CERT for the EU institutions, bodies and agencies

• Pre-configuration team
• 60+ clients
• Resources made available by the clients
• Operational support
• Off-line
• Collaboration with internal ITsec teams
• Single point of contact
• European Digital Agenda
Clients
Partners
Office layout, walls, doors, carpet, painting
Furniture
Sunshield, sunblinds
Fridge, microwave
Security doors, security locks
Intrusion detection, alarm, Videophone
Fire- and waterproof safe
Server room, airco, fire extinction, UPS
High speed direct internet connection
Servers, routers, firewalls, switches
Isolated local area network
Desktop computers, printers
Office automation software, email system
Help desk
Temporary server to host webportal
Photocopy, scanner, shredder
Beamer, projection screen
Videoconferencing
Functional mailbox, phone and smartphone
Recruitments (AD, END)
Service passes, SYSPER
Mission and training budget
Small procurement budget
Business cards
EUROPA page, guide des services
Webportal EMM, sources, keywords
Logo and graphical image
PGP, ACID, CHIASMUS, SECEM
Domain name
Name registration
Created 1/6/2011

- 10/5: go ahead
- 13/5: recruitment interviews
- 20/5: premises made available
- 14/6: revamping of offices finished
- 14/6: furniture and office computers installed
- July: design web portal
- July: client survey
- July-September: meetings with 15 CERTs
- August: construction of server room
- August: design of graphical identity
- 15/8 and 1/9 arrival of new staff
- 15/9: installation of servers
- 20/9: dry run of web portal
- 22/9: official inauguration
<table>
<thead>
<tr>
<th>Reactive Services</th>
<th>Proactive Services</th>
<th>Artifact Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts and Warnings</td>
<td>Announcements</td>
<td>Artifact analysis</td>
</tr>
<tr>
<td>Incident Handling</td>
<td>Technology Watch</td>
<td>Artifact response</td>
</tr>
<tr>
<td>Incident analysis</td>
<td>Security Audits or Assessments</td>
<td>Artifact response coordination</td>
</tr>
<tr>
<td>Incident response support</td>
<td>Configuration and Maintenance of Security</td>
<td></td>
</tr>
<tr>
<td>Incident response coordination</td>
<td>Development of Security Tools</td>
<td></td>
</tr>
<tr>
<td>Incident response on site</td>
<td>Intrusion Detection Services</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Handling</td>
<td>Security-Related Information Dissemination</td>
<td></td>
</tr>
<tr>
<td>Vulnerability analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability response coordination</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Fig. 1.** CSI RT Services list from CERT/CC
Anonymous Declares Sept 24 “Day Of Vengeance” In The US, Plans A “Series Of Cyber Attacks”

Hacktivist group Anonymous have been busy bees this year, and they’re not planning to cool down any time soon. Earlier this morning, Anonymous (or some 12-year old kid labeling himself Anonymous, who knows) issued a press release announcing that the collective and “other cyber liberation groups”......

Articles published more than 1 hour ago

Win32/SpyEye.AHT

Win32/Spyeye is a family of bot controlled Trojan design to capture keystrokes using "form grabbing" method of internet browser like Firefox and Internet Explorer. It employs rootkit
CERT-EU webportal
  - 800+ sources
  - Automatic scraping of relevant news
  - Categorisation and clustering
  - Next step: html5

EMM Private
  - Underground sources
  - Authoring access for other CERTs

http://cert.europa.eu/
### Advisories

- 2011 (Sept – Dec) 33
- 1Q2012 46
- 2Q2012 22

**Sources:** EMM, mailing lists  
**Subjects:** vulnerabilities, generic threats

### Alerts

- 2011 (Sept – Dec) 50
- 1Q2012 154
- 2Q2012 122 (49)

**Sources:** Customers (incidents), CERTs (alerts), passive monitoring  
**Subjects:** compromised systems, immediate threats

### Average number of unique visitors per day

![Graph showing the average number of unique visitors per day from Sep-11 to Jun-12. The number of visitors increases steadily over the months.]
Most frequent infection vectors

- Infected USB sticks
- XSS/SQL injection
- Web browsing
- Emails (attachments, links)
Extent of the problem not clear to the constituent

- Hidden in the noise of spam
- Lack of user awareness
- Lack of internal reporting mechanisms
- Lack of tools to analyse emails (extraction, testing of links and attachments)
Problems with targeted attacks

- Undetected by the protection systems
- IT department underestimates the problem
- Highly specialised resources to analyse the problem
- Fear of informing hierarchy
- Fear of involving law enforcement
- Difficult to perform the attribution
- Difficult to demonstrate the damage
- Never sure if the problem is resolved
Detection

Client
- Multiple A/V systems
- Additional systems scans
- Network protection systems
- Log analysis
- User awareness (anomalies)

CERT-EU + partners
- Passive malevolence monitoring
- TLD website monitoring
- Mail scanner
- CIMBL
Containment

Client
- Set up reaction team
- Call in the experts
- Isolate compromised system
- Forensic image
- Analyse logs
- Scan other systems
- Assess potential impact on information
- Inform other concerned parties
- Involve LE?

CERT-EU + partners
- Forensic imaging guidelines
- CERT Toolbox
- Interpret and advise
Eradication

Client
- Reimage infected or suspected systems
- Reset passwords (all at the same time)
- Reset passwords in external accounts
- Rescan (regularly)
- Analyse logs (regularly)

CERT-EU + partners
- Analyse malware
- Interpret and advise
- Inform other constituents
- Inform other CERTs
Prevention

Clients
- Risk assessment of information assets (value / risk)
- Information security policy
- Perimeter protection (IDS, AV, WAF) and segmentation
- Log analysis in/out/internal -> anomalies?
- User and password management
- Version and patch management
- Regular scans (MSS)
- Embed security in the application development
- Deactivate autorun (Windows XP), upgrade to Windows 7 - enforcement of policies
- User awareness

CERT-EU
- Advisories and white papers
- Client specific advise and consultancy
- Awareness raising and training material
Tools for detection
- Cymru, Shadowserver, Arbor, N6
- Microsoft / Google
- AbuseHelper
- Pastebin scanning
- Mail scanner / analyser

Next steps
- More sources
- IDS sensors (SNORT / third party)
- DMARC
Malware analysis

- Small internal capacity
- Expertise in clients (EC, GSC)
- Other CERTs
- IT sec partners

Systems

- Internal infrastructure being built up
- System for information sharing on non-public malware
- Automated tools (EC, VirusTotal)
Broader issues

- "Industrial-scale" detection of anomalies
  - Capitalise on existing capacities
  - Foster open exchange of data on indicators of malevolence
- "Industrial" exchange and protection mechanisms
  - Standardisation of meta-data
  - Automated upload in network protection - ISP and network borders
  - Systems and tools for trusted information exchange on incidents, malware

- More effective collaboration between CERTs
  - Sharing of validated IOCs in a standardised format
  - Sharing of information on critical incidents

- Reporting compromises to individuals, SMEs, cross-sector

- "Break the silence", everybody is suffering targeted attacks
- "Break the silos", sharing between CERTs, LE, intell

- Aim for consolidated, validated, up-to-date data set of IOC
Outlook CERT-EU

Challenges
- User awareness / internal processes to handle anomalies
- Better information sharing by clients
- Better responsiveness of clients to alerts
- Better automated detection mechanisms, more sources
- Automated protection processes

Next steps
- More capacity in alerting and incident handling
- Basic artifact analysis capacity
- More client-specific service
- Broader and modular service package, including network sensors for some clients requesting such service
- Systems and tools development in particular for "industrial" detection of anomalies and exchange of information
Thank You

http://cert.europa.eu/