Conficker After Action Report

David Piscitello

2 June 2010

Conficker Summary and Review

https://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf

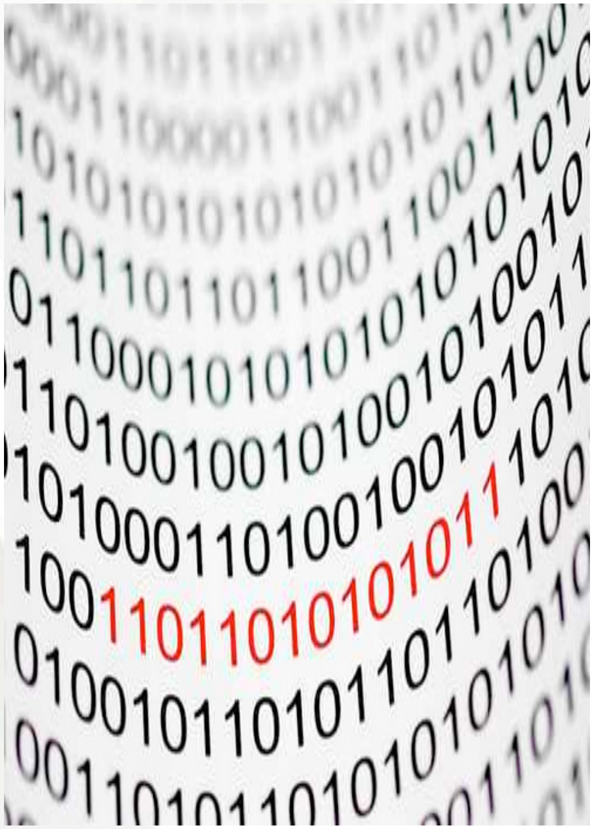
David Piscitello
Sr. Security Technologist
ICANN

ICANN

BRUSSELS

No.38 | 20-25 June 2010

What is Conficker?



An Internet worm (self-replicating malware)

- Uses a network for distribution
- Enlists infected computer into a botnet

Armored

- Protects itself from detection and removal

Configurable and upgradeable

- Connects to rendezvous points using HTTP to obtain instructions or additional malware

Resilient and adaptable

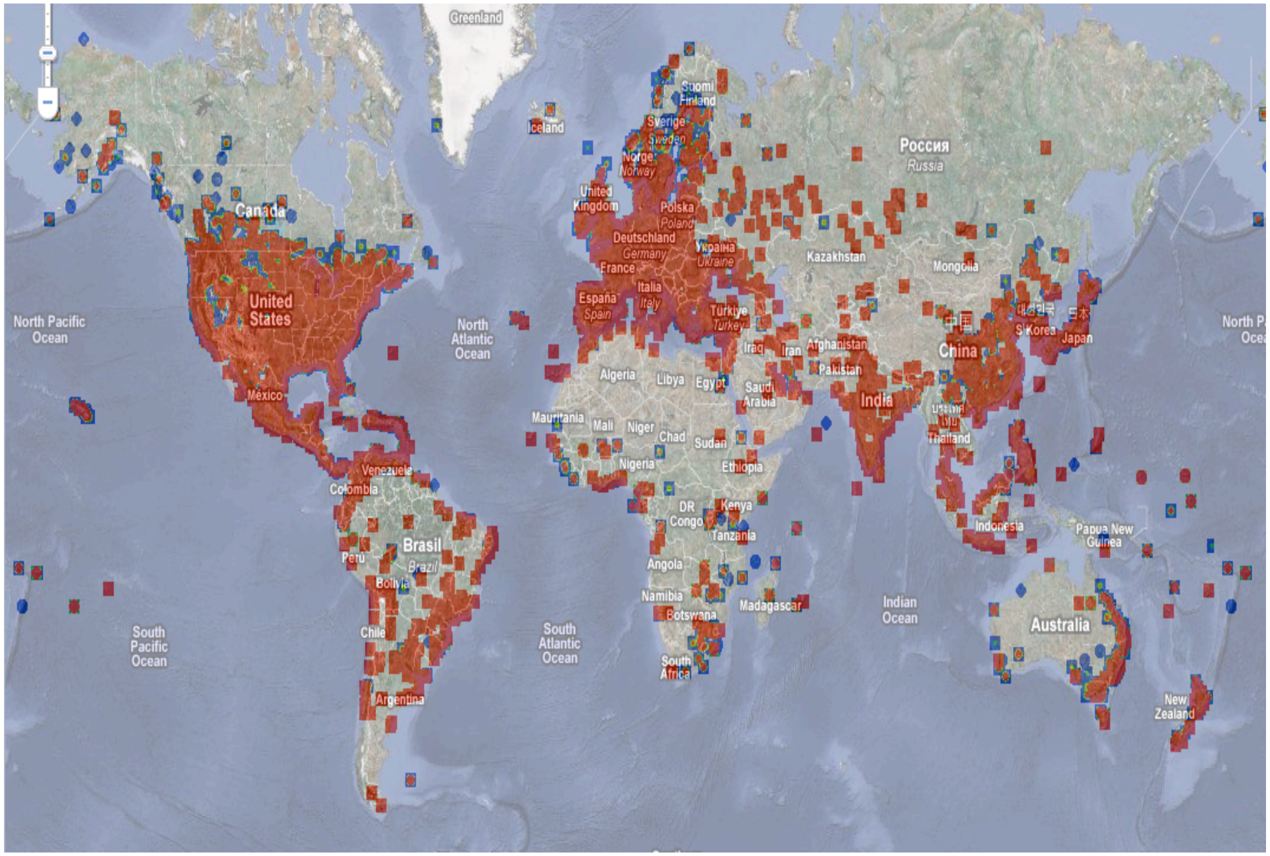
- Initially used algorithmically generated domain names to identify rendezvous points
- Switched to peer-to-peer network

What is a Conficker botnet

An army of remotely controlled, infected computers

Botnets can be “hired” for malicious, criminal or terrorist activities…

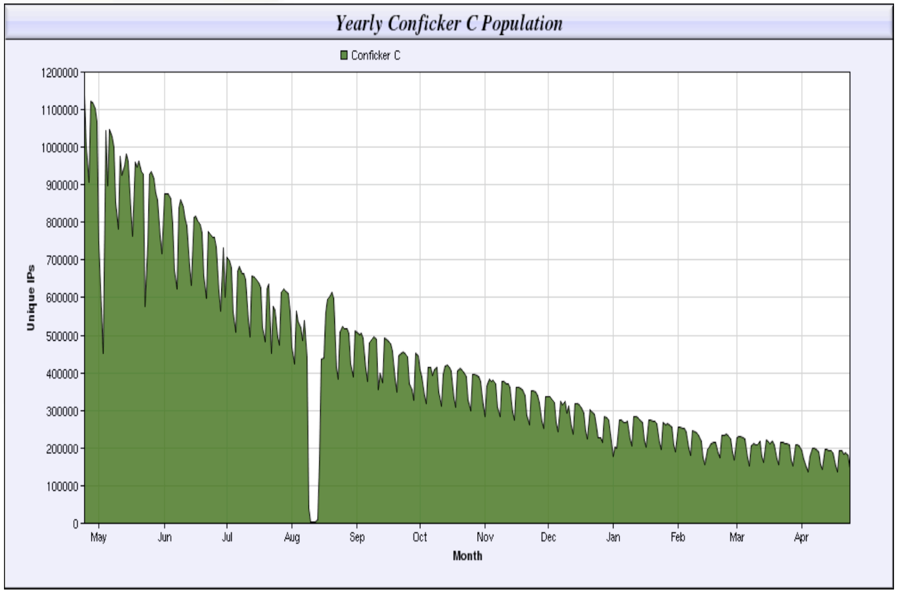
for as long as the computer remains infected fFor as long as the bots remain under the control of the bot herder



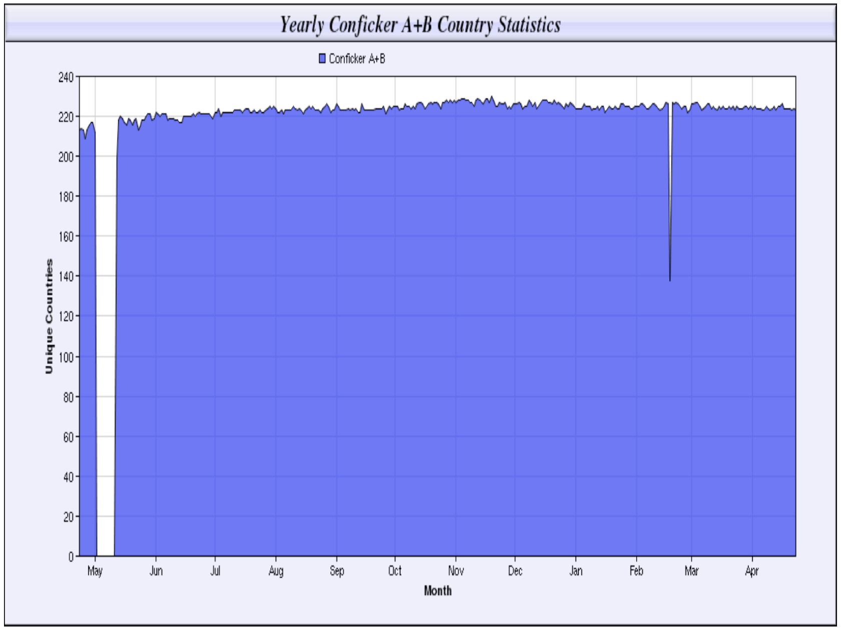
Source:
http://www.confickerworkinggroup.org

ICANN
BRUSSELS
No.38 | 20-25 June 2010

Conficker today

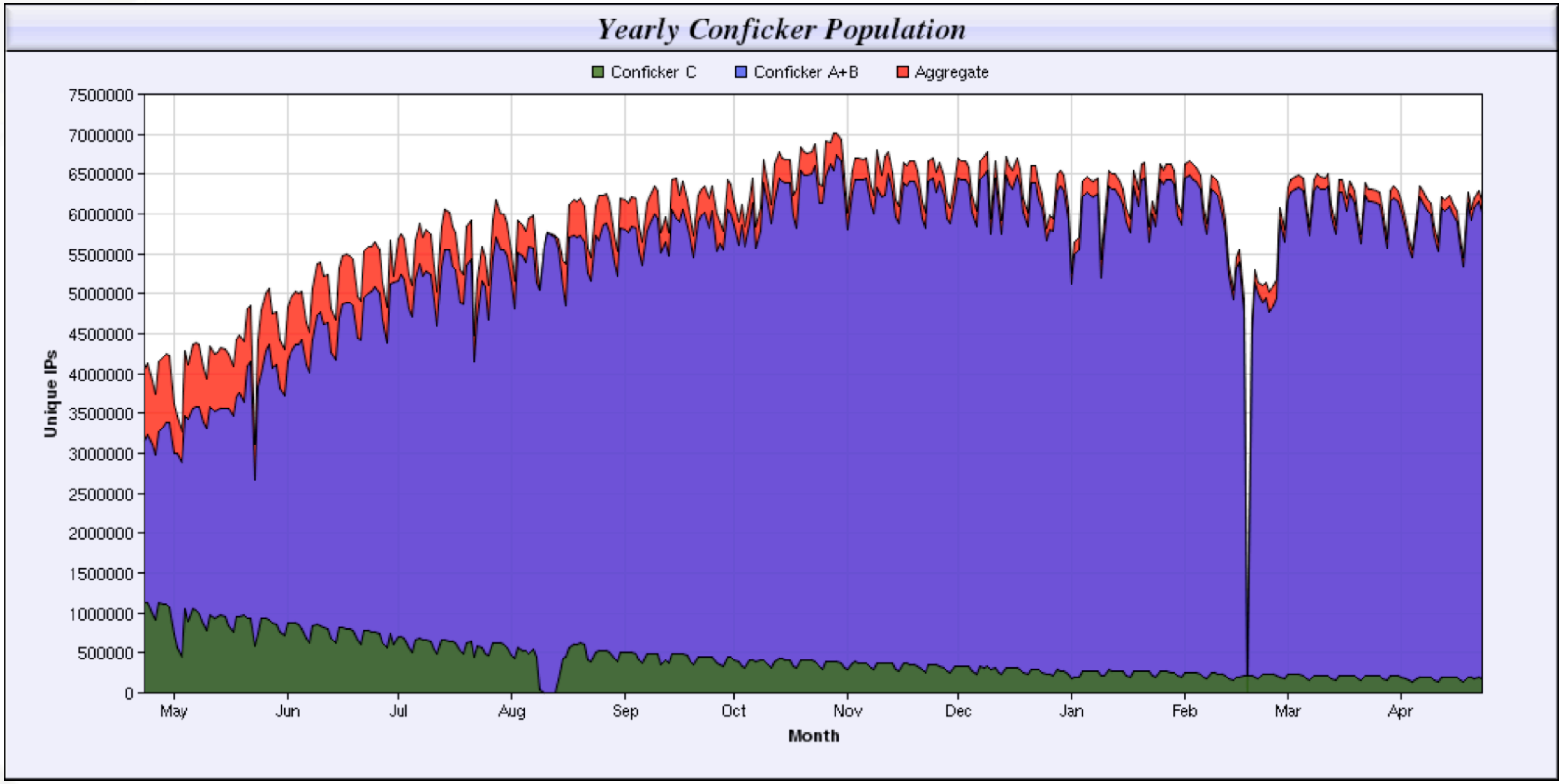


Conficker.C population has diminished



Aggregate A+B populations is still large

Total Conficker infections still in millions



Positive outcomes

DNS, security, and law enforcement can collaborate when an incident of global proportion is identified

Conficker Working Group disrupted botnet communications and contained infection

Disappointing outcomes

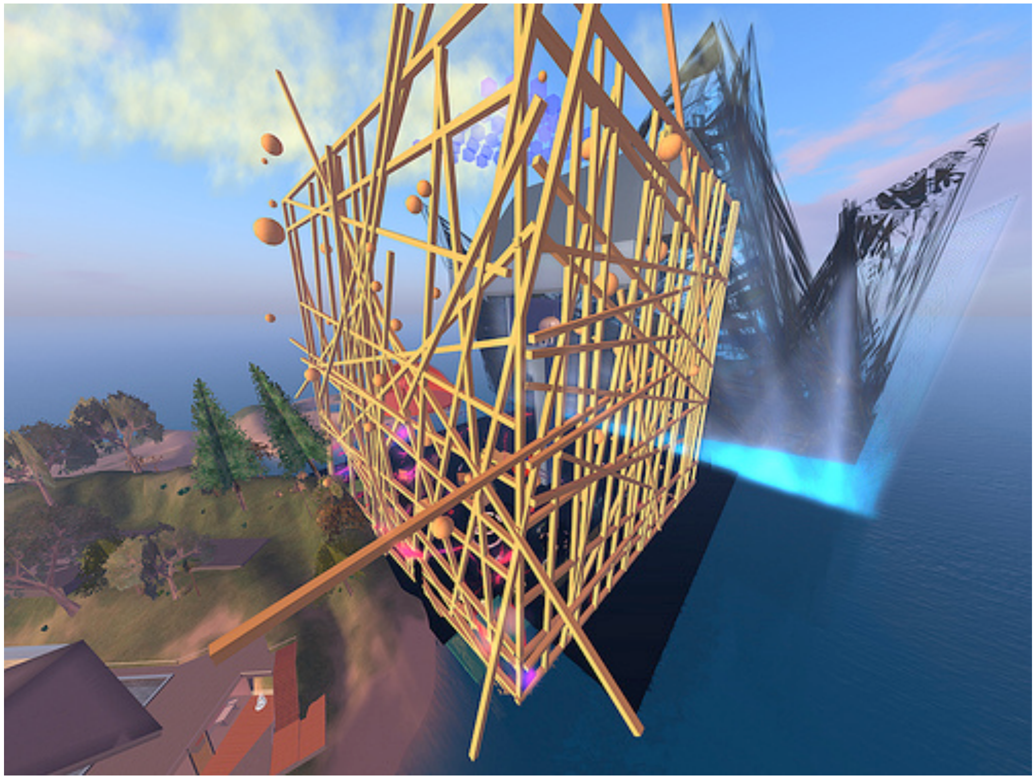
Containment was temporary

Malware writers adapted Conficker to counter the containment measures

What can we learn from past experiences

Ad hoc responses are not sustainable

Problems that encumbered the Conficker response will persist without complementary formal structures or commitments

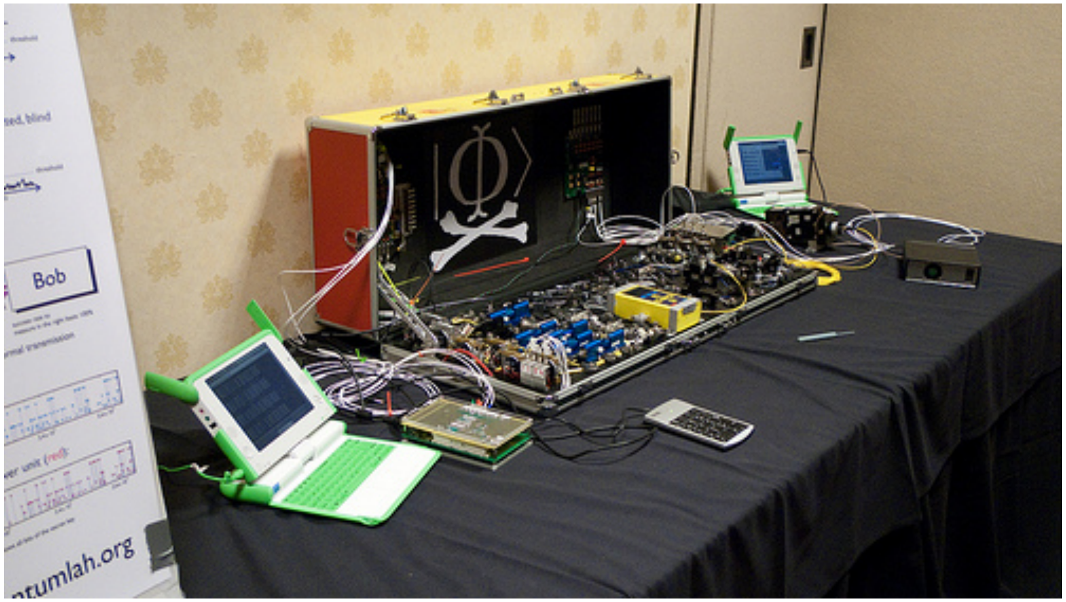


Malware writers adapt to countermeasures

But…

DNS is likely to continue to be part of malware writer toolkits

Consider ways for engage DNS community quickly and efficiently

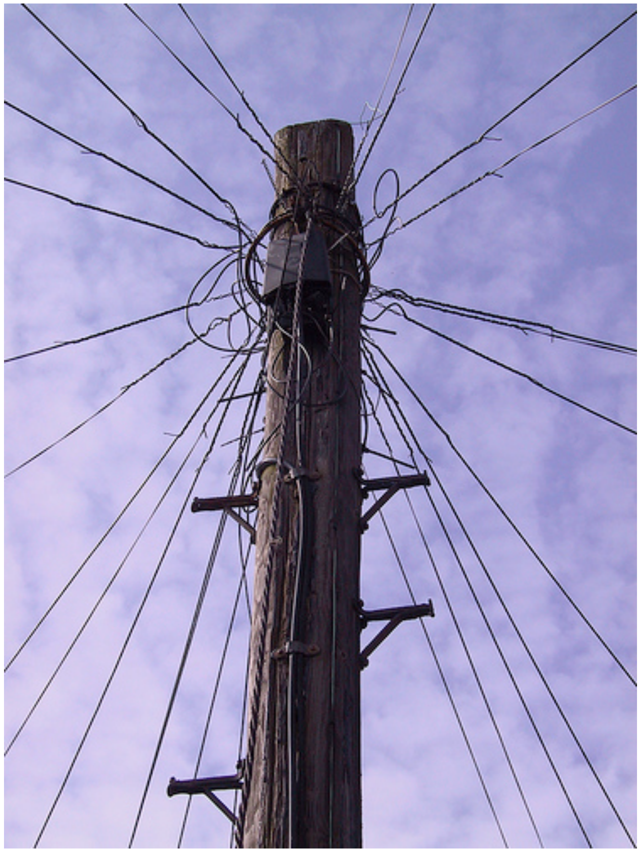


Maintaining consistent, complete and accurate information is challenging

Chronicling the Conficker response has been difficult

Consider formal action tracking or auditing

Informal communications may not be sufficient for global incident response



Formal channels with agreed-upon or mandatory exchanges and exchange frequencies should be considered for future response efforts

Scaling trust is hard

Volunteer efforts are based on personal webs of trust

Consider ways to rely upon and assure that participation and availability

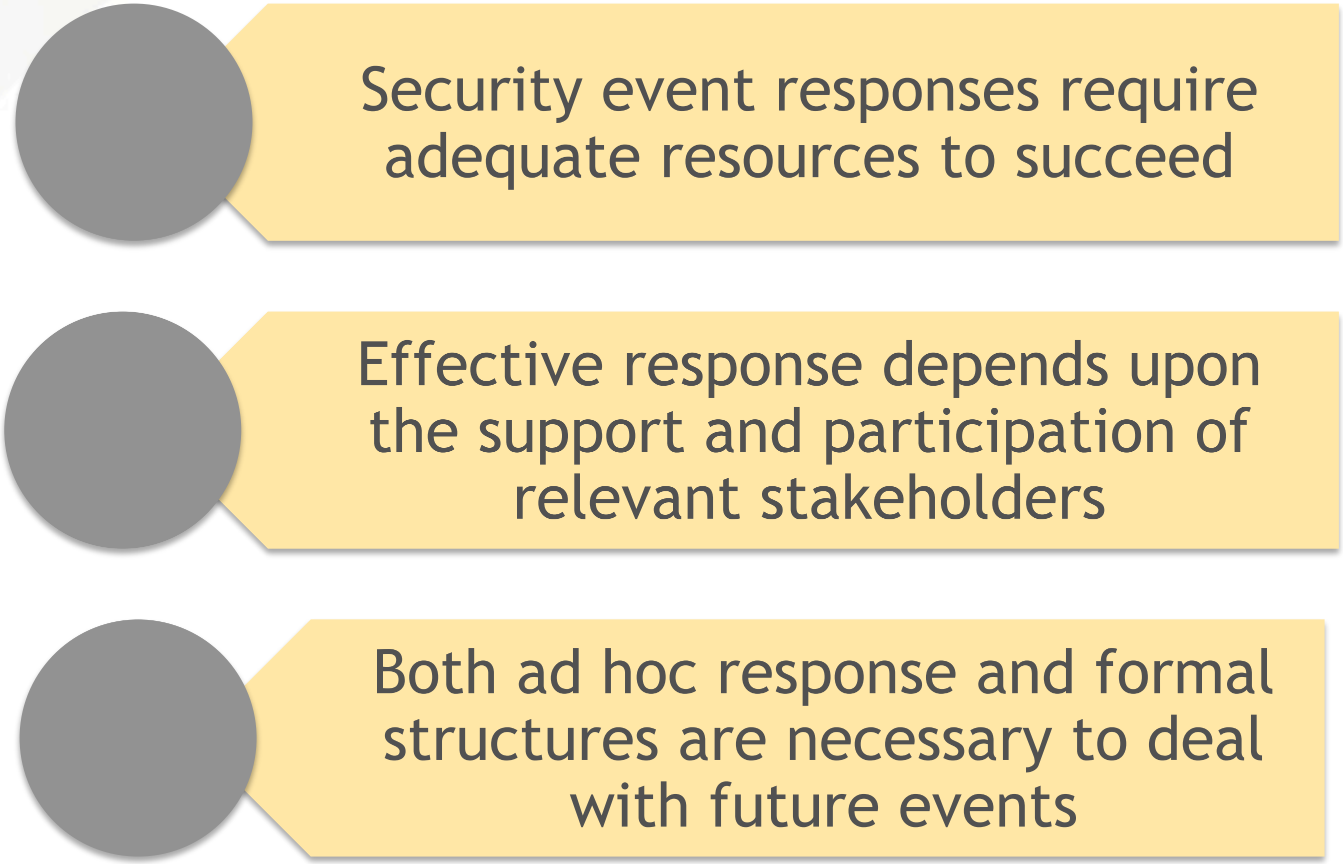
DNS incidents may be global, but TLD registries have local issues to consider

Response actions may raise contractual issues for gTLDs

Response actions may have operational impact

Certain response actions cannot be implemented unilaterally by all TLD operators

Summary of lessons learned



Security event responses require adequate resources to succeed

Effective response depends upon the support and participation of relevant stakeholders

Both ad hoc response and formal structures are necessary to deal with future events

Way forward for ICANN community

Formalize relationships among parties that become involved when security events of a global nature occur

Put structure in place to deal with contractual issues that may arise during a global security event (ERSR)

Consider a security coordination center to assist DNS operators and supporting organizations (DNS-CERT)

Thank you

Photo Credits

Uncredited photos are from ICANN's Flickr page, or by ICANN staff. The following photos were used under a Creative Commons non-commercial attribution license:

- Slides 2, 17, Ninako
- Slide 7, SquirrelQueen
- Slide 8, LiveandRock
- Slides 10, Lance Shields
- Slide 11, Anderson Ramos
- Slide 12, Fernando Gregory
- Slide 13, Nicholas Smale
- Slide 14, Forbes Images
- Slide 15, SassyH, FotoFluke, Bristol Born & Bred

ICANN

BRUSSELS

© vzw Atomium

No.38 | 20-25 June 2010

Questions