

Security incident management - what's going on in Latvia?

Baiba Kaškina, Artūrs Medenis
NIC.LV CERT, IMCS UL

“Cooperation to Enhance Security in Cyber Environment” –

21 November 2007, Vilnius

The top of the slide features a blue header bar. On the left, the word "CERT" is written in large, light blue, sans-serif capital letters. To the right of this text, there is a decorative graphic consisting of a stylized, metallic-looking structure with sharp, upward-pointing elements, resembling a traditional East Asian architectural ornament. Further to the right, there is a small, square grid pattern with varying shades of blue and white.

CERT

“The superior man, when resting
in safety, does not forget that
danger may come”

Confucius

Outline

- CERTs in Latvia
- Statistics
- CERT initiative in Latvia
- Future ideas

A blue banner at the top of the slide. On the left, there is a stylized tree logo. In the center, the word "CERT" is written in large, light blue, sans-serif capital letters. To the right of "CERT", there is a smaller, faint "CERT" logo. On the far right, there is a circular logo with a stylized tree inside, and a small grid of blue and white squares.

CERT

CERTs in Latvia

LATNET CERT

- Established in summer 2006
- Part of IMCS UL, LATNET laboratory, Latvian NREN
- Status “listed” in Trusted Introducer
- Constituency – LATNET customers – academic, commercial
- More info: <http://cert.latnet.lv>

New name – NIC.LV CERT

- Part of IMCS UL, under umbrella of ccTLD.LV
- Free services to Latvian internet users
 - Black-white-grey lists
 - Traffic analysis
 - Support to the new CERT teams
 - ...

CERT

VITA CSIRT -



- Established at the end of 2006
- DDIRV operates under the auspices of State Information Network Agency management board,
- Start of Operations – 1 January 2007
- Status “listed” in Trusted Introducer from August 2007
- Constituency – state and municipal institutions (autonomous system AS8194)
- Cooperating with ENISA in projects related to information security

VITA CSIRT -



- Webpage www.ddirv.lv provides:
 - computer security incident report form
 - actual viruses and vulnerabilities (RSS feed)
 - publications about IT security
 - quarterly statistics
 - DDIRV news and actual information related to IT security in Latvia

Third CERT - military

- Plans to establish in December 2007
- 6 people team
- Constituency – all military organisations

CERT

CERT

Statistics

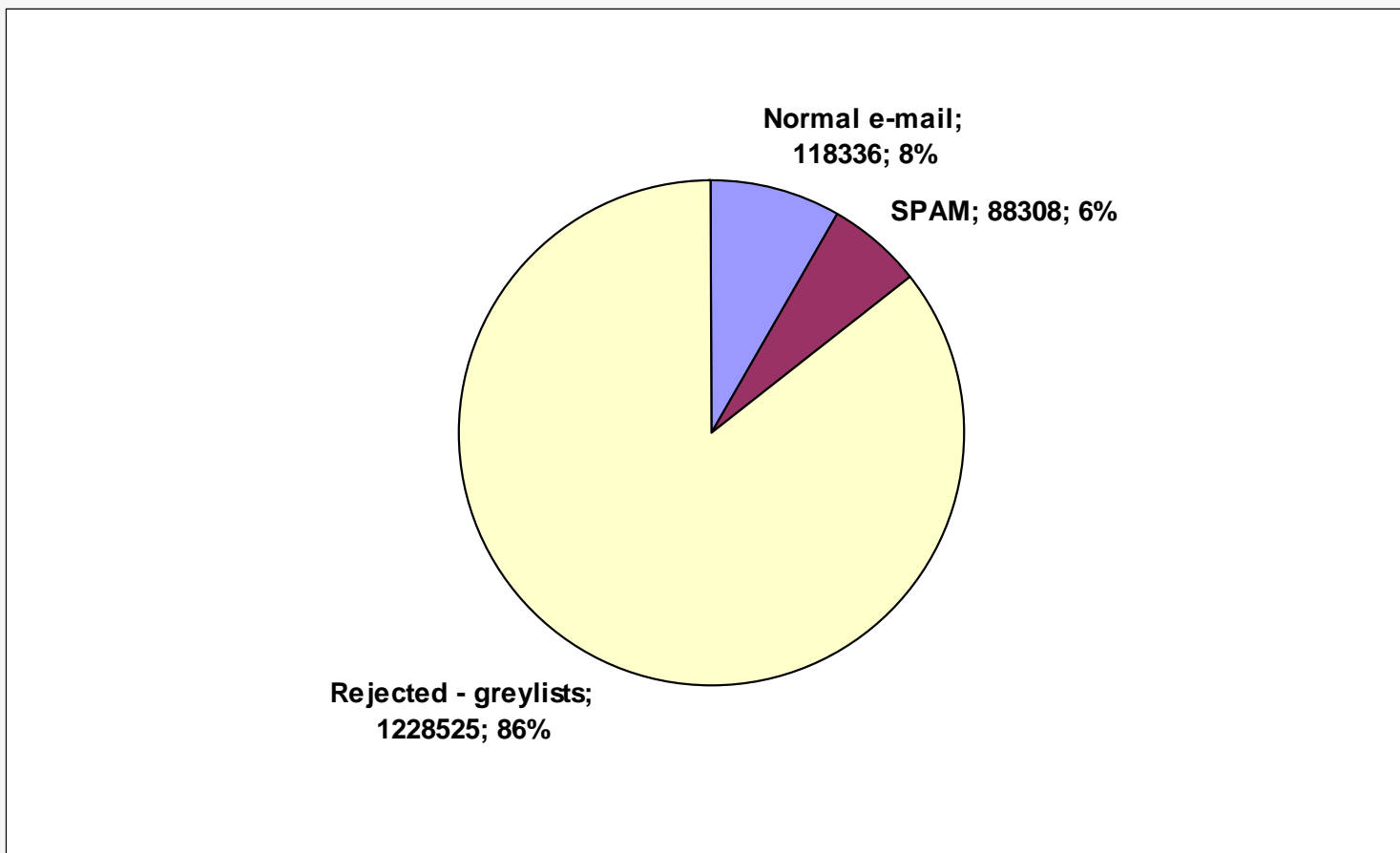
Incident statistics

- LATNET-CERT data - 95% - SPAM;
- The rest – port scan, phishing, unauthorized access, copyright issues, worms, trojans, etc.

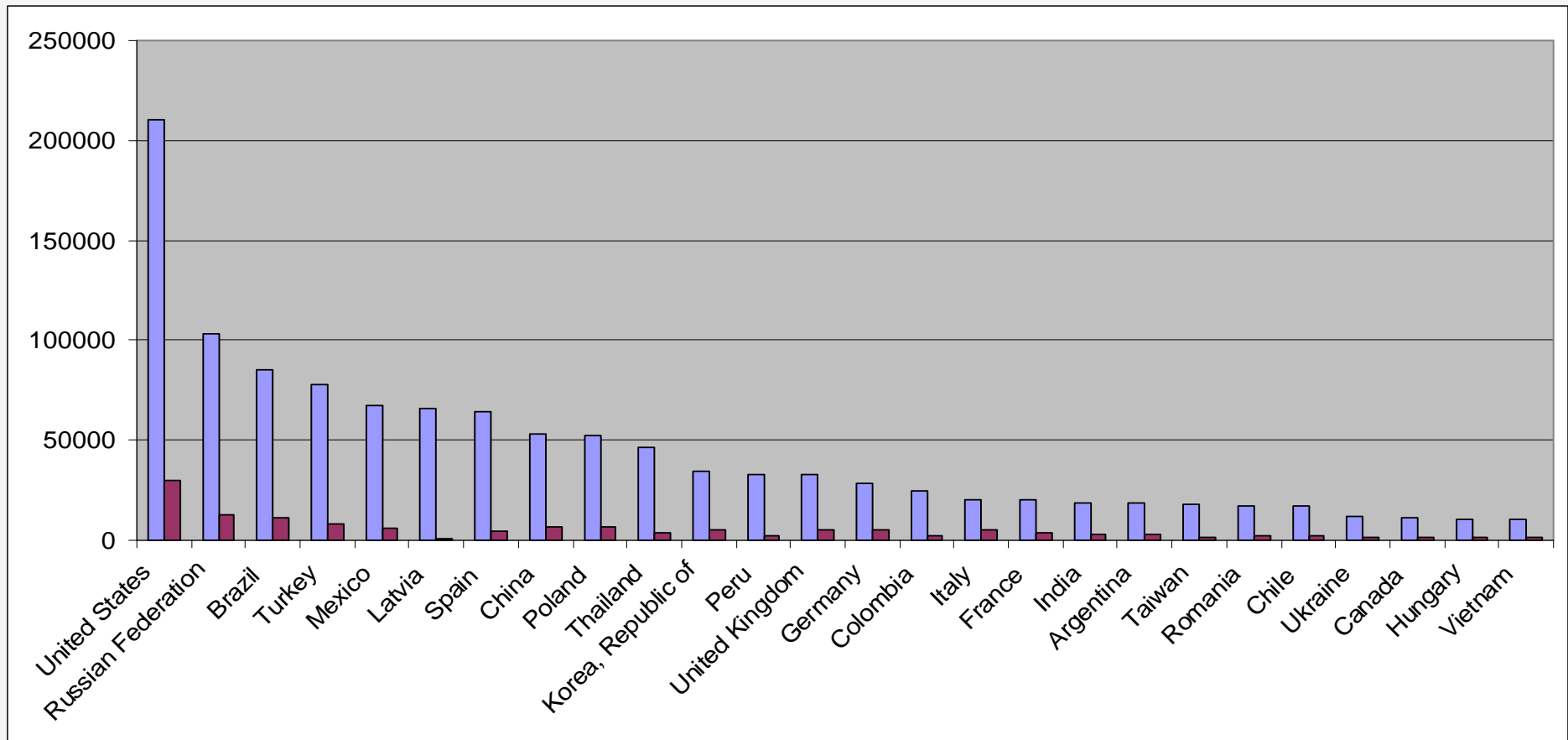
E-mails – 1 day – 15 November

- IMCS UL e-mail servers
- E-mail processing:
 - Greylists
 - SPAM Assassin, D-SPAM
 - Normal e-mail distributed to end-users
- Total in 24h = 1 435 169

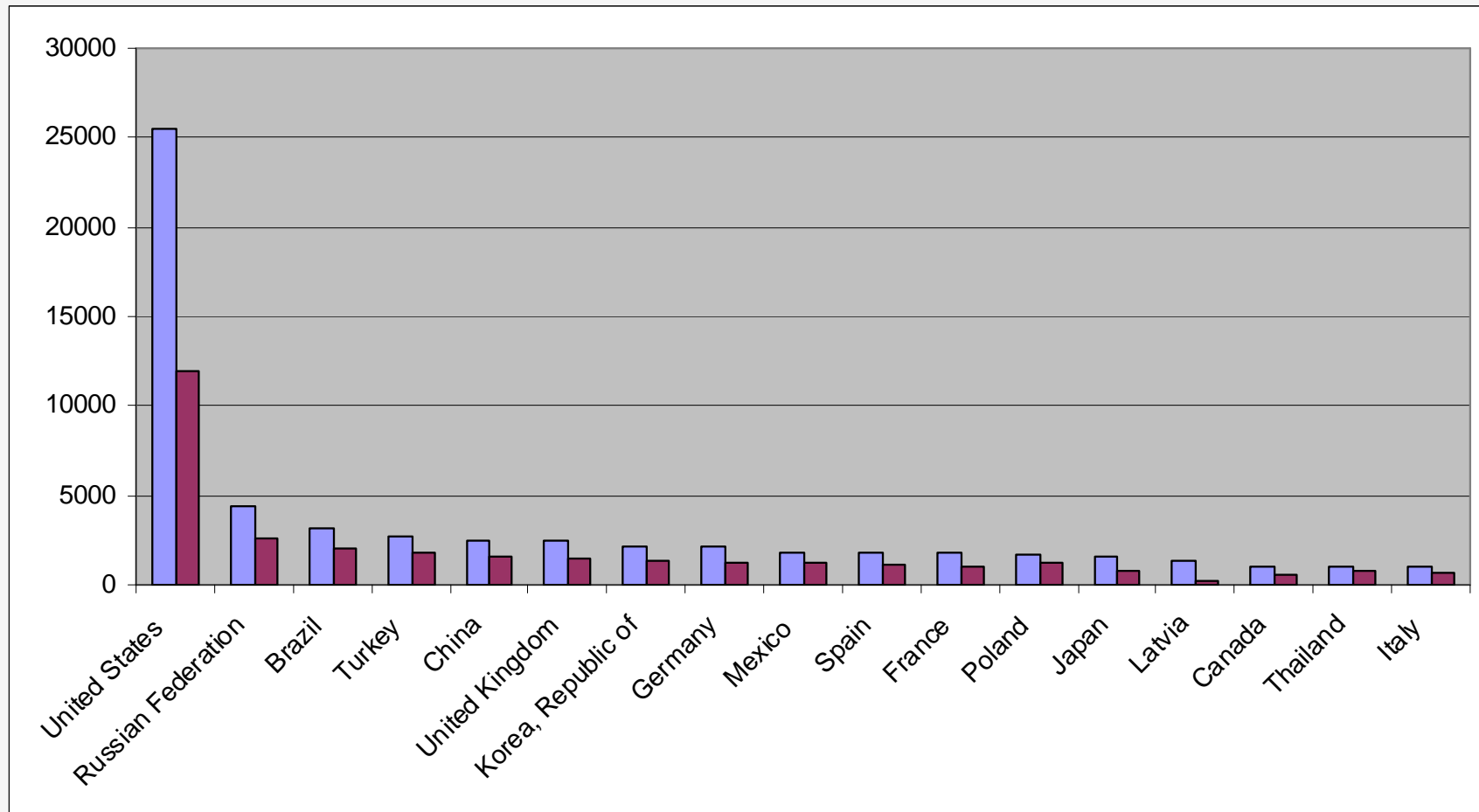
Greylists, SPAM Assassin, normal e-mail



Greylists - countries



SPAM - countries



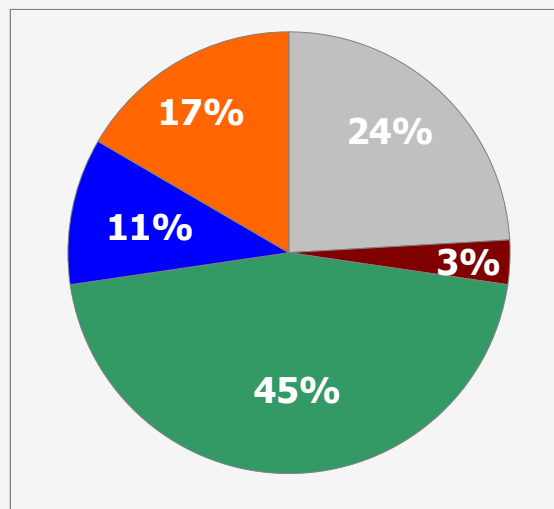
Situation - Latvia

- Greylists – 66227 e-mails a day!
 - 677 unique IPs (97,8 ratio)
 - Zombies
 - Open relay servers
 - Good connectivity
- SPAM – 1364 e-mails a day!
 - 189 unique IPs (7,2 ratio)

VITA CSIRT -



Statistics from 1 January – 30 September 2007



Unauthorized access - 24%
DoS/DDoS attacks - 3%
Compromised system- 45%
Phishing- 11%
Other - 17%

Incidents in Latvia

- Many incidents remain unknown
 - Uncompetent IT department
 - Compromising organisation
 - No proper monitoring
- There are few incidents which become famous
 - State Police home page altering
 - Altering of the Presidents home page
 - *Phishing* attacks against the big banks
 - ...

The top banner features the word "CERT" in large, light blue, sans-serif capital letters. To the right of the text is a decorative graphic consisting of a stylized, metallic-looking structure resembling a dragon or a complex sculpture, set against a blue background with a pixelated pattern on the right side.

CERT

LV-CERT initiative

The top of the slide features a blue header bar. On the left, the word "CERT" is written in large, light blue, sans-serif capital letters. To the right of the text, there is a decorative graphic consisting of a stylized, dark grey, thorny branch or wreath. Further to the right, there is a small, square grid of pixels in various shades of blue and black.

CERT

All that is necessary for the triumph of evil is that good men do nothing.

Edmund Burke

Why to collaborate?

- Growing number of incidents
- Impossible to fight alone
- International pressure
- No team knows everything
- Collaboration needed on the country level

CERT

CERT

LV CERT initiative



LATNETCERT



LV-CERT Goals

- Activity coordination
- Awareness raising
- Cooperation on incident handling and prevention
- Collaboration with all parties who want to improve security and safety in the Internet

LV-CERT Activities

- Exchange of contact details
- Cooperation – hosted by NIC, IMCS UL
 - Mailing list
 - Meetings
 - Exchange of information
- Collaboration on incident response
 - Exchange of incident data

LV-CERT Cooperation

- Co-operation with other organisations
 - LIKTA
 - Several ministries (E-issues, Transport and Connection)
 - State Police
 - Military organisations
- TF-CSIRT, FIRST

CERT

CERT

Future ideas

LV-CERT plans

- Webpage, more info on-line
- Awareness raising campaigns
- Participation in work-groups
 - Critical infrastructure
- Support for new CERTs in the country
- More proactivity, monitoring
- International collaboration

Summary

- We welcome all initiatives!
- We are happy to help
- We are idealists...

The top of the slide features a blue banner. On the left, the word "CERT" is written in large, light blue, semi-transparent capital letters. To the right of the text, there is a decorative graphic consisting of a stylized, metallic-looking structure with sharp, upward-pointing spikes, resembling a crown or a piece of armor. The background of this graphic is a blue and white pixelated pattern.

CERT

Thank you!

If you have any questions, please do not
hesitate to contact us: *info@cert.lv*