nic.br cgi.br | cert.br

GFCE Triple-I Capacity Building | The Internet Infrastructure Security Day

La Paz, BO | August 5, 2019

CSIRTs and Collaboration

Lucimara Desiderá, M.Sc.
Security Analyst
lucimara@cert.br

cert.br nic.br cgi.br

cert.br

TLP:WHITE

Incident Management	Training and Awareness	Trend Analysis
Coordination	Courses	Distributed Honeypots
Technical Analysis	Presentations	SpamPots
Support for recovery	Best Practices	Processing of threat feeds
	Meetings	

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Network

The Honeynet PROJECT

Creation:

August/1996: report with a proposed model for incident management for the country is published by the Brazilian Internet Steering Committee – CGI.br[1]

June/1997: CGI.br creates CERT.br (at that time called NBSO – *NIC BR Security Office*) based on the report's recommendations[2]

[1]https://www.nic.br/grupo/historico-gts.htm | [2]https://www.nic.br/pagina/gts/157

Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Focus of the Activities

- National focal point for security incident reports
- Support technical analysis and the understanding of attacks and threats
- Develop collaborative relationships with other entities
- Increase the capacity of incident detection, event correlation and trend analysis in the country
- Transfer the acquired knowledge through courses, best practices and awareness materials

Credits

Slides of this presentation are based on

- FIRST Training “Incident Response for Policymakers”
  https://www.first.org/education/trainings
- Report of the 2014 IGF Best Practices Forum on Establishing and supporting CERTs for Internet security
  https://www.intgovforum.org/multilingual/content/2014-best-practices-forums

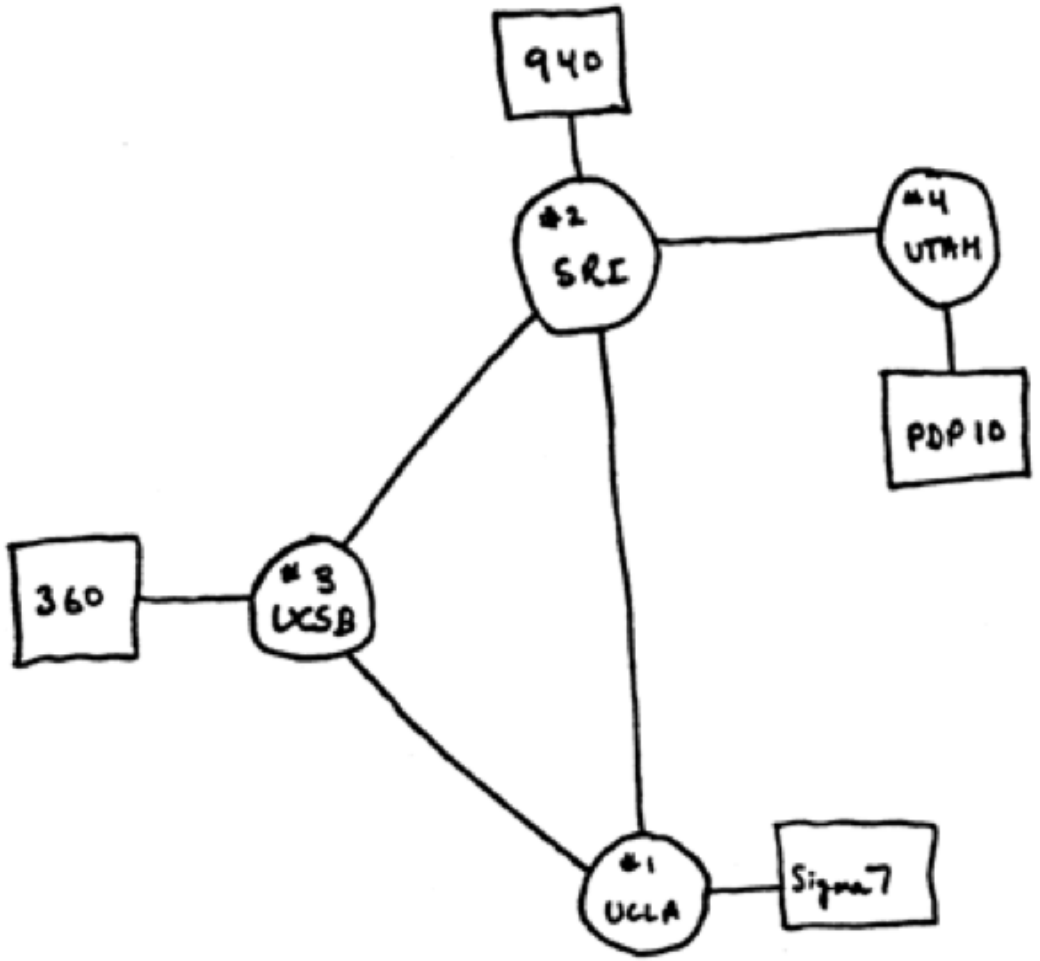
What is a CERT/CSIRT?

"*A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for* ***receiving, reviewing, and responding to computer security incident reports and activity****. Their services are usually performed* ***for a defined constituency*** *that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client.*"

"*An Incident is any* ***real or suspected adverse event in relation to the security of computer systems or computer networks***."

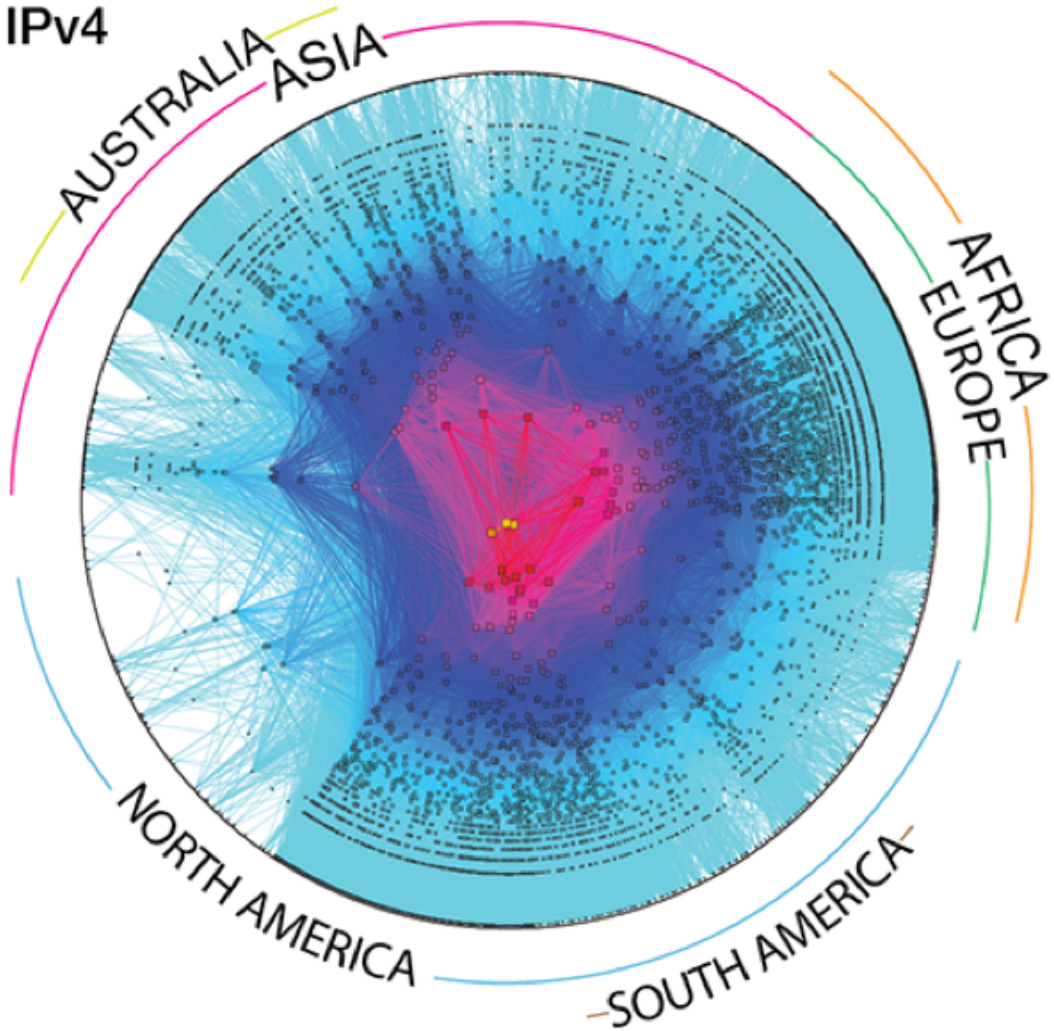
Source: CERT/CC CSIRT FAQ

Internet in 1969



Source: https://www.darpa.mil/about-us/darpa-history-and-timeline?PP=2

Internet today



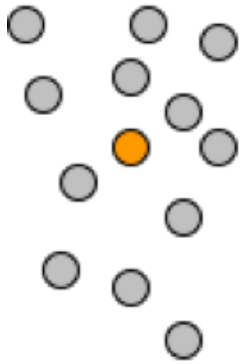
Source: https://www.caida.org/research/topology/as_core_network/2015/

Governance

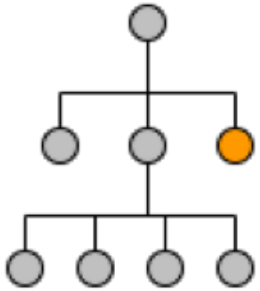
Governance is the use of institutions, structures of authority and collaboration to allocate resources and coordinate or control activity in society or the economy

(Patrick Kenis, Tilburg University)

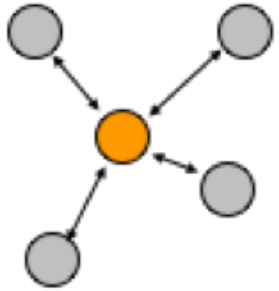
Market



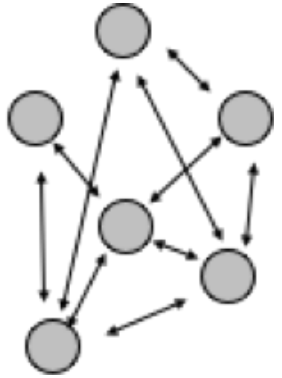
Hierarchy



Collaboration



Network



Network governance

*Governance [is achieved] through relatively **stable** cooperative relationships between three or more legally autonomous organizations **based on horizontal**, rather than hierarchical coordination, recognizing one or more network or **collective goals***

The late Elinor Ostrom receives the 2009 economic sciences Nobel price for her ground-breaking work: “Governing the Commons”.

Source: https://commons.wikimedia.org/wiki/File:Nobel_Prize_2009-Press_Conference_KVA-31.jpg

Main ingredients:

- **Common goals**
- **A high level of trust**

CSIRT History and Cooperation

- **CERT/CC was the first CSIRT, created in 1988 in response to the Morris worm incident**
- **CSIRTs form a cooperation network**
  - there is **no hierarchy**
  - the cooperation is **based on trust**
  - it helps organizations to improve their own security **and simultaneously this improves the whole Internet ecosystem security**
  - There are different types of CSIRTs. Their constituencies and services may differ, but they are **connected by their goals** of mitigating incidents on behalf of a constituency.

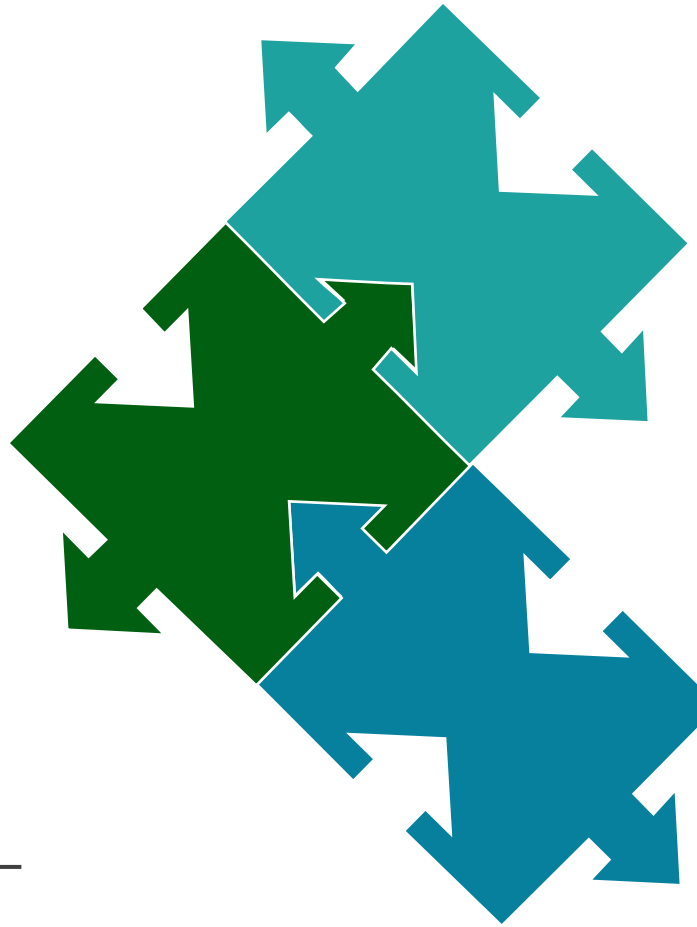
CSIRT History and Cooperation (cont.)

- **CSIRTs have been working together and sharing information for many years. Much of this is due to that most CSIRTs need to respond to similar threats.**
- **Success of a CSIRT is tied to correctly determining deliverables, and their perception with other stakeholders.**
- **Many best practices exist and are freely shared, resulting out of trusted relationships and existing collaboration.**
- **Cooperation is rooted in trust. Legislation does not provide trust, it is built up over time, by delivering what is needed.**
- **The role of the government is very delicate:**
  - **Top-down approaches from governments on creating CSIRTs do not always work well. A bottom up approach was preferred over top down development. Everything has to do with Trust.**
  - **Placement of the CSIRT in the ”wrong” place**

Existing CSIRT Forums

- APCERT, **Asia Pacific**
- AfricaCERT, **Africa**
- LAC-CSIRTs, **Latin America and Caribbean**
- OIC-CERT, **Organisation of The Islamic Cooperation**
- TF-CSIRT and EGC-CERT, **Europe**
- FIRST, **Global**
  - FIRST is an association with 489 Teams in 92 different countries.

FIRST Events:
Meet each other, share, learn, build trust



Symposium

- Four per year
- Typically in each major region (Africa, Europe, Latin America, Asia)
- Hosted by FIRST and often a partner

Conference

- Flagship event
- Once per year, travels between regions
- ~1000 attendees

Technical Colloquium

- Organized by individual members
- National or regional event
- Typically 10-15 events per year

Other Players

There are other organizations which have similar goals but different stakeholders.

- APWG is the international coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors and NGO communities.

- M3AAWG: The Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG) is where the industry comes together to work against bots, malware, spam, viruses, DoS attacks and other online exploitation.

¡Gracias!
Thank You!

www.cert.br

lucimara@cert.br @certbr

August 5, 2019

nic.br cgi.br

www.nic.br | www.cgi.br