Redesigning CERT.at’s incident handling capabilities – cherrypicking and learning from AH and Megatron

L. Aaron Kaplan
<kaplan@cert.at>
Disclaimer / Motivation

- I am not an AH expert
- I am not a Megatron expert

- But... neither are most of us ;-)
- We all need to improve our incident handling automation
- Discuss our ideas early, avoid working in parallel
THE PROBLEM
Categorization of incidents in 2011 (logscale)
Longterm trend (per month)
Current situation

• Bunch of Bash and Perl scripts, each connected to RTIR
• Batch oriented, confirm each batch (Press "y")
• Scripts pull in extra info (BGP table, ...)
• Wabuse: anything which needs visual eyeballing (websites, defacements, phishing, etc).

Wabuse is good and practical BTW

Source: AH workshop 2012, http://www.insourcess.com/Portals/1/graphics/jim%20blal...
Feeds

- At the moment we process mainly feeds from:
  - INTECO
  - AusCERT/CERT Australia
  - Shadowserver
  - Torpig/mebroot
  - Defacements (own), phishing (own), zone-h

- No good trending / statistics capabilities

- How will this scale in the future with more feeds?

2012/01/24
Requirements

• ContactDBs <-> IR automation process
• Automate as much as possible
• Uniform processing of mass-log events
• Integration with RTIR: mail sending via RTIR
• New feeds must be included quickly
• Have database for statistics
• Limit number of outgoing mails per org
• Standardized output format (XARF, ...)
• Include feedback loop for report recipient (helpful: yes/no)
• Support VIP customers
BTW nice idea: contacts.cert.at

CERT.at geolocate the national CERT abuse service

Version: 0.6
IP-Addresses:
6.6.6.6

☑ show the national CERT contact ☑ show header ☐ be verbose
Output-seperator:
☑ TAB ☐ ; ☐ ,

Submit

Syntax for accessing the data directly via HTTP

HTTP GET: https://contacts.cert.at/cgi-bin/abuse-nationalcert.pl?ip=1.2.3.4
HTTP POST: https://contacts.cert.at/cgi-bin/abuse-nationalcert.pl

Options:
- sbhowNationalCERT=on: Show national CERT contact info
- sbhowHeader=on: Display a CSV header
- sbVerbose=on: Display the source of the data, and other infos
- isep=(TAB, comma, semicolon, pipe): Separator for the (output) CSV format
First iteration: lumberjack

• Tables:
  – Logrecord
  – Report
  – Report_types

• ... But then we decided to look what other teams already did
Existing solutions: AH

- Well known in the TF-CSIRT community
- ++Lots of effort, buy-in from community
- ++Unix philosophy: lots of small bots
- -- Nevertheless: only a framework
- -- Sometimes hard to debug (very parallel)
- -- no concept of „data owner“
- We need to switch from Perl to Python. Ok...
- ++possibility for federation
- AH workshop in Helsinki 2012
- Result: quick wins are possible, integration doable
AH architecture

• „Botnet“ of small python scripts. Each is like a small unix tool
• „Graph of unix pipes“ is realized via XMPP (jabber, chat)
• Bots take something out of chat room and put it into other chat rooms
• Bots can filter, enrich data („scraming experts“) or export data (i.e. send mail via RTIR)
Existing solution: Megatron

- From CERT.se
- ++ successfully used in production
- ++ Very clean, well planned, very complete
- Java based
- ++ DB and Batch-driven
- ++ concept of „data-owner“
- monolithic
- -- slow (?) Need to understand Java frameworks
- -- we did not see large community buy-in
Synthesis: AH + DB

• Idea:
  – Add contactDB to AH (design finished)
  – Add eventlog DB: stores logrecords ➔ gives us statistics
  – Improve AH’s batch capabilities
  – Eventlog DB is also a „data owner“ ➔ restarting jobs is doable
Synthesis (2)

• XMPP component for Megatron? Connect the two systems?

• Formed a small team so far:
  – CERT.at (Aaron, Stefan Lenzhofer)
  – CERT.be (David, Erik)

Regular conf calls, progress reports, hackathons

And what about YOU?
Collaboration

- Regular Hackathons
- Staff exchange (a.k.a. a hackathon for a week)
- Feedback loops amongst CERTs for feed data quality
- contactDB: request for TI (and FIRST): enhance TI DB so that we can export it into our respective contactDBs (ASNs, CIDRs, domain-suffixes)
- Standardization + documentation ! (⇒ helps new teams)
- If I saved 5 minutes of your time each day, then that‘s a lot of time in total
LET’S GET THIS ROLLING!