

- AbuseHelper remains critical part:
  - Helps with input parsing
  - Screaming experts
  - Interface with RTIR (or ???)
  - Feeding database
  - -> plumbing (Enterprise Service Bus)
Future: database

- Database critical for:
  - Persistence for events in progress
    - recover from crash, possible non-realtime enrichment of events ...
  - Allowing statistics
    - trending, correlation, research
  - Long term archiving
    - research, legal requirements?
Future: visualization

- Database is needed for:
  - Non-realtime visualisation
  - Customized dashboards
  - Easy personalized customization
  - Allows personalized exports and/or API to data
  - Keystone for our « myCERT » project
Feedback  SEC-T (8-9 September 2011)

- RTIR has also cli-API (using REST-API)

- CERT-SE uses BGP routing table to match AP-ASN

- No IPv6 sources yet

- CERT-EE
  - setup S2S XMPP server - push and/or retrieve
  - « event hash » to identify duplicates?

- A lot of sources can be found on AH wiki + many bots
Feedback SEC-T

- Megatron will develop XMPP connector
- During session BGP-ranking expert bot developed
- WHOIS expert bot available
Questions, Answers and Discussions...

Thanks for your attention.

Feel free to contact us at david.durvaux@cert.be