security is not an island
HILTON MALTA

FIRST Conference
MALTA
17 - 22 June 2012

FIRST
Improving Security Together
FROM ZERO TO CERT IN 60 DAYS
IN 35 MINUTES
SINDRI BJARNASON, CERT-IS
In August 2011, a three man team was given the task of establishing a national CERT in Iceland ... Pressed for time and under severe budgetary constraints, they pressed on towards this goal ... This is their story ...
• The team operates as a branch of the Icelandic Post and Telecommunication Administration (Telco Regulatory Authority)

• Legislation “enacted” in spring 2012 as an addendum to the local telecommunication act

• Icelandic Telecommunication companies form the initial constituency (along with picking up the tab)

• Constituency expansion scheduled for Q4 2012
• This talk is intended to address some of the key challenges likely to emerge during the founding of a CERT team (a national CERT in particular) using CERT-IS as a frame of reference.

• We will cover the 60 day period that followed our initial implementation and focus on the pivotal role AbuseHelper played during the founding process.
We made a lot of mistakes along the way, the details of the more severe ones will appear in this box.

Observations made with the benefit of hindsight will appear in this box.

Lessons learnt: We made a lot of mistakes along the way, the details of the more severe ones will appear in this box.
THE DIGITAL LANDSCAPE

FROM ZERO TO CERT IN 60 DAYS

Networked nation, high availability for Internet connectivity

Network security getting more exposure by the media

Increased pressure at the government level to address public system security

PRIVATE SECTOR

TELECOMMUNICATIONS

WEP INSECURITIES

IT SERVICES

FINANCE

MALWARE ATTACKS

GAMING INDUSTRY

DDOS

SERVICE HOSTING

STARTUP FIRMS

RESEARCH

EDUCATIONAL SECTOR

UNIVERSITY NETWORKS

PUBLIC SECTOR

FUNDING

SCADA

ENERGY

SECURITY CONCERNS

PTA

WE ARE HERE!!
Late September 2011, we find ourselves facing an existential dilemma!

The increased number of abandoned projects hints at a general lack of direction

CERT-IS was being designed as a ready-to-run product

This period can be called the “savior complex”-era. It is not until we left our own egos at the door that actual progress was made.
IS IT AN ECOSYSTEM?

FROM ZERO TO CERT IN 60 DAYS

we are here

Observations of recent infosec-related processes
The relationship between our CERT team and that of our constituency is symbiotic, to be sustainable it must be mutually beneficial.

IT IS AN ECOSYSTEM

- Within there is a continuous cycle of evolution in response to security threats.
- Opportunities for quick integration, i.e. easy visibility, tend to reside near reactive events as opposed to proactive ones.
- By ignoring the importance for integration, we were making our team success dependent on our own expertise.

The relationship between our CERT team and that of our constituency is symbiotic, to be sustainable it must be mutually beneficial.
THE NEW DIRECTION

- We made the decision to become useful!
- Less “educated guesses”, more “concrete requirements”
- New motto: “maximum utility, minimum effort”
- Collaboration a priority

FROM ZERO TO CERT IN 60 DAYS

We made the mistake of approaching collaboration formally at first, which is suboptimal until your team becomes “established”
Once we went utility-oriented, the necessity for data became obvious.

“Situational awareness” the concept formerly known as “we could really do with some data”

Data acquisition and processing is an easy thing to get wrong, especially in “exploratory” fashion.

The importance of data acquisition and the impact it had on our development as a team was not obvious at the start.
“AbuseHelper is a modular and (hopefully) scalable and robust framework to help you in your abuse handling”

Our team force multiplier

Data acquisition framework that happens to be tuned towards incident handling

Standard and reusable components

Under active development
FAMILIAR MODEL
FROM ZERO TO CERT IN 60 DAYS

DATASOURCE
DATASET

SORT
FILTER

UPDATE

PULL

PARSE

PUSH

FEED SOURCE
FEED BOT

SANITIZE
VALIDATE

REPORT
POPULATE

FUNCTIONAL VIEW

we are here

0 10 20 30 40 50 60
THE 60 DAY PROGRAM

FROM ZERO TO CERT IN 60 DAYS

DATA ACQUISITION
available sources
prioritization
evaluation

DATA PROCESSING
the generic event
value adding processes
extensions

DATA MARKETING
presentation
constituency collaboration
examples

we are here
AbuseHelper has built-in support for most transport types (www, RSS, xml, ...)

Community aspect of AbuseHelper has real value

Extensive list for available sources can be found as part of their AbuseHelper Wiki site (“feeds”)

Useful reference for any CERT team
STEP 1.1: EVALUATION

FROM ZERO TO CERT IN 60 DAYS

Feed list \[\rightarrow\] access type \[\rightarrow\] availability

PUBLIC
- abuse-ch
- D-Shield
- clean-mx
- zone-h
- dragonssh
- phishtank
- Project Honeypot
- ... (we are here)

RESTRICTED
- Arbor Networks
- Shadow Server
- Team Cymru
- ... (we are here)

NOT AVAILABLE
- Microsoft SNDS
- Google
- ...
STEP 1.2: QUALITY CONTROL

FROM ZERO TO CERT IN 60 DAYS
STEP 2: DATA PROCESSING

FROM ZERO TO CERT IN 60 DAYS

- Integration of known sources is trivial*
- *processing the data is the next challenge
- AbuseHelper (by design) ships with limited processing capabilities
- The quality of the data processing implementation becomes a governing factor for future expansions, take care of your data at this point

we are here
STEP 2.1: DEFAULT BEHAVIOR

FROM ZERO TO CERT IN 60 DAYS

We are here
STEP 2.2: EXTENSIONS

FROM ZERO TO CERT IN 60 DAYS

• Was there a need to extend AbuseHelper?
  • The distribution of events is heavily clustered
  • Sending reports is not an optimal form of introduction
  • Each event carries limited information
  • Opportunity for collaboration with the constituency
STEP 2.2: EXTENSIONS

FROM ZERO TO CERT IN 60 DAYS

Properties
- source
- description
- ip

Normalization
- classification
- naming convention

Increased Report Accuracy
- Event Score Assignment
- Detailed Description

Expansions
- CIDR block

CIDR Block View
- Report Prioritization

Tracking
- ip ttl frame

Persistence Value
- Visibility Value

we are here
STEP 2.2.1: EXTENSIONS

FROM ZERO TO CERT IN 60 DAYS

Requirements:
- Increased Report Accuracy
- Event Score Assignment
- Detailed Description
- CIDR Block View
- Report Prioritization
- Persistence Value
- Visibility Value

Utility:
- Consistent Naming Convention
- Event Class Prioritization
- Informative Reporting
- Generate CIDR Reports
- CIDR Priority Level
- Identify Residual Problems
- Per-IP Tracker with TTL

we are here
DAY 60: EVALUATION

- Automated reports (generated daily/weekly)
  - Situational awareness for our team
  - Tool for our constituency: getting familiar with the types of problem; the impact on their networks and estimated workload
  - Identification of emerging problems as well as residual ones
STEP \( n \): DATA MARKETING

Data Marketing Examples

FROM ZERO TO CERT IN 60 DAYS
CERT-IS: THE BIG LESSONS

- Commit early to your data acquisition, ensure your infrastructure has the capacity to support and maintain such processing
- Do not isolate your team, make networking an early priority
- Get your constituency involved in the data processing step
- Consider AbuseHelper to be a continuous effort
FROM ZERO TO CERT IN 60 DAYS

CERT-IS: OUR TIMELINE

The past 10 months
QUESTIONS?

FROM ZERO TO CERT IN 60 DAYS
ClarifiedNetworks:
https://www.clarifiednetworks.com/

AbuseHelper:
https://bitbucket.org/clarifiednetworks/abusehelper/

AbuseHelper Installation:
https://bitbucket.org/clarifiednetworks/abusehelper/wiki/INSTALL

AbuseHelper Extension Package:
#TBA#

CERT-IS:
cert@cert.is ; sindri.bjarnason@cert.is