“Knowledge is power. Knowledge shared is power multiplied.”

Robert Noyce
About CERT.be and us

CERT.be
The federal cyber emergency team

a service of Fedict
operated by Belnet
Agenda

1. Current situation
2. Proposal for a new model for sharing
3. New issues
4. Sharing time = Q&A
Propagation time

- **Internet delay:** milliseconds

![Terminal output]

```
Terminal — bash — 69x31
Last login: Fri May 18 15:34:20 on ttys001
You have mail.
Christian-Van-Heurck-MacBook-Pro:~ christian$ ping cert.be
PING cert.be (193.190.198.61): 56 data bytes
64 bytes from 193.190.198.61: icmp_seq=0 ttl=56 time=15.555 ms
64 bytes from 193.190.198.61: icmp_seq=1 ttl=56 time=15.219 ms
64 bytes from 193.190.198.61: icmp_seq=2 ttl=56 time=14.995 ms
^C
--- cert.be ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 14.995/15.256/15.555/0.230 ms

Christian-Van-Heurck-MacBook-Pro:~ christian$ ping cert.at
PING cert.at (83.136.33.148): 56 data bytes
64 bytes from 83.136.33.148: icmp_seq=0 ttl=48 time=54.930 ms
64 bytes from 83.136.33.148: icmp_seq=1 ttl=48 time=53.603 ms
64 bytes from 83.136.33.148: icmp_seq=2 ttl=48 time=54.256 ms
^C
--- cert.at ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 53.603/54.263/54.930/0.542 ms

Christian-Van-Heurck-MacBook-Pro:~ christian$ ping first.org
PING first.org (72.3.219.184): 56 data bytes
64 bytes from 72.3.219.184: icmp_seq=0 ttl=40 time=125.394 ms
64 bytes from 72.3.219.184: icmp_seq=1 ttl=40 time=124.970 ms
64 bytes from 72.3.219.184: icmp_seq=2 ttl=40 time=124.729 ms
^C
--- first.org ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 124.729/125.083/125.394/0.275 ms
Christian-Van-Heurck-MacBook-Pro:~ christian$ 
```
Propagations time: milliseconds

- SOURCE of incident
- FEED provider
- Internet
- XMPP / X-ARF / ...

Proposal for a new model for information sharing between CSIRTs
Propagating time: days to weeks

- **SOURCE of incident**: suspicious system
- **FEED provider**: EVENT DB, sensors
- **Internet**
- **Email**
- **CSIRT**: human, mail system

Proposal for a new model for information sharing between CSIRTs
Propagation time: back to milliseconds

Proposal for a new model for information sharing between CSIRTs
Propagation time: back to seconds

We need to **SHARE**

more efficiently!
1 Current situation
Information overflow

• Numerous valuable sources
  • remote
  • local
  • near real-time

• Processing all the data
  • how: scripting?
  • what to treat?
Lack of large-scale overview
Contact point issues

Whom
Criminals are organised and DO share
CSIRTs are like islands
Legal issues

• Allowed?

• What?

• With whom?

• How?
Political issues

Voici l’arme de la FN que portait Kadafi

HUGUES DORZEE, DAMIEN SPIELTER AND ALAIN LALLEMAND

Le dictateur déchaîné, capturé puis tué ce jeudi près de la ville de Syrte, avait en sa possession une arme droite fabriquée en Belgique.

Le pistolet dont le combatant rebelle Mohammed al-Behi (nom du nom) dans les airs est formé personnellement du colonel Kadafi, mort hier dans des circonstances encore floues, après avoir été capturé près de la ville de Syrte.

24th annual FIRST conference
Malta, 17-22 June 2012
Proposal for a new model for information sharing between CSIRTs
Technical issues
Proposal for a new model for sharing

Proposal for a new model for information sharing between CSIRTs
Connecting our islands efficiently

Proposal for a new model for information sharing between CSIRTs
Creating archipelagoes

- European Union .eu
  - 27 countries already sharing
  - Why not on incidents?
Creating archipelagoes

- Benelux .be .nl .lu
- 3 countries sharing since 1944
- EU sub archipelago
Creating archipelagoes

- Belgium .be
  - CERT.be proxy
  - Febelfin
  - Sectorial CSIRTs
  - ISP’s
  - Law Enforcement
Seeds for archipelagoes

• Geo-political decisions / history

• Existing organizations
  • FIRST
  • TF-CSIRT
  • ENISA
  • National / governmental CSIRTs

• Fighting a common issue
  • DCWG.org

• Anything that pushes countries to collaborate!

• Requires **TRUST**!
Proposal for a new model for information sharing between CSIRTs

Decision tree

- Event
- Legal?
  - yes
  - Political Support?
    - yes
    - Need to Know?
      - yes
      - Too Sensitive?
        - yes
        - Filter
        - no
      - no
    - no
  - no
- no
- Don’t Share
- Share
Routing model: top-down

- Event
  - Archipelago
    - Sub Archipelago
      - Sub Sub Archipelago
        - Concerned Constituent
Security is no longer an island!

[Diagram showing various islands and archipelagos connected with arrows, illustrating information sharing between CSIRTs.]
How can we share?

Island A

Jabber S2S Only

events

Island B

Jabber S2S Only

Island C

Jabber S2S Only

Proposal for a new model for information sharing between CSIRTs
What can we share?

- **Events**
  - IP’s (src & dst) - Ports - Protocols
  - URL’s

- **Binaries and/or hashes of**
  - malware
  - suspicious files

- **Information on domains, IP’s, AS’s**
  - owner
  - history (passive DNS)

- **Binary answer to a question (yes/no)**
  - have you seen that IP before?

- **Contacts**
Tools already exist ... for years!

- Phone
- mail
- chat
- FTP
- scripts
- AbuseHelper
- Megatron
- fordrop
AbuseHelper: the collaborative agents
Megatron: the central vacuum cleaner
fordrop: human collaboration
New issues
Correlated events: rating & feedback

- Source A
  - Event A
- Source B
  - Event B
- Processing
  - Correlated Events
- Concerned Constituent

- Rating of event based on
  - Correlation with other sources (including internal ones)
  - Feedback report (quality of events)
  - "+1" button
4 Conclusion
You can share too

Please SHARE and help us do that EFFICIENTLY
You are in good company

- cert-fi autoreporter
- Clarified Networks
- CERT.at
- CERT.be
- CERT.EE
- NORDUnet
- CIRCL
- SURF
- CERT.EU
- CERT.IE
- CERT.is
- CERT.LV
- Nationaal Cyber Security Centrum

Proposal for a new model for information sharing between CSIRTs
Sharing time!

Please

SHARE

and help us do that

EFFICIENTLY

david@cert.be
christian@cert.be