CyberGreen

A global community to measure and improve cyberhealth

Improving Cyber Ecosystem Health through Metrics, Measurement and Mitigation Support

Dr. Paul Twomey

Chairman, CyberGreen Institute

September 2017, LACNIC 28, Montevideo

Points I will discuss

- Our vision of the Goal of Ecosystem Security
- Introduce CyberGreen's people and activities
- Outline types of metrics we measure
- Look at SSDP and IoT Distributed Denial of Service attacks
- Look at cases of improved performance in LACNIC countries.
- What can we all do to help mitigate the risk
- Ask for your practical help – including financial support for more data work.

CyberGreen

But first

- Congratulations to LACNIC!

CyberGreen

And a quick word from my sponsor…

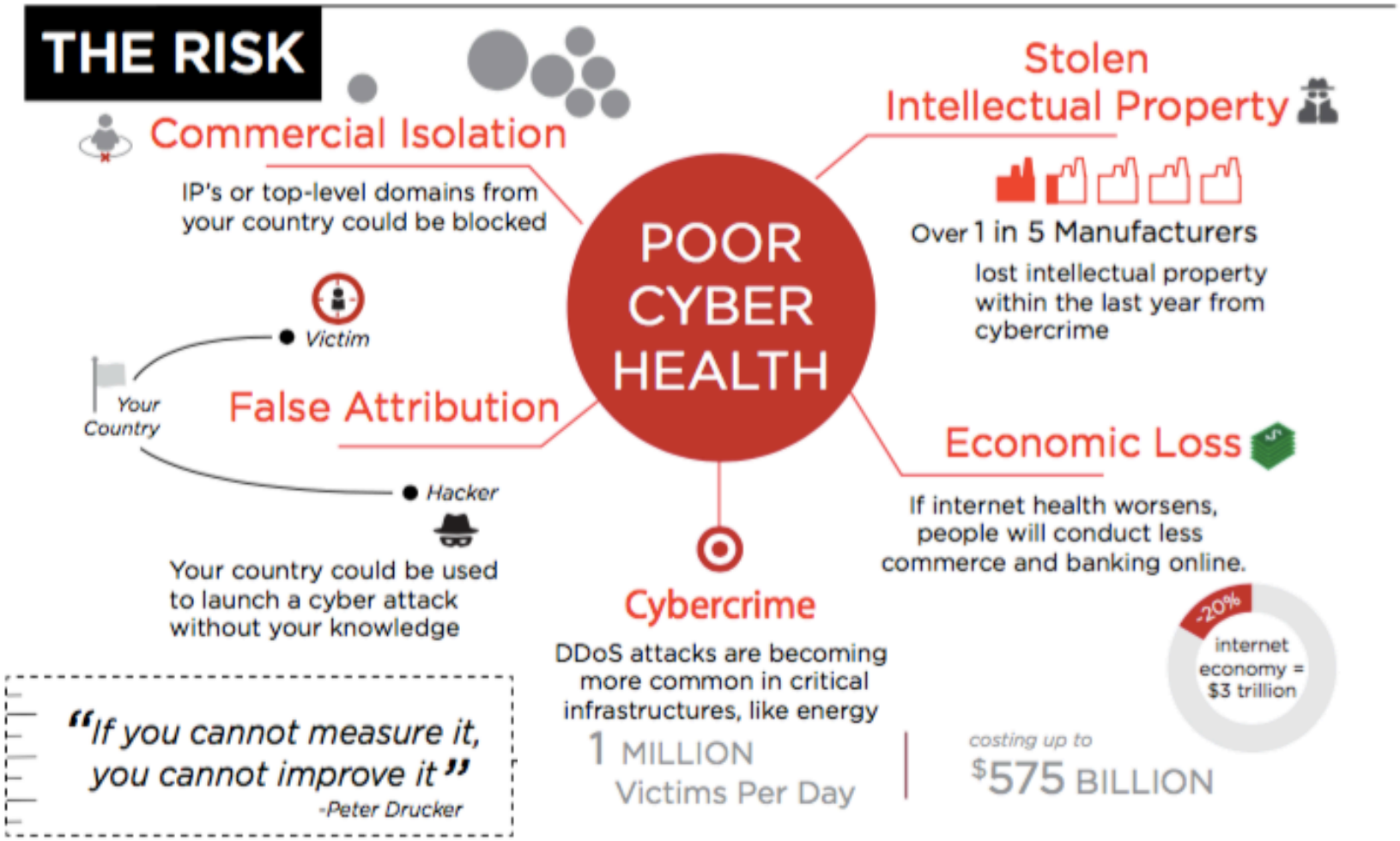
- www.stash.global
- Very secure data storage and content sharing as a SaaS offering.
- Working with North American ISPs
- Looking for partners in Latin America and the Caribbean

STASH®

Datacentric Security Technology

CyberGreen

Threat and Risks



CyberGreen

The "Big Picture" Goal

Increase security, safety, stability and resiliency of the

- Open, neutral, global Internet
- Infrastructure for economic and social prosperity

What do we need to do to achieve that?

- Improve the quality of the Cyber Ecosystem
  - *The **Cyber Ecosystem** is composed of any device which connects to the Internet, for example, but not limited to: clients, servers, virtual instances, embedded systems, and the Internet of Things.*

CyberGreen

How to make the Cyber Ecosystem healthier

Step 1: Understand and identify the systemic risks in your cyberspace (e.g. vulnerabilities, outdated devices, misconfigurations…)

Step 2: Mitigate the systemic risks through

- Policy implementation
- Technical mitigation at the network operation level (e.g. ISPs, corporations, end users…)

Step 3: Continue to monitor and measure the systemic risks

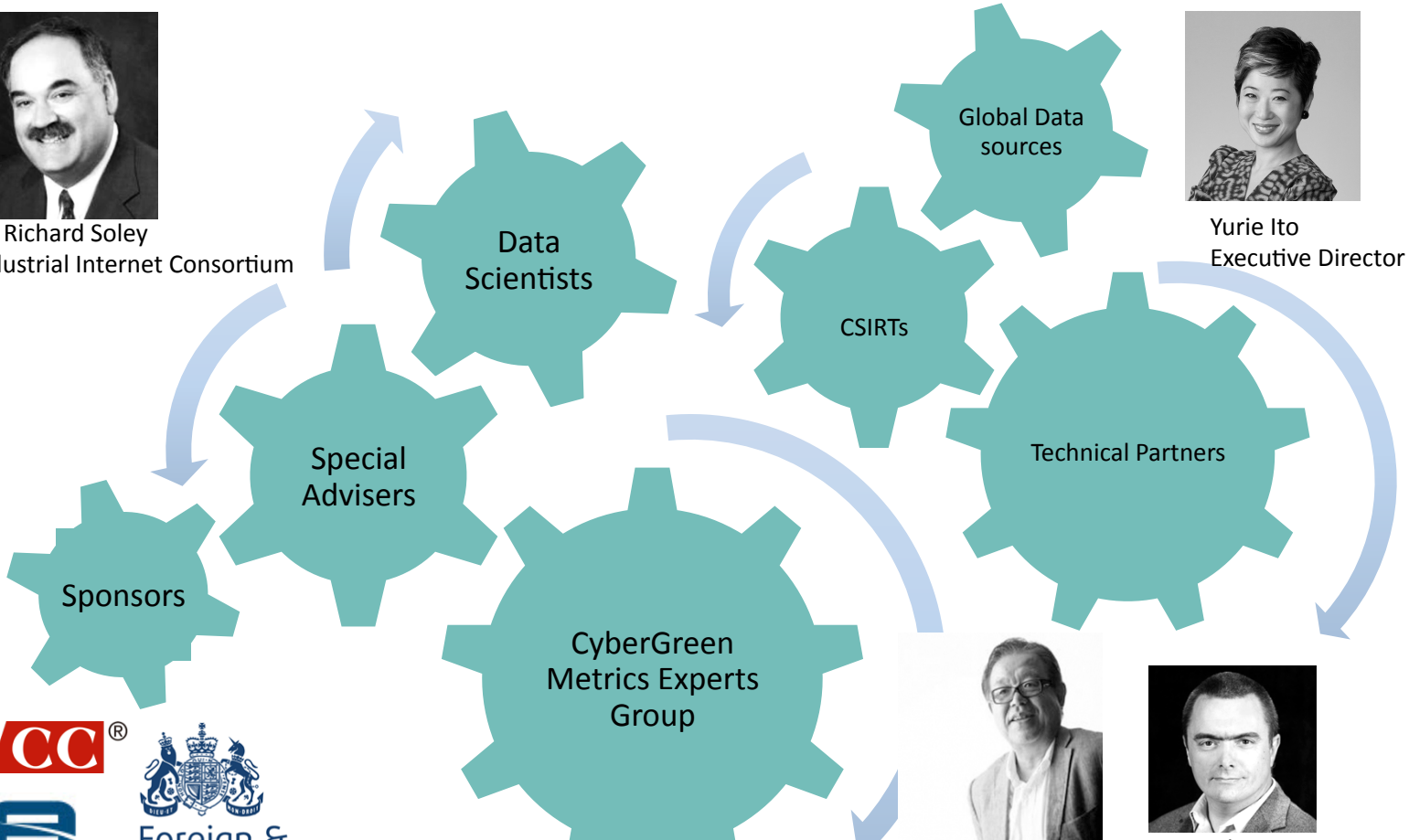
CyberGreen

CyberGreen: Who we are

Dr. Paul Twomey
Former ICANN CEO

Dr. Richard Soley
Industrial Internet Consortium

Dr. Dan Geer
Special Adviser on Metrics



Yurie Ito
Executive Director

Dr. Jun Murai
Dean, Keio University

Dr. Paul Vixie
Farsight Technology
(Special Adviser)

JPCERT CC®

CSA SINGAPORE

Foreign & Commonwealth Office

CyberGreen

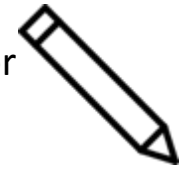
CyberGreen: What we do

Cyber Health Measurement.
We measure **Risk-to-others.**

Source risk condition data

Provide a clearinghouse for
Risk Mitigation BCPs.

Advocacy



Capacity Building
needs analysis and
impact measurement

CyberGreen

Using data to drive decisions

- CSIRTs: Prioritizing specific risks based on prevalence

- Management: Monitor improvement, analyze mitigation impact and ROI

- Policymakers: Analyze and formulate policy

CyberGreen

Poor maintenance = risk to others AND yourself

Risks that make the Cyber Ecosystem unhealthy:

Misconfiguration

Infection

Vulnerabilities

CyberGreen

DDoS and the emergence of IoT

- Fundamentally, DDoS attack and defense is about
  - What defender can handle
  - What attacker can launch
- IoT adds unique problems
  - New community of developers repeat the mistakes of the last 40 years
  - Systems are often unmaintainable, unpatchable → 'cheaper to throw out than fix'
  - Nobody knows where these devices are; you can't protect what you can't see
  - Lots of copied and pasted code, vulnerabilities spread along supply chain

<u>Techniques used:</u>

- 1980s – Black faxes, junk mail
- 1990s – Smurfing, Ping of Death
- 2000s – Botnets
- Mid-2000's – purpose-built botnets (LOIC, HOIC), SlowLoris
- 2010's – Reflection attacks, IoT

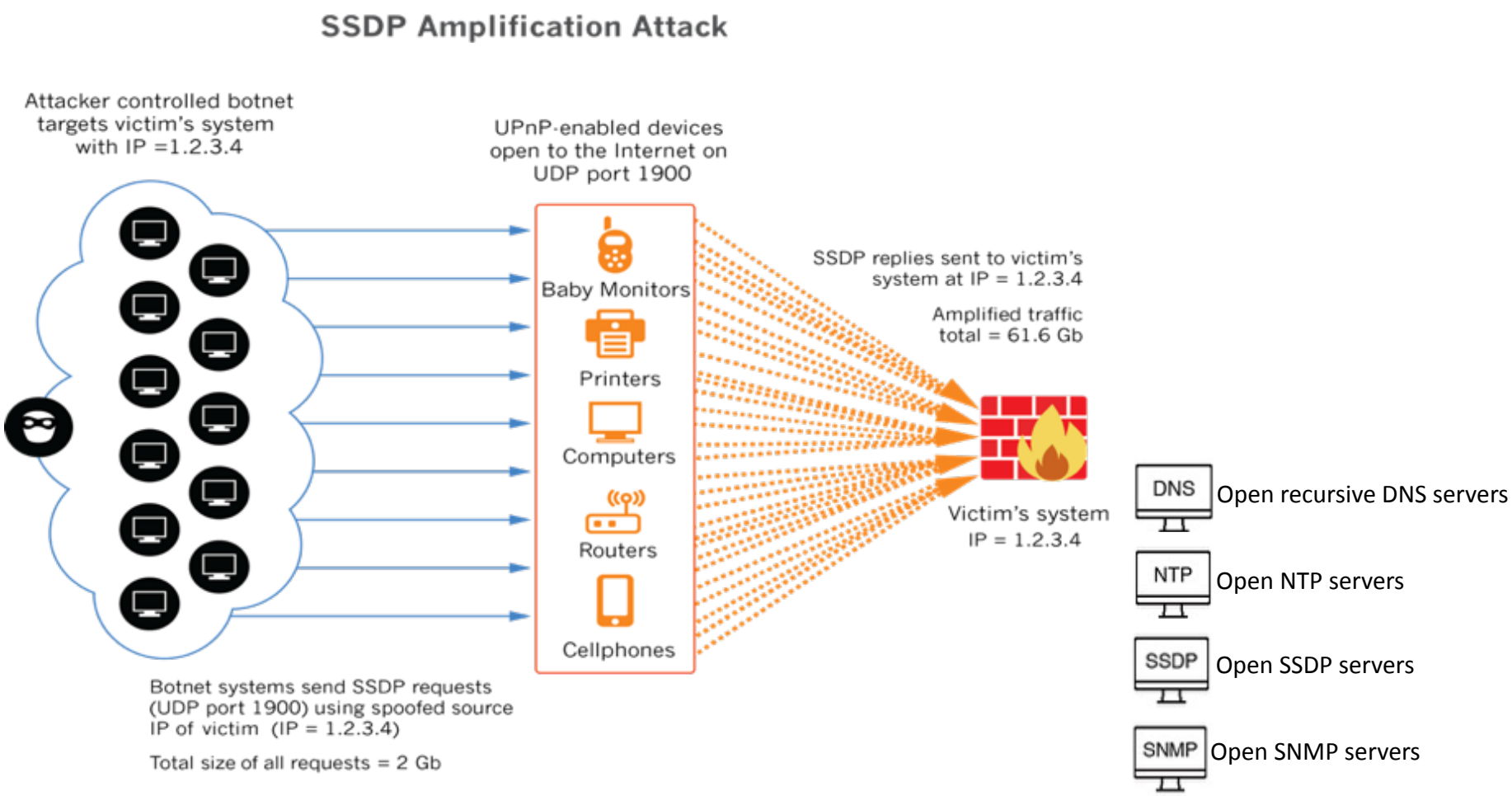
CyberGreen

Why focus on SSDP?

- SSDP: **S**imple **S**ervice **D**iscovery **P**rotocol
- Common protocol in IoT, can be used to launch reflection attacks
- Can be identified using scanning tools and analyzed using data and metrics (i.e. CyberGreen)

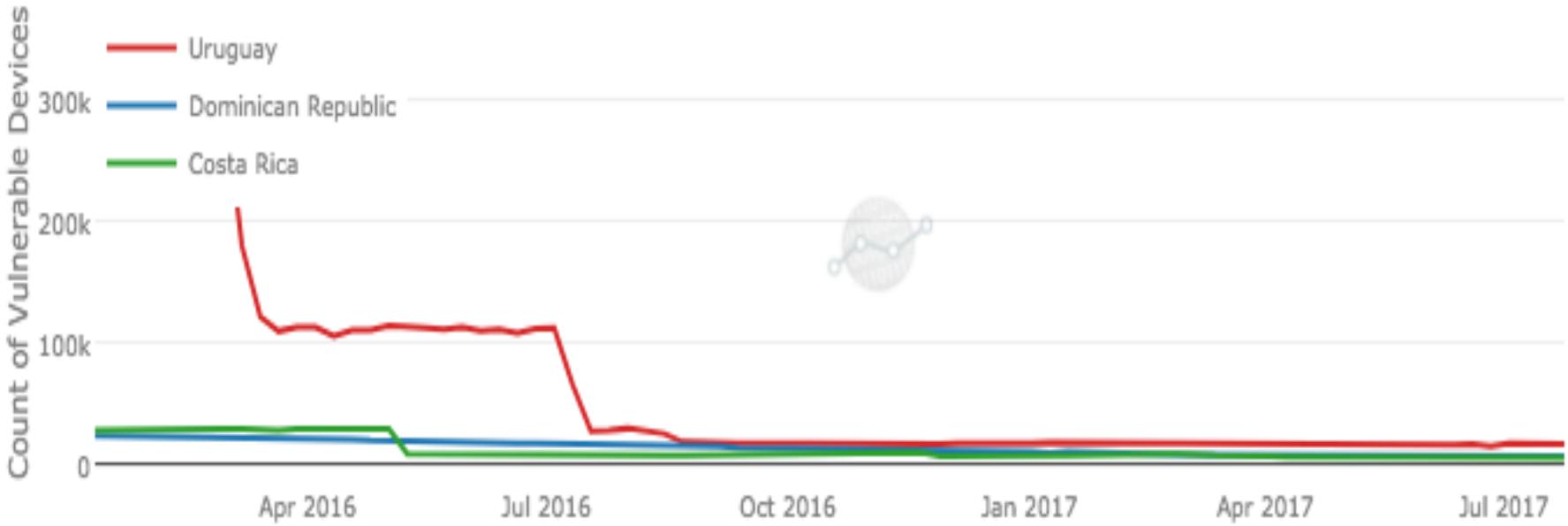
CyberGreen

Abuse-able systemic conditions posing risks to others *including to yourself*



CyberGreen

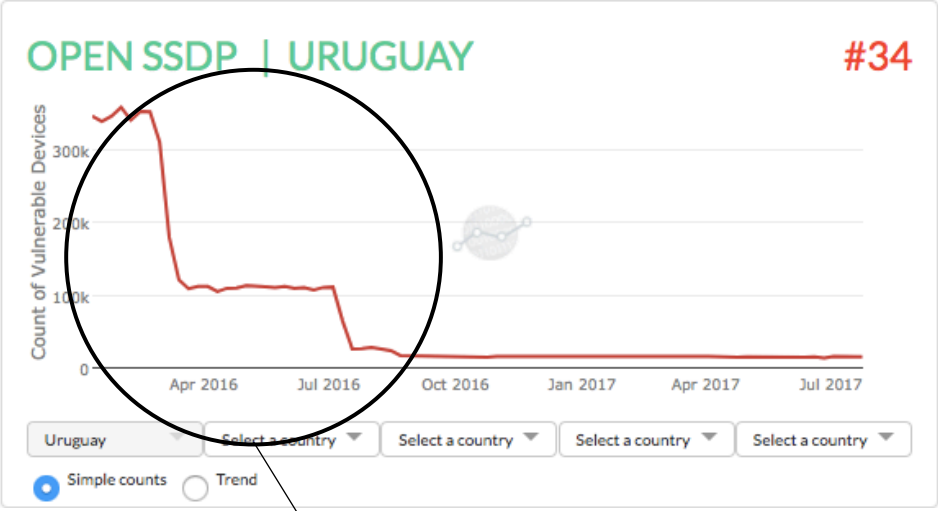
Trends for 3 LACNIC Countries

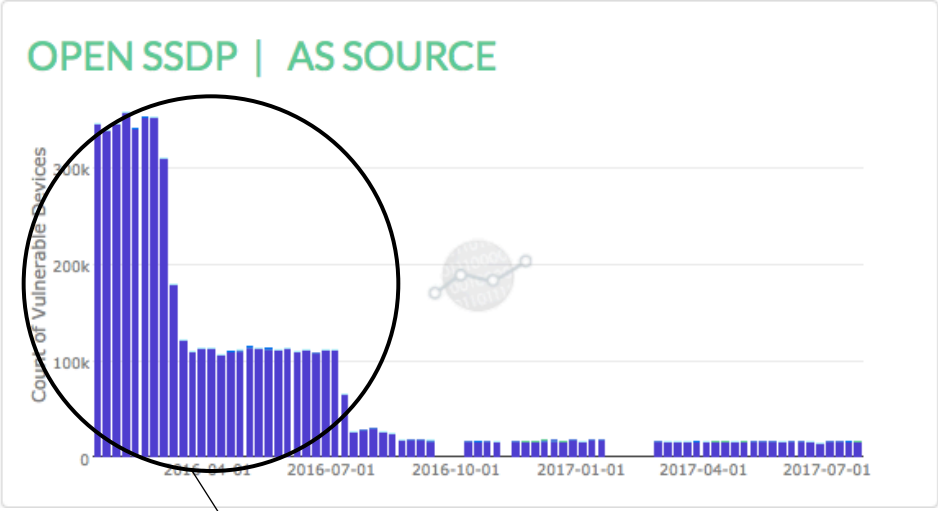


- Raw counts for open SSDP devices/servers (not normalized)
- Can be difficult to understand trends when comparing three countries with different IP spaces

CyberGreen

SSDP Trend: Uruguay (S. America)





NATIONAL LEVEL

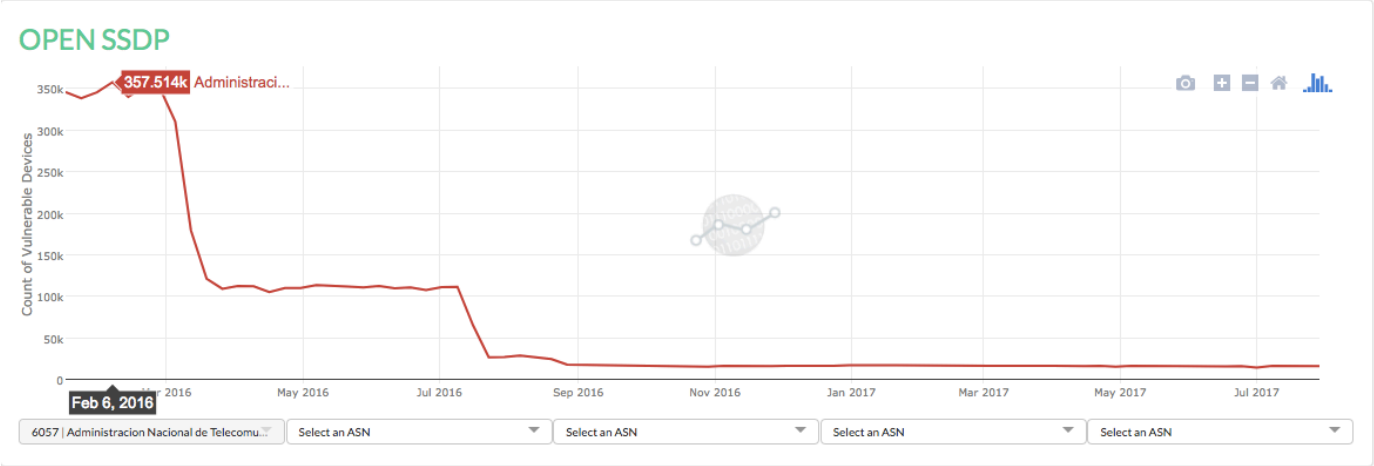
- Nice reduction in open SSDP servers
  - What caused it?
  - How can we spread the word and make it a best practice?

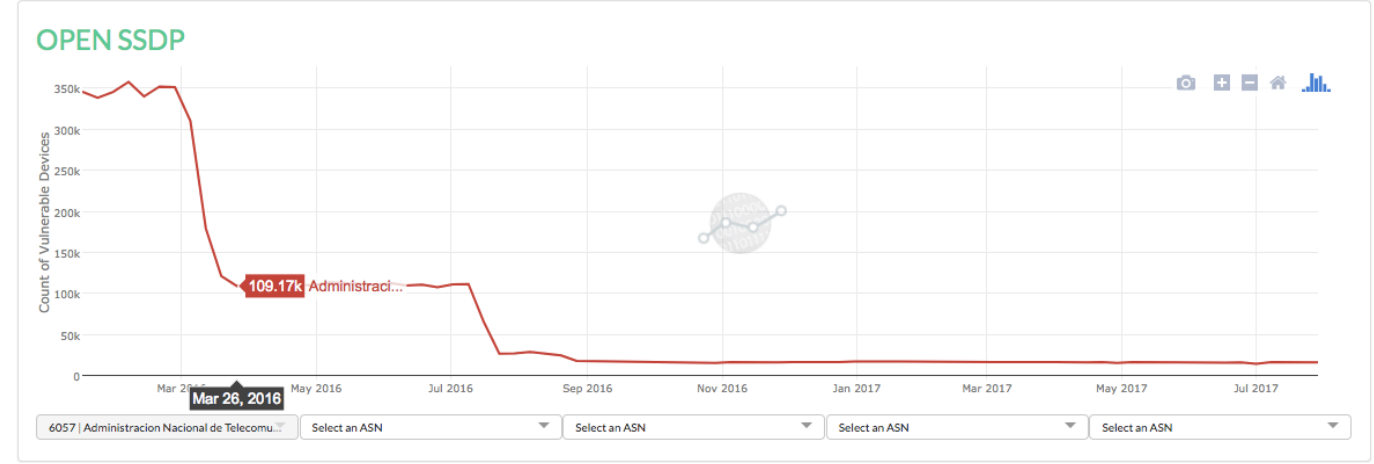
AS LEVEL

- Which Autonomous System(s) were primarily responsible for the decrease in open SSDP servers?
- How can we get in touch with them to find out more?

CyberGreen

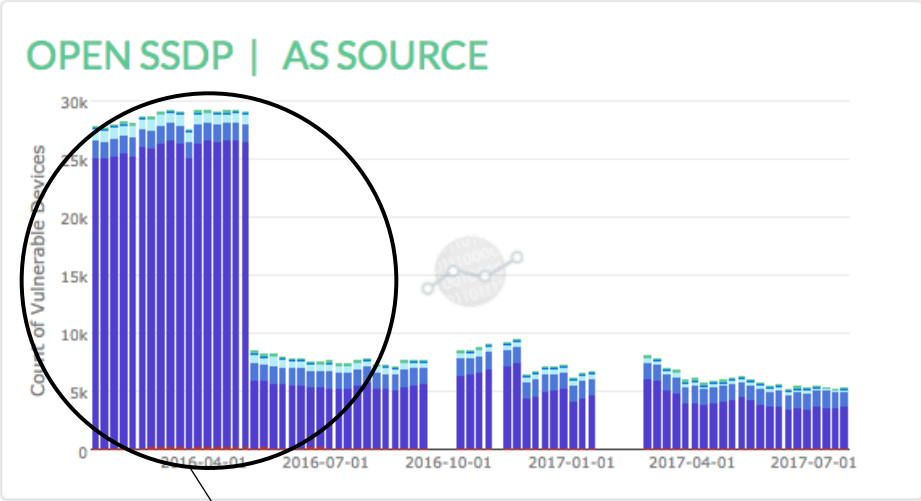
AS Uruguay - 6057
Administracion Nacional de Telecomunicaciones





CyberGreen

SSDP Trend: Costa Rica (C. America)



NATIONAL LEVEL

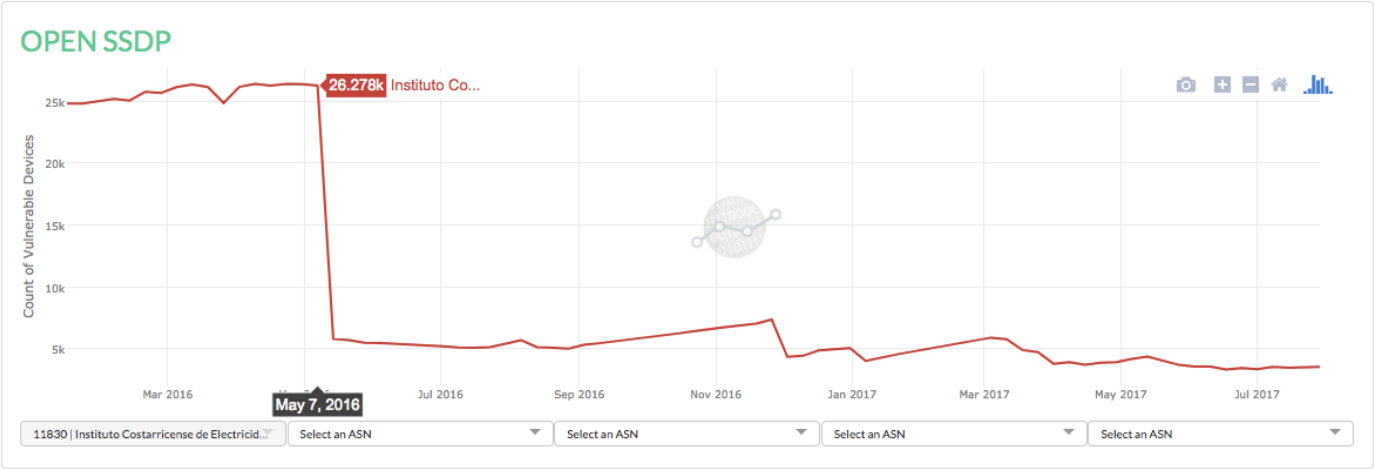
- Nice reduction in open SSDP servers
  - What caused it?
  - How can we spread the word and make it a best practice?

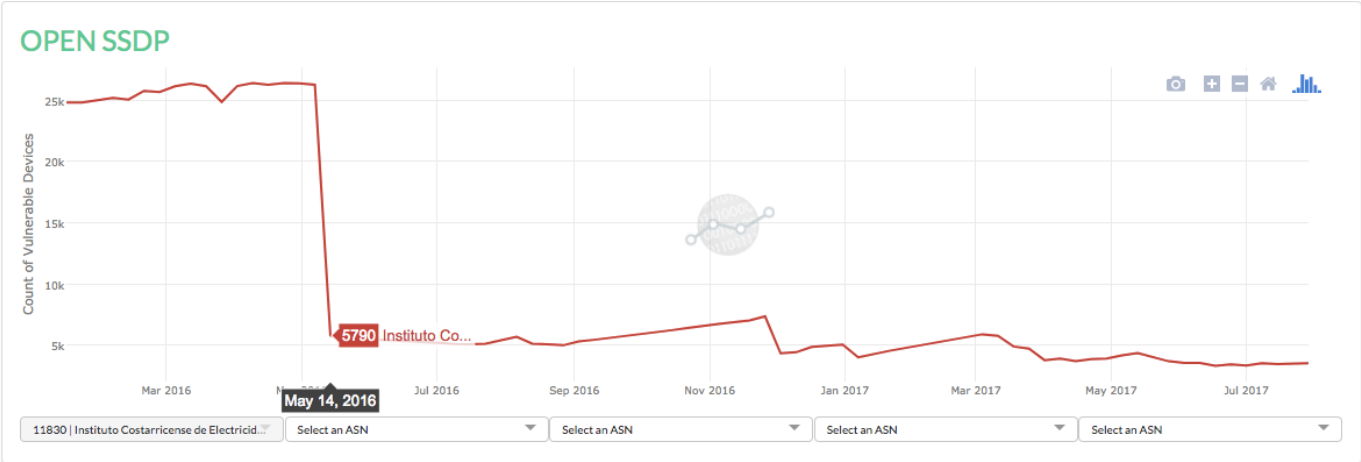
AS LEVEL

- Which Autonomous System(s) were primarily responsible for the decrease in open SSDP servers?
- How can we get in touch with them to find out more?

CyberGreen

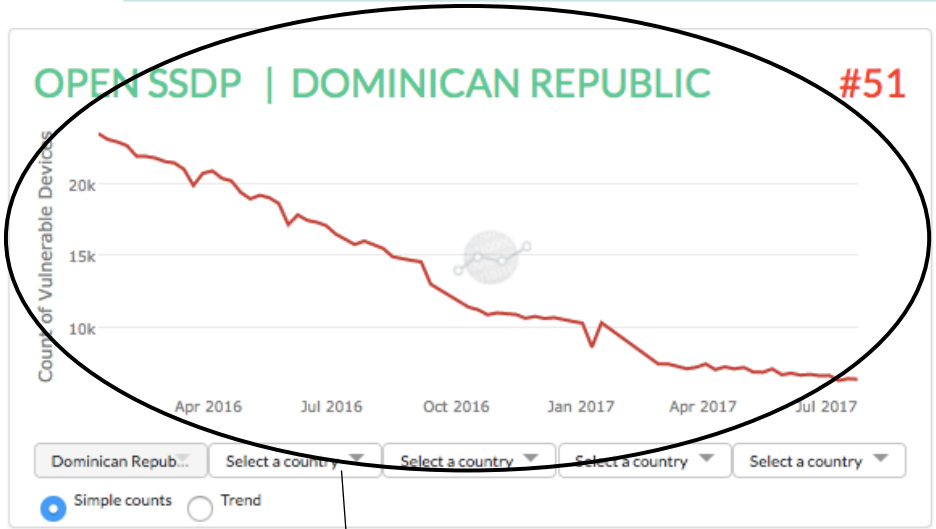
AS Costa Rica - 11830
Instituto Costarricense de Electricidad y Telecom.

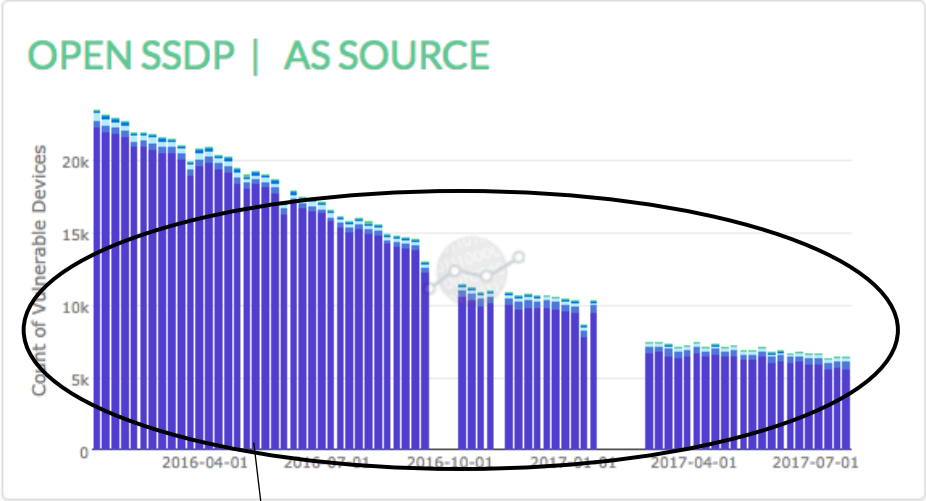




CyberGreen

SSDP Trend: Dominican Republic (Caribbean)





NATIONAL LEVEL

- Nice reduction in open SSDP servers
  - What caused it?
  - How can we spread the word and make it a best practice?

AS LEVEL

- Which Autonomous System(s) were primarily responsible for the decrease in open SSDP servers?
- How can we get in touch with them to find out more?

CyberGreen

AS Costa Rica - 11830
Instituto Costarricense de Electricidad y Telecom.

CyberGreen

Greater Impact of Mitigation for Global Common Good

Efforts to improve Cyber Ecosystem health by eliminating proxy attack infrastructure would:

- **National level** → build confidence
- **Business level** → increase social responsibility, branding power
- **End user level** → indicate high degree of maturity of cyber society, educational and awareness level

CyberGreen

What can network operators do?

- Review CyberGreen statistics for your country/AS: https://stats.cybergreen.net/
- Download CyberGreen capacity building/mitigation materials: https://www.cybergreen.net/mitigation/

Capacity Building Materials

Download CyberGreen's mitigation best current practices for three risk conditions that are present in the Cyber Ecosystem.

Download Open SSDP

Download Open NTP

Download Open DNS

Download SpamBot

CyberGreen

Current and future metrics at CyberGreen

- Current metrics are asset owner focused
- Next version of metrics will focus on IoT device health

CyberGreen seeks sponsorship and support for research and development of its metrics.

Please contact us to find out how you can help!

contact@cybergreen.net

CyberGreen

CyberGreen

Help us foster the CyberGreen approach.

Participate in the mitigation campaign.

Together, we can develop a success case for the LACNIC region and global community in the next 12 months.

Email:

contact@cybergreen.net

The public policy challenge

The problem: Lack of incentive for network operators/ device vendors to ensure improved cyber security practices in their operations.

The result: Market failures and a large global base of vulnerable servers, IoT devices, etc. which can be used as attack infrastructure.

CyberGreen

What can policymakers do?

- Promote transparency in the supply chain and labeling to reveal distinctions among market alternatives.
- Coordinate on an internationally consistent IoT/ Software Bill of Materials which contains no known vulnerabilities.
- Require that IoT devices be patchable.
- Legally require vendors and/or ISPs to offer life-long security updates
- Engage citizenry with educational materials on IoT safety.

CyberGreen