COMPUTER SECURITY INCIDENT RESPONSE TEAM

RU-CERT

10 years of experience in incident response in Russian Federation

12-17 June 2011 Vienna

About

- 1998. Start as RIPN (Russian Institute of Public Networks) project 1998 as CSIRT of RBNET (NREN)

- FIRST, TI member

- 2011. RU-CERT - non-commercial organization that plays a role of a national level CSIRT team of Russian Federation

- Hours of work - 10:00-18:00 every day, except weekends and national holidays

- Responsibility domain – whole Russian address space

- Funding model - sponsorship

OPERATIONAL DETAILS

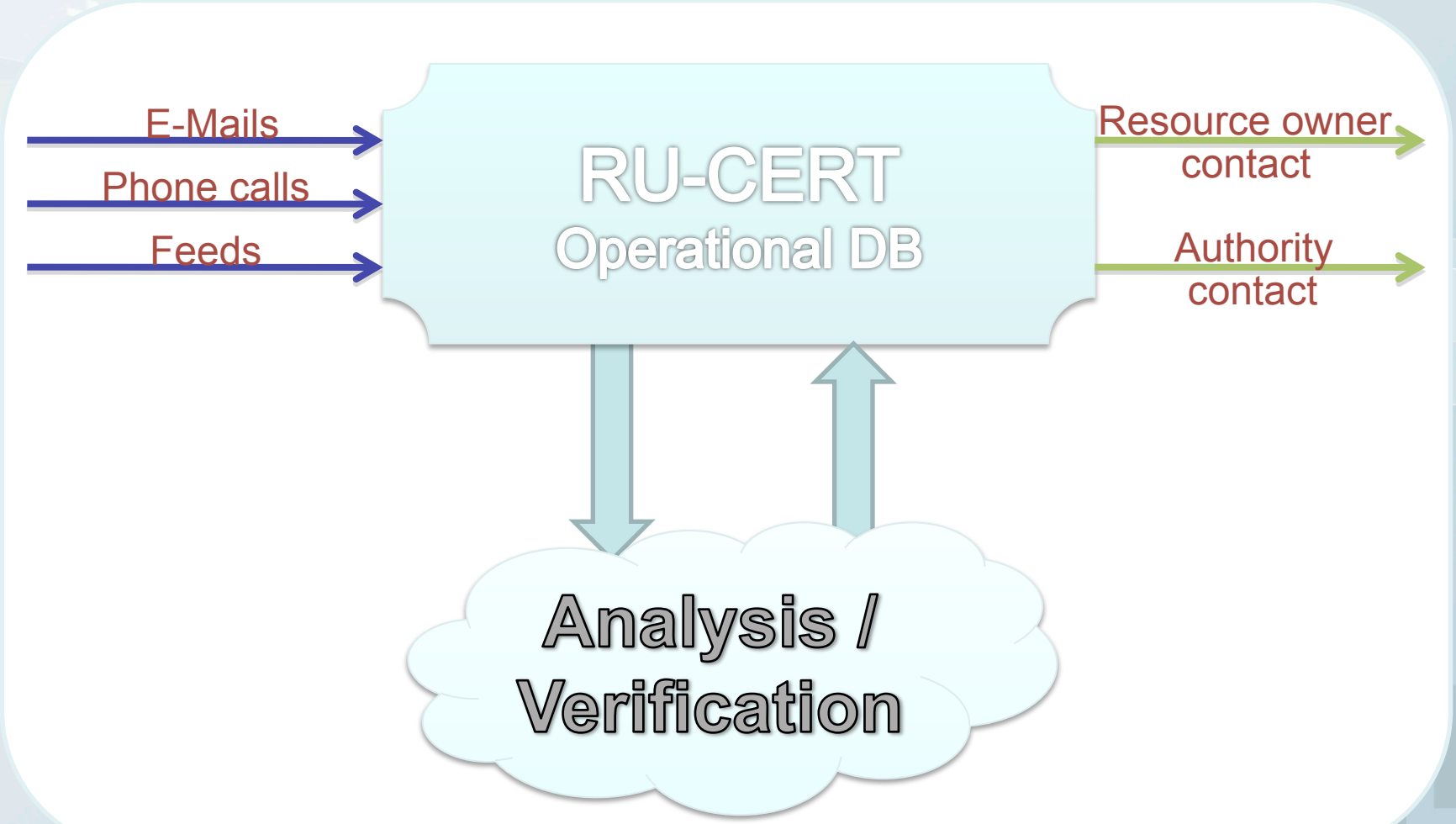
Environment - reality

- No authority over ISPs, domain registrars, etc.
- No IP resources under control

Mode of operation

1. Gathering (getting) all the information about malicious Russian resources and network activity related to Russian address space
2. Information analysis and verification
3. Attempting to solve the problem

Mode of operation (continued)



Another operational mode

- Dispatching urgent requests to Russian LEA

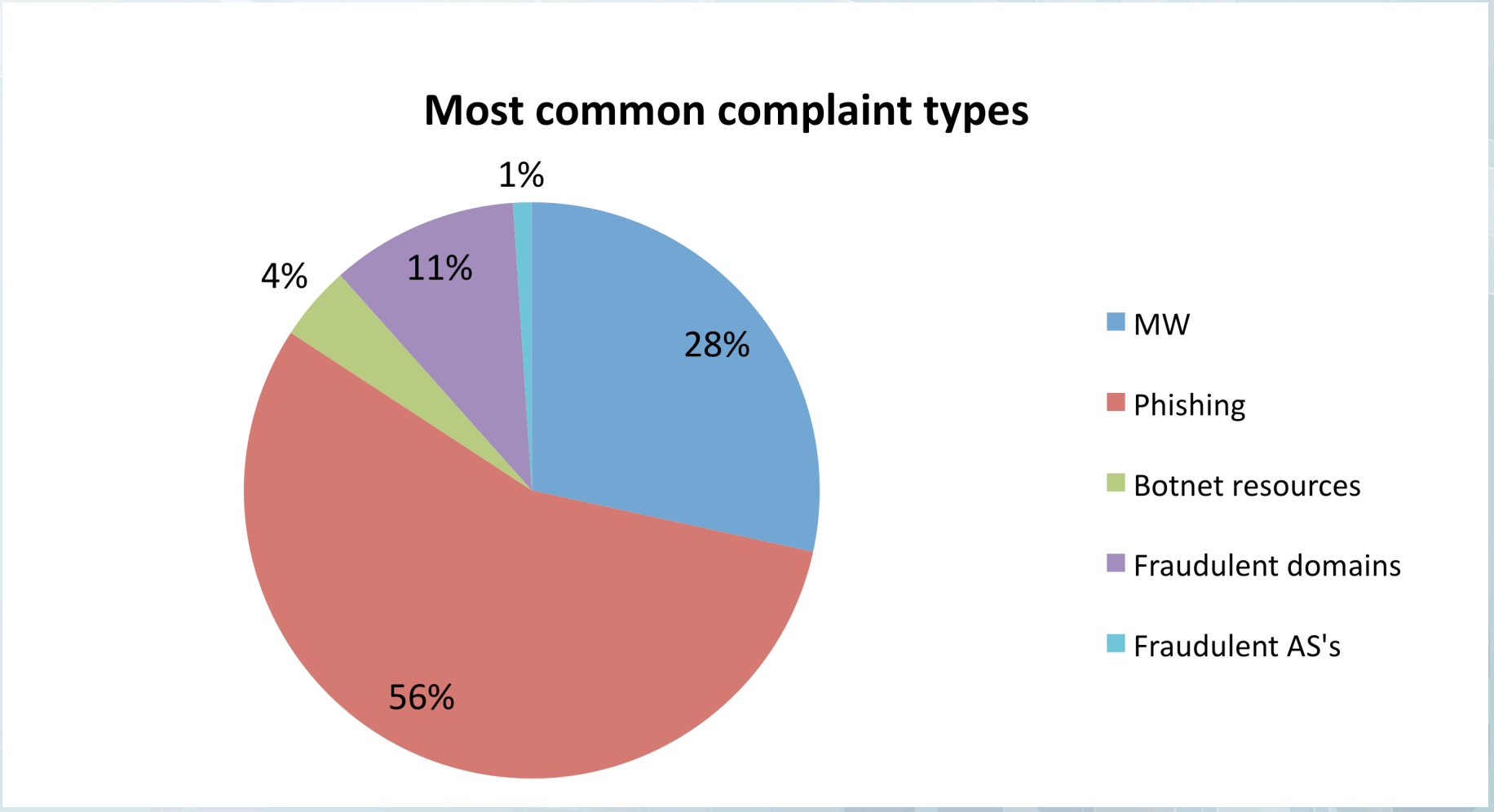
Requests direction

1. Foreign countries -> Russia 95%
2. Russia -> Foreign countries 1%
3. Russia -> Russia 4%

INPUT details

Incidents processed

All kinds of «typical» incidents, except SPAM cases



Feed sources

- Arbor Networks
- Shadowserver
- Abuse.ch bundle
- Malwaredomainlist
- CleanMX
- Phishtank
- Malc0de
- Team Cymru
- Some other's (3-4, incl. temporary)

Feed data volume (average/ per day)

Type	New	Unique	Summary
Phishing	62	176	199
MW	250	508	523
C&C	4	31	32

Top list of e-mails input (5 months)

	MW	Phishing	Attacks
mycert@mycert.org.my	126		105
auscert@auscert.org.au	219	6	
ftsteam@paypal.com	14	189	
cert@cert.br	100	68	
csirt@bradesco.com.br	70	34	
@markmonitor.com	76	19	
@brandprotect.com	32	83	

CC/TO balance statistic

	RU-CERT in TO field	RU-CERT in CC field
mycert@mycert.org.my	110	121
auscert@auscert.org.au	17	208
ftsteam@paypal.com	4	198
cert@cert.br	168	
csirt@bradesco.com.br	104	24
@markmonitor.com	67	14
@brandprotect.com	92	23
cais@cais.rnp.br		65
afcc@rsa.com	57	

Information processing

Security event – any information related to computer security case

Incident – SE, that RU-CERT reacts to in some way

Will **SE** be transformed into **Incident** or not significantly depends on results of verification:

Phishing

- 95-98% of all requests are really phishing resources
- ~80% of phishing resources are located on compromised servers
- Second level domains used for phishing sites – lately occurs very seldom
- Most cases - non-Russian banks and payment systems

Malware 70-75% can be verified (MHR, etc)

Attacks Unverified

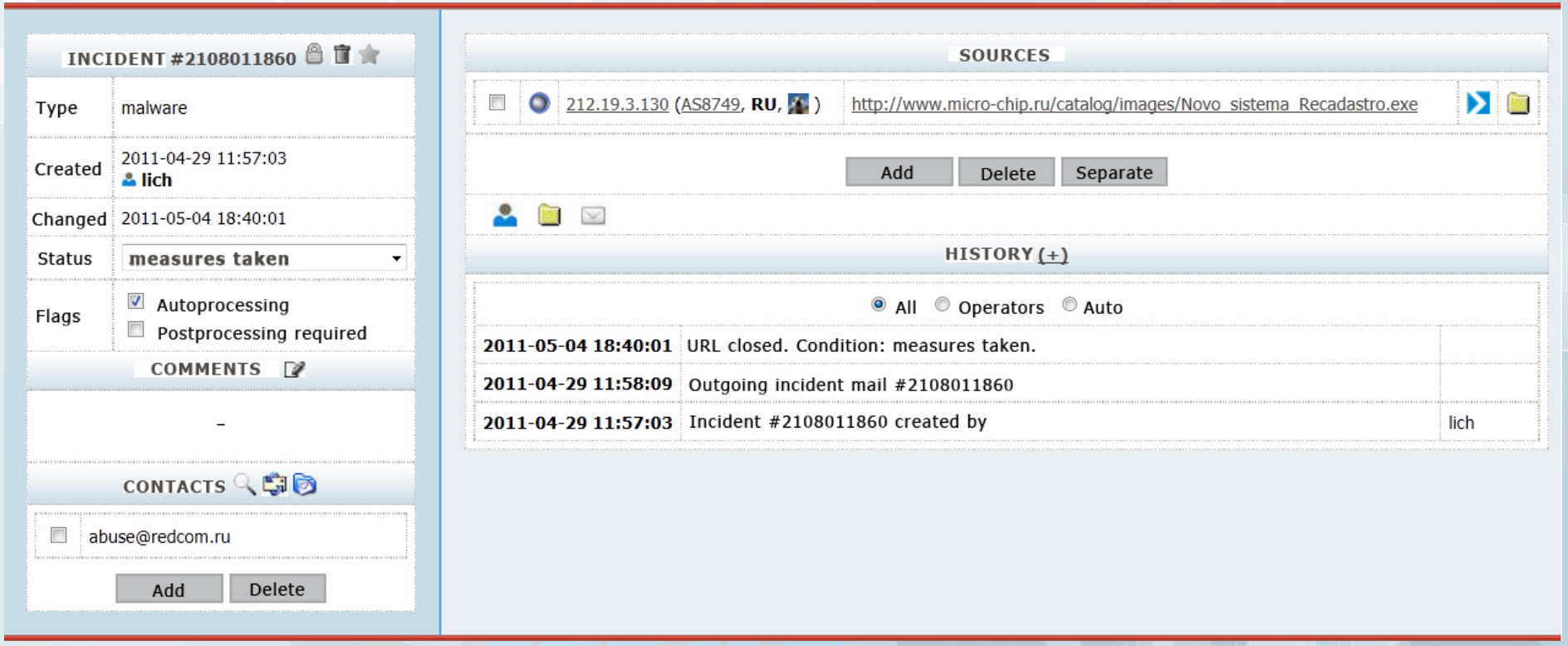
C&C 10-15% can be verified

Contact details

1.Resource owners – more than 600 contacts in RU-CERT database
2.LEA's – 3-4 cases/per month
3.CCTLD (Coordination Center of Russian TLD zone) (domains in .ru/.pф zones)

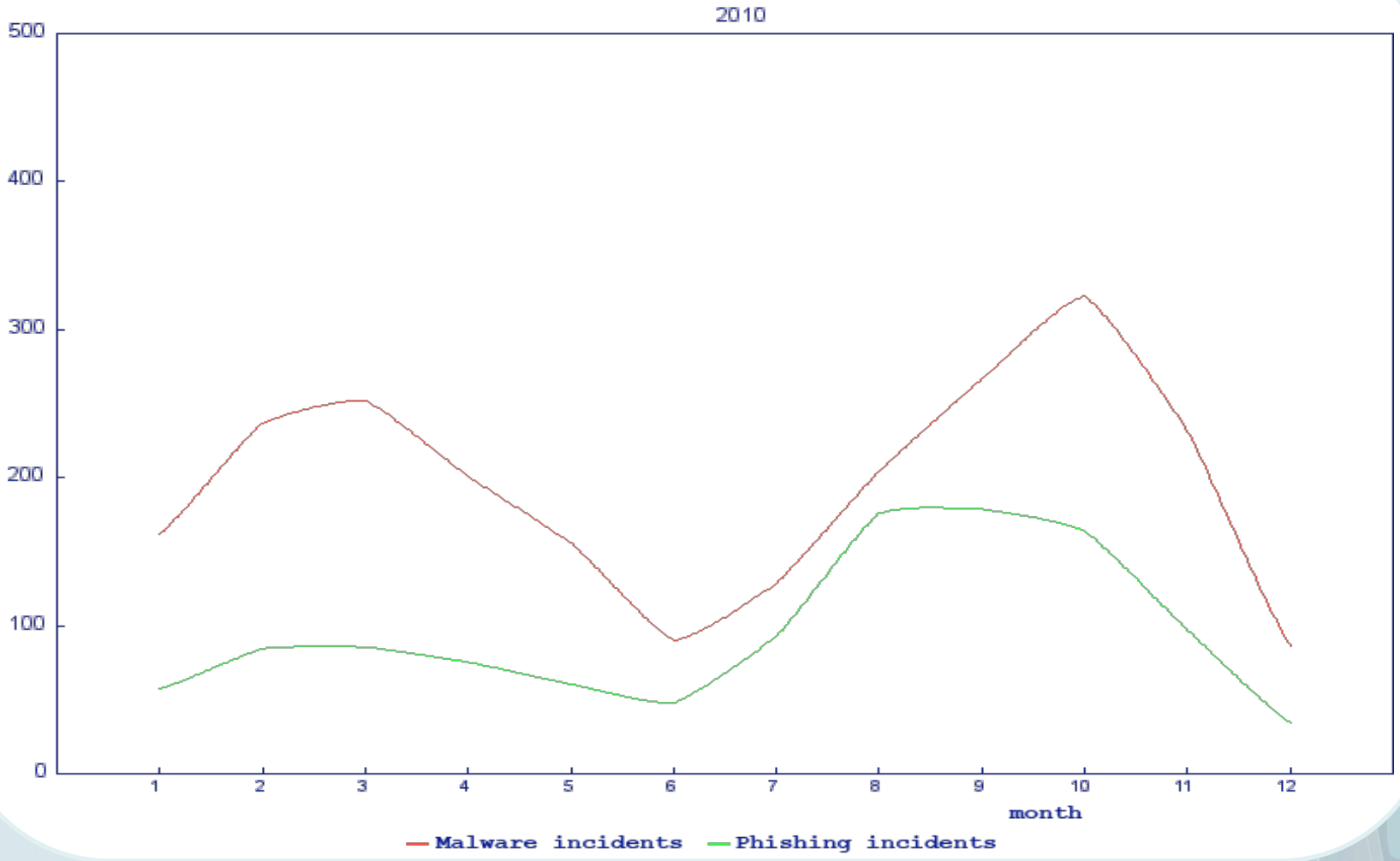
Monitoring model

Incident processing software



INCIDENT PROCESSING STATS

Summary (mw/phishing) 2010



Destination geographic distribution

City	MW	Phishing
Moscow	3054 (47.07%)	191 (12%)
St. Petersburg	609 (9.38%)	22 (1.4%)

Difficulties (technical)

- Incorrect information in RIPE database
- Small net objects often not listed in database
- AS's ownership often can't be discovered without ISP support (VPN)

Effectiveness

Not easy to estimate – but performance index is positive because of:

- We have a lot of established contacts with ISPs/domain registrars
- Better chance to find out correct contacts (5-6 calls chain is normal)
- Requests coming from a Russian organization are usually treated in a more friendly manner

Questions

ganev@cert.ru, info@cert.ru
http://www.cert.ru/