Proactive Detection of Network Security Incidents – A Study

Andrea Dufkova (ENISA)
Piotr Kijewski (CERT Polska/NASK)

FIRST 2012 Conference
21st June 2012, Malta
OUR TALK TODAY ...

i. Links with ENISA work
ii. Facts about the study
iii. Dive into the research findings
iv. Impact of the study in Poland
v. Open questions
vi. Recommendations
ENISA CERT relations/operational security – focus in 2012 - studies

- Definition of baseline capabilities of national and governmental CERTs
- Training and exercises
- Cybercrime prevention
- Information sharing and alerting
- Early warning
Some Facts

- Project ran for ½ year
- Study published in December 2011

... 133 pages to read, but...

- Inventory of services/tools and mechanisms (pages 27-98)
- 16 shortcomings – pages 108 - 127
- 35 recommendations - pages 128-132
- Where to get the study:

Problem definition

★ Reactive approach
  ★ Wait for incoming incident reports (internal/external)

vs

★ Proactive approach
  ★ Actively look for incidents taking place
    • Subscribe to external services informing about problems
    • Deploy internal monitoring tools / mechanisms

★ Provide a sort of ‘Early warning’ service from the constituent’s (client’s) perspective
Objectives

- Inventory of available methods, activities and information sources for proactive detection of network security incidents

- Identify good practice and recommended measures

- What needs to be done to improve and by whom
Target audience

- National / governmental and other CERTs
- Abuse teams
- Data providers

new or already established ....
Approach

**Authors of the study – ENISA experts and CERT Polska / NASK (contractor)**

**Main steps:**

- Desktop research
- **Survey among CERTs (>100 invitations, 45 responses)**
- Analysis
- **Expert group (active survey participants, other experts)**
  - Meeting
  - Mailing list
Survey

Respondent profile

- Government/public administration: 33%
- Academic: 12%
- ISP: 14%
- Other (please specify): 2%
- Commercial Company: 7%
- Financial: 32%
Survey

How do you feel with the incident information sources you currently have?

- **4%** We are fully satisfied with information sources we currently have
- **47%** We would consider to try other sources to improve
- **49%** We feel information deficit in general – we think there are significantly more incidents we do not know about
- **4%** We feel we have too many information sources
Survey

What you would like to improve?

- Accuracy
- Coverage
- Timeliness
- Ease of use
- Resources required

Number of responses

- Accuracy: 15
- Coverage: 13
- Timeliness: 11
- Ease of use: 6
- Resources required: 5
Survey

How do you obtain incident related data about your constituency?

- Internal monitoring
- Monitoring of external sources
- Monitoring of commercial sources
- Monitoring of closed sources
- Incoming Incident Reports (reactive)

Number of responses

- Primary source
- Auxiliary source
- Not used
We do process all incoming information, but only higher priority incidents are further handled, more input information would leave even more lower priority incidents without attention.

We can fully handle current amount of incident information. We could handle even more incident information.

We can fully handle current amount of incident information, but would not be able to handle more.

We cannot properly handle even the amount of incident related information currently available.
Survey
External sources of information

Rates for timeliness, accuracy of results, ease of use, coverage and resources required are all summed up.
Survey
CERTs that use most popular source (Shadowserver)

40%
Survey

External sources of information

Do you use any closed sources of information you cannot disclose?

- Yes: 61%
- No: 39%
Survey

Internal tools used

- Firewalls
- System logs
- AV
- Netflow
- IDS/IPS
- Router logs
- Server honeypot
- App logs
- Proxy logs
- Darknet
- Database logs
- Spamtrap
- Sandboxes
- Web Application Firewalls
- Passive DNS monitoring
- Client honeypot

No answer
I never used it and will not use it.
I used it in the past, but dropped it.
I don't use it but plan to use it in future.
I use it
Survey

Do you collect data about other constituencies?

- 45% yes
- 43% no
- 7% cannot tell
- 5% not sure
Survey
Do you share this information?

- Yes: 52%
- No: 48%
Survey

Under what rules do you share?

- Limited access: 56%
- Anyone (public): 15%
- Commercial: 7%
- Public subscription based: 18%
- Other: 4%
Survey
CERTs that collect info about others and share

23,4%
Survey

Do you correlate?

Yes 80%

No 20%
Survey

how do you correlate information from multiple sources

- Adhoc: 56%
- Automated system: 26%
- Adhoc and automated system: 18%
Survey
CERTs that automate the correlation process in any way

35,2%
Analysis

★ Evaluation criteria:

★ Timeliness
★ Accuracy
★ Ease of use
★ Coverage
★ Resources required
★ Scalability (for internal tools)
★ Extensibility (for internal tools)

★ Significant degree of subjectiveness present
(expert judgment, survey responses, workgroup expert opinions)
## Summary of external sources

<table>
<thead>
<tr>
<th>Service</th>
<th>Timeliness</th>
<th>Accuracy of results</th>
<th>Ease of use</th>
<th>Coverage</th>
<th>Resources required</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS-BH Malware Domain Blocklist</td>
<td>Fair</td>
<td>Good</td>
<td>Excellent</td>
<td>Excellent</td>
<td>Excellent</td>
</tr>
<tr>
<td>MalwareURL</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
<td>Excellent</td>
<td>Excellent</td>
</tr>
<tr>
<td>DSHIELD</td>
<td>Excellent</td>
<td>Fair</td>
<td>Good</td>
<td>Excellent</td>
<td>Excellent</td>
</tr>
<tr>
<td>Google Safe Browsing Alerts</td>
<td>Good</td>
<td>Fair</td>
<td>Good</td>
<td>Excellent</td>
<td>Good</td>
</tr>
<tr>
<td>HoneySpider Network (as a service)</td>
<td>Excellent</td>
<td>Fair</td>
<td>Good</td>
<td>Fair</td>
<td>Excellent</td>
</tr>
<tr>
<td>AusCERT</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
</tr>
<tr>
<td>Cert.br data feed</td>
<td>Good</td>
<td>Good</td>
<td>Fair</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>FIRE</td>
<td>Good</td>
<td>Good</td>
<td>Fair</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Team Cymru - TC Console</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
<td>Excellent</td>
</tr>
<tr>
<td>EXPOSURE</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
<td>Good</td>
<td>Excellent</td>
</tr>
<tr>
<td>AmaDa</td>
<td>Excellent</td>
<td>Good</td>
<td>Excellent</td>
<td>Fair</td>
<td>Excellent</td>
</tr>
<tr>
<td>Malware Domain List</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
</tr>
<tr>
<td>Zeus/SpyEye Tracker</td>
<td>Good</td>
<td>Excellent</td>
<td>Excellent</td>
<td>Fair/Good</td>
<td>Excellent</td>
</tr>
<tr>
<td>The Spamhaus Project Datafeed</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
</tr>
<tr>
<td>Shadowserver Foundation</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>SGNET</td>
<td>Good</td>
<td>Excellent</td>
<td>Good</td>
<td>Fair</td>
<td>Good</td>
</tr>
<tr>
<td>ARAKIS</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
<td>Good</td>
<td>Excellent</td>
</tr>
<tr>
<td>Malc0de database</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
<td>N/A</td>
<td>Excellent</td>
</tr>
<tr>
<td>ParetoLogic URL Clearing House</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
<td>N/A</td>
<td>Good</td>
</tr>
<tr>
<td>SpamCop</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
<td>Good</td>
</tr>
<tr>
<td>Arbor ATLAS</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
<td>Good</td>
<td>Excellent</td>
</tr>
<tr>
<td>CBL (Composite Blocking List)</td>
<td>Excellent</td>
<td>Excellent</td>
<td>Fair/Good</td>
<td>Good</td>
<td>Excellent</td>
</tr>
<tr>
<td>Cert.br Spampots</td>
<td>Excellent</td>
<td>N/A</td>
<td>Good</td>
<td>Fair</td>
<td>Fair</td>
</tr>
<tr>
<td>Team Cymru’s CAP</td>
<td>Good</td>
<td>Excellent</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Project Honeypot</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
<td>Good</td>
<td>Excellent</td>
</tr>
<tr>
<td>Malware Threat Center</td>
<td>Good</td>
<td>Fair</td>
<td>Excellent</td>
<td>Fair</td>
<td>Good</td>
</tr>
<tr>
<td>Smart Network Data Services</td>
<td>Good</td>
<td>Good</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Malware Patrol</td>
<td>Excellent</td>
<td>N/A</td>
<td>Excellent</td>
<td>N/A</td>
<td>Excellent</td>
</tr>
<tr>
<td>Zone-H</td>
<td>Excellent</td>
<td>Excellent</td>
<td>Good</td>
<td>N/A</td>
<td>Fair/Excellent</td>
</tr>
<tr>
<td>Cisco IronPort SenderBase</td>
<td>Excellent</td>
<td>Good/Excellent</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
</tr>
</tbody>
</table>
Top 5 recommended external sources

- Shadowserver foundation
  (http://www.shadowserver.org)

- Zeus/SpyEye Tracker

- Google Safe Browsing Alerts
  (http://safebrowsingalerts.googlelabs.com)

- Malware Domain List
  (http://www.malwaredomainlist.com/)

- Team Cymru's CSIRT Assistance Program
  (http://www.team-cymru.org/Services/CAP/)
## Summary of internal tools

<table>
<thead>
<tr>
<th>Category</th>
<th>Timeliness</th>
<th>Accuracy of results</th>
<th>Ease of use</th>
<th>Coverage</th>
<th>Resources required</th>
<th>Scalability</th>
<th>Extensibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client honeypot</td>
<td>Excellent</td>
<td>Fair-Excellent</td>
<td>Fair/ Good</td>
<td>Fair/ Good</td>
<td>Good</td>
<td>Excellent</td>
<td>Fair</td>
</tr>
<tr>
<td>Server honeypot</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Firewalls</td>
<td>Excellent</td>
<td>Fair</td>
<td>Good</td>
<td>Fair/ Good</td>
<td>Good</td>
<td>Excellent</td>
<td>Fair- Excellent</td>
</tr>
<tr>
<td>IDS/IPS</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
<td>Fair- Excellent</td>
<td>Fair/ Good</td>
<td>Good</td>
<td>Fair- Excellent</td>
</tr>
<tr>
<td>Netflow</td>
<td>Excellent</td>
<td>Good</td>
<td>Fair</td>
<td>Fair/Good</td>
<td>Fair</td>
<td>Good/ Excellent</td>
<td>Good</td>
</tr>
<tr>
<td>Sandboxes</td>
<td>Excellent</td>
<td>Fair/ Good</td>
<td>Fair</td>
<td>N/A</td>
<td>Fair</td>
<td>Fai- Excellent</td>
<td>Fair- Excellent</td>
</tr>
<tr>
<td>Darknet</td>
<td>Excellent</td>
<td>Good</td>
<td>Fair</td>
<td>Fair- Excellent</td>
<td>Fair</td>
<td>Good</td>
<td>Fair</td>
</tr>
<tr>
<td>Passive DNS monitoring</td>
<td>Excellent</td>
<td>Good/ Excellent</td>
<td>Good</td>
<td>Fair/ Good</td>
<td>Good</td>
<td>Good/ Excellent</td>
<td>Fair</td>
</tr>
<tr>
<td>Spamtrap</td>
<td>Excellent</td>
<td>Fair/ Good</td>
<td>Fair</td>
<td>Fair</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Web Application Firewalls</td>
<td>Excellent</td>
<td>Good/ Excellent</td>
<td>Fair</td>
<td>Fair</td>
<td>Fair</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>App logs</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Excellent</td>
<td>Good</td>
<td>Good</td>
<td>Fair- Excellent</td>
<td>Good</td>
<td>Good</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Recommended tools

Tools divided in 3 groups

★ Standard
★ Often by design part of network and available for use by CERTs
★ Examples: routers, firewalls, antivirus systems, IDS/IPS systems, netflow and various kinds of logs

★ Advanced
★ Beyond the standard networking tools. Additional resources may be required
★ Examples: darknets, server honeypots, spamtraps and networks of sensors

★ Upcoming
★ Even more resources and skills needed.
★ Examples: client honeypots, sandboxes, passive DNS analysis techniques
Study impact

What changed for CERT Polska?

Incidents for Poland: 2011

- Bots: 9,887,006
- Scanning: 5,703,211
- Spam: 4,677,560
- Open DNS Servers: 581,428
- Malicious URLs: 179,752
- Brute force: 159,687
- C&C: 2,263
- Phishing: 2,145
- Data from Sandboxes: 2,119
- Fast-flux: 757
- DDOS: 16
- Others: 14,564
Tools for correlation & sharing

- Abuse Helper (http://www.abusehelper.be/)
- Megatron (contact SITIC/CERT.se)
- Collective Intelligence Framework (http://code.google.com/p/collective-intelligence-framework/)
- n6 by CERT Polska (currently in beta)
n6 PLATFORM

Security Data
- URLs
- Domains
- IPs
- Malware
- Credentials

n6 ENGINE

HTTPS

ISPs
CSPs
CERTs
Banks

files by SMTP
files by HTTP
What we share

Aggregated sources:
- our systems (ARAKIS, HSN, internal tools ...)
- external organizations - major data providers covered in this report & closed ones

<table>
<thead>
<tr>
<th>Types of data</th>
</tr>
</thead>
<tbody>
<tr>
<td>malicious URLs</td>
</tr>
<tr>
<td>malicious artifacts</td>
</tr>
<tr>
<td>infected hosts (bots)</td>
</tr>
<tr>
<td>scanning</td>
</tr>
<tr>
<td>C&amp;C servers</td>
</tr>
<tr>
<td>DDoS</td>
</tr>
<tr>
<td>brute force</td>
</tr>
<tr>
<td>fast flux</td>
</tr>
<tr>
<td>phishing</td>
</tr>
</tbody>
</table>

www.enisa.europa.eu
Some open questions ...

★ Why are CERTs not interested in obtaining free information about problems in their constituency?
★ Why are CERTs not interested in sharing data?
★ Why do CERTs not deploy tools for automated sharing of incidents?
Recommendations for improvements

Data providers

★ Identification and vetting of data consumers
  ★ Establish contacts with relevant communities
  ★ Do screening of data recipients
  ★ Easy process of registration

★ Data format and distribution
  ★ Adapt existing standards and methods whenever possible
  ★ Provide complementary data usable for correlation (e.g., timestamps, incident type)
  ★ Provide data timely
  ★ Provide description on how the data is obtained

★ Data quality enrichment
  ★ Filter, correlate, verify to reduce false positives
  ★ Provide feedback mechanisms
  ★ Implement and explain principles of data aging and removal
  ★ Assign confidence levels to data
  ★ Keep aggregated data to analyse trends and patterns, enrich data with statistical information
Recommendations for improvements

Data consumers

★ Acquire access to datasets
  ★ Review and consider usage of sources, tools recommended here
  ★ Develop own monitoring capabilities
  ★ Establish relationships with relevant communities (eg, FIRST, TF-CSIRT)
  ★ Consider what data can be shared with others

★ Integrate external data feeds with incident handling systems
  ★ Try to be flexible and prepared to handle different formats
  ★ Store data in a way which would help to provide correlation, analysis, visualisation
  ★ Correlate, verify with data from internal monitoring systems

★ Verify quality of data feeds
  ★ Correlate, filter, enrich data; group related incident reports
  ★ Give feedback to data providers

★ When possible improve internal monitoring capabilities possibly becoming data provider
  ★ More you are ready to give – more you can expect to get back
Recommendations for improvements

EU and national level

★ Facilitate wider usage of underused technologies

★ Encourage the adoption of common standards for the exchange of incident information

★ Integrate wide scale statistical incident data
  ★ perform long term analysis and correlation
  ★ produce reports, research materials, advisories and predictions

★ How to improve reporting of data leaks to victims?

★ How to reach the balance between privacy protection and security provision needs?
European Network and Information Security Agency (ENISA)
Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece
cert-relations@enisa.europa.eu

CERT Polska/NASK
ul. Wąwozowa 18, 02-796
Warsaw, Poland
n6@cert.pl

REPORT: