Government Computer Emergency Response Team The Netherlands
Monitoring threats and vulnerabilities

Taranis
Monitoring threats & vulnerabilities (1)

- 12x7 active duty
- 24x7 available for handling ICT security incidents
- Monitoring of open and closed sources
  - Websites
  - Honey pots
  - Other CERT's
  - Mailing lists
  - IRC
- Handle reports send to cert@govcert.nl
Monitoring threats & vulnerabilities (2)

Writing security advisories for our constituency (government)

Writing a weekly overview of security news (‘End-of-Week’)

Alerting citizens and small business through Waarschuwingdienst.nl

Informing colleagues through an internal mailing list

Weekly circulation (9 persons)
The monitoring process

Collect  Assess  Analyze  Write  Publish
The monitoring process

Collect
Assess
Analyze
Write
Publish
Taranis principles

• Integration of all phases into one tool
• Minimal ‘copy-and-paste’ actions
• Higher efficiency, lower error rates
• Use of templates for standard texts
• Taranis as the source for advisories, alerts and End-of-Weeks
• Modular composition
• Sharing with the community
• Traceability of actions
Taranis

UI / Authorization Framework

Collect  Assess  Analyze  Write  Publish

CVE, CPE

Phishing checker
WHOIS
mod_tools

HTTP(S)
POP3
IMAP

End-of-Week
Alert
Alert
Alert
Advisory
Dear abuse,

On behalf of GOVCERT.NL, I would like to request your assistance. GOVCERT.NL is the Computer Emergency Response Team for the Dutch Government.

We have received a report of phishing activity against a large Dutch bank. The phishing site is located at hXXp:// Details of the phishing website:

URL:

hXXp:// /home2.php
(link modified for security reasons)

This web address resolves to .6, for which you are listed as the abuse contact.

WHOIS:

A5 | IP | CC | AS Name
10297 | .6 | US |

We kindly ask you to investigate this matter and to take appropriate action. Any feedback of your actions is highly appreciated. Many thanks in advance for your help.

Kind regards,
Demo
How to obtain the software?

• Sent e-mail to info@govcert.nl

• Sign the Gentleman’s Agreement you will receive in return

• After signing you will receive a Software CD and manual
More information?

- contact info@govcert.nl
- Check our website:
  http://www.govcert.nl/render.html?it=210

Taranis Workshop organized 17th November (after our symposium)
=> Hands-on class + a change to meet with the developers
Thank you for your time!

Questions?