Internet Infrastructure Initiative

Triple I: a GFCE Capacity-building project

#AISDakar, 7 May 2018

(maarten@gnksconsult.com)

Global Forum on Cyber Expertise (GFCE)

Ambition: to become the global platform where public and private companies exchange expertise and best practices on cyber capacity building.

Organisation: such international cooperation currently takes mostly place via bilateral relations or in a regional setting.

Offering: a platform to effectively cooperate on a global level that is pragmatic, action oriented and flexible.

Aim: to develop practical initiatives in order to:

- take advantage of opportunities in cyberspace, and:
- overcome evolving challenges in the field.

Global Risks Report 2018

“… this generation enjoys unprecedented technological, scientific, and financial resources, which we should use to chart a course towards a more sustainable, equitable and inclusive future.

At the same time, the risks are greater than ever, with an important role for disruptive technologies that may be used to affect societies in good and bad ways, and with cyberattacks amongst today’s biggest threats to disrupt society.”

WORLD ECONOMIC FORUM

Internet Infrastructure Initiative

- Aim: to help build a robust, transparent and resilient internet infrastructure.
- Rationale: A robust, open and resilient internet infrastructure is key to counter infringements and threats to the cyber domain, and:
  - diminishes the chances and impact of cyber-attacks (like DDoS) and cybercrime (hacking malware, phishing, botnets) and SPAM.
  - enables the public to maintain confidence and trust;
  - is a precondition for the use of the internet as a means to boosting innovative and economic activities.
- Offering: this Initiative seeks to deepen and broaden the know-how in locally applying, testing and monitoring compliance with widely agreed open internet standards.
  - Key elements include national internet infrastructure protection, internet exchange points, registries, open source software, email security and routing security.

Focus on accepted Open Internet Standards

- DNSSEC
- TLS
- DANE
- IPv6

- DMARC
- DKIM
- SPF
- …

Setting up Capacity building events

➢Targeted at regions that are catching up

➢Bringing together regional stakeholders

➢Awareness raising on Open Internet Tools

➢Inspiration through Good Practice Examples

➢Impact through joint commitment for action

GFCE

Help make the Internet more reliable in your region

1. Contribute with good practice examples to events

2. Support an event in your region as co-organizer or participant

3. Improve the reliability of Internet by taking action

Supported by global and regional stakeholders

- GFCE members
  - Governments
  - International Organisations
  - Businesses
- Regional Internet Registries
  - All regions
- Internet Society
  - Global office
  - Local chapters
- NL Ministry of Economic Affairs

AGENDA

11:30	Block I: Better Use of Today’s Open Internet Standards
13:00	Lunch
14:00	Block II: Inspiration from Good Practice Actions
16:00	Block III: Action Planning for a More Trusted Internet
17:30	Conclusions and Closing Remarks

From State-of-Practice to State-of-the-Art, together

Joint priority setting and action planning following the Open Space method

"What to do to improve justified trust in using the Internet and email in the region"

Purpose of the Day

Open Space Method

- All of the issues that are most important to those attending will be raised and included in the agenda: YOU set the agenda.
- All of the issues raised will be addressed by the participants best capable of getting something done about them: YOU choose to which issues you contribute.
- All of the most important ideas, recommendations, discussions, and next steps will be documented in our meeting report.
- Taking into account the time we have we will identify the “Top 5”.
- You may decide to form a group to draft action plans for the highest priority issues, after the workshop.

Success formulae

1. Power of the coffee machine: why is gathering around the coffee machine such an important contribution to developing a business? People gather without an agenda and discuss what is most prevalent.
2. *Law of Two Feet: when there is nothing more to contribute to a conversation, use your feet and walk on to join the conversation about another issue.*
3. Be concise, and don’t get lost in “stories” – it is all about *purpose* and *approach*

The Four Principles

Every issue of any importance, to any person willing to take some responsibility for it, gets posted on the community bulletin board, the *Marketplace wall.*

Please use one of the A4's and a marker and also put your name on it!

Remember:

1. *Whoever comes is the right people.*
2. *Whatever happens is the only thing that could have.*
3. *Whenever it starts is the right time.*
4. *When it is over, it is over.*

At 16:30 we start the Market

Be there to explain your idea and to get input – or to provide input to one or more ideas that you want to contribute to.

Triple I is a GFCE project

www.thegfce.com

For more information contact:
maarten@gnksconsult.com

About Maarten Botterman

- More than 25 years experience with work “in the public interest”: where connected technologies touch society - internationally
- Independent analyst, strategic advisor, moderator and chairman, see for more: www.gnksconsult.com
- Currently chairing: IGF Dynamic Coaltion on Internet of Things (www.iot-dynamic-coalition.org/); PICASSO Policy Expert Group (www.Picasso-project.eu), and Supervisory Board of NLnet Foundation (www.nlnet.nl.)
- ICANN Board Member (www.icann.org)
- Full CV: https://www.linkedin.com/in/botterman
- Email: maarten@gnksconsult.com

CyberGreen

A global community to measure and improve cyberhealth

Improving Cyber Ecosystem Health through Metrics, Measurement and Mitigation Support

GFCE workshop, Senegal

May, 7, 2018

The CyberGreen Institute is a global non-profit organization focused on helping to improve the health of the global Cyber Ecosystem.

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

Conduct weekly Internet scans for risk condition data

Provide a clearinghouse for Risk Mitigation BCPs.

Capacity Building needs analysis and impact measurement

Advocacy

We work with partners, including governments, seeking to address Cyber Risks.

Sponsors

JPCERT CC®

Foreign & Commonwealth Office

CSA SINGAPORE

Collaborators

AfricaCERT
United in promoting cyber security in Africa

APNIC

FARSIGHT SECURITY

GLOBAL CYBER ALLIANCE

GFCE

RCC
المركز العربي الإقليمي للأمن السيبراني
ITU - ARAB REGIONAL CYBERSECURITY CENTER

APWG

ICANN

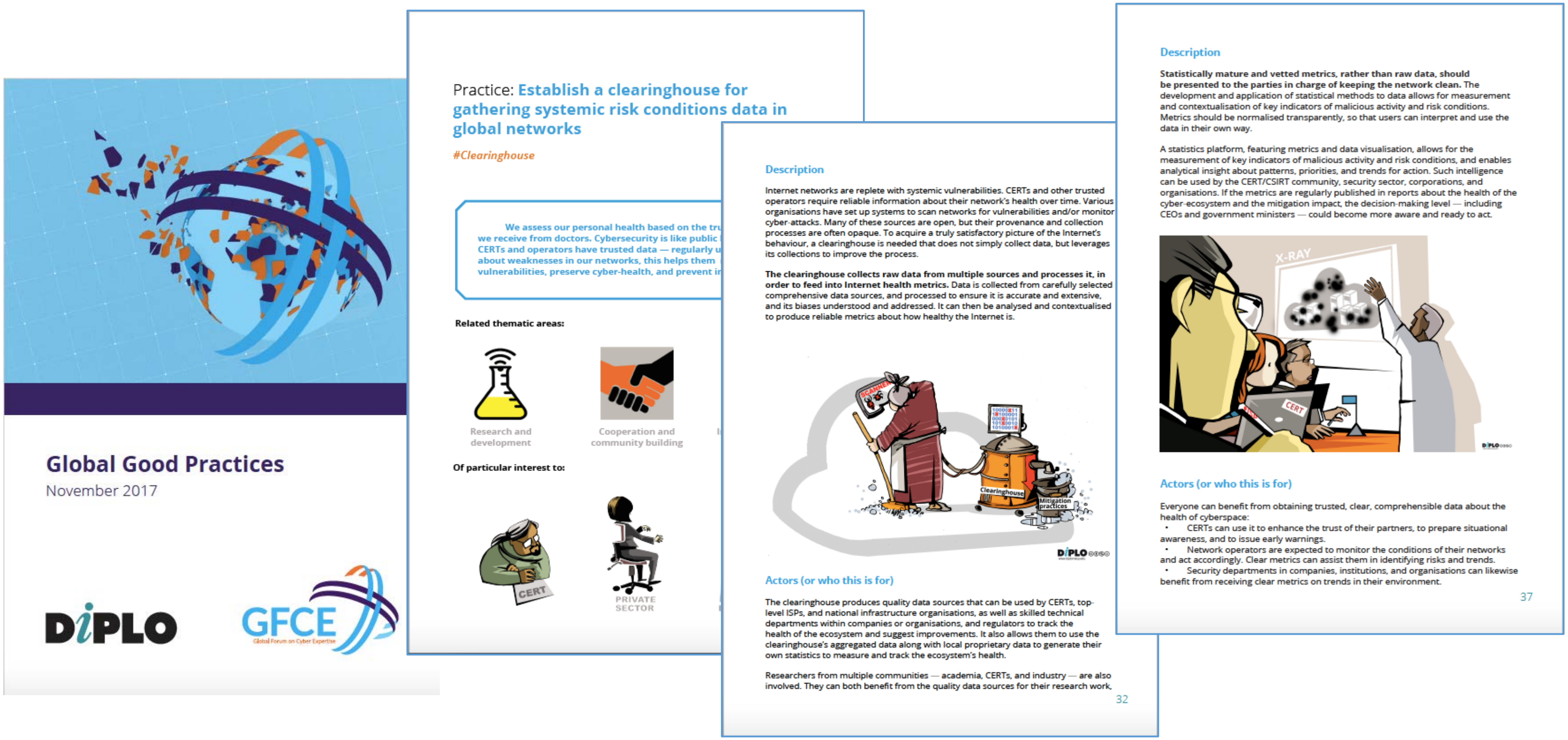
APCERT
Asia Pacific Computer Emergency Response Team

Internet Society

OIC-CERT
Computer Emergency Response Team

Recognized as Global Good Practice

presented at GFCE / GCCS conference in New Delhi
https://www.thegfce.com/good-practices/incident-capture-and-analytics



Global Good Practices
November 2017

Practice: **Establish a clearinghouse for gathering systemic risk conditions data in global networks**

#Clearinghouse

We assess our personal health based on the tru
we receive from doctors. Cybersecurity is like public
CERTs and operators have trusted data — regularly u
about weaknesses in our networks, this helps them
vulnerabilities, preserve cyber-health, and prevent in

Related thematic areas:

Research and development

Cooperation and community building

Of particular interest to:

Description

Internet networks are replete with systemic vulnerabilities. CERTs and other trusted operators require reliable information about their network's health over time. Various organisations have set up systems to scan networks for vulnerabilities and/or monitor cyber-attacks. Many of these sources are open, but their provenance and collection processes are often opaque. To acquire a truly satisfactory picture of the Internet's behaviour, a clearinghouse is needed that does not simply collect data, but leverages its collections to improve the process.

The clearinghouse collects raw data from multiple sources and processes it, in order to feed into Internet health metrics. Data is collected from carefully selected comprehensive data sources, and processed to ensure it is accurate and extensive, and its biases understood and addressed. It can then be analysed and contextualised to produce reliable metrics about how healthy the Internet is.

Actors (or who this is for)

The clearinghouse produces quality data sources that can be used by CERTs, top-level ISPs, and national infrastructure organisations, as well as skilled technical departments within companies or organisations, and regulators to track the health of the ecosystem and suggest improvements. It also allows them to use the clearinghouse's aggregated data along with local proprietary data to generate their own statistics to measure and track the ecosystem's health.

Researchers from multiple communities — academia, CERTs, and industry — are also involved. They can both benefit from the quality data sources for their research work,

32

Description

Statistically mature and vetted metrics, rather than raw data, should be presented to the parties in charge of keeping the network clean. The development and application of statistical methods to data allows for measurement and contextualisation of key indicators of malicious activity and risk conditions. Metrics should be normalised transparently, so that users can interpret and use the data in their own way.

A statistics platform, featuring metrics and data visualisation, allows for the measurement of key indicators of malicious activity and risk conditions, and enables analytical insight about patterns, priorities, and trends for action. Such intelligence can be used by the CERT/CSIRT community, security sector, corporations, and organisations. If the metrics are regularly published in reports about the health of the cyber-ecosystem and the mitigation impact, the decision-making level — including CEOs and government ministers — could become more aware and ready to act.

Actors (or who this is for)

Everyone can benefit from obtaining trusted, clear, comprehensible data about the health of cyberspace:

- CERTs can use it to enhance the trust of their partners, to prepare situational awareness, and to issue early warnings.
- Network operators are expected to monitor the conditions of their networks and act accordingly. Clear metrics can assist them in identifying risks and trends.
- Security departments in companies, institutions, and organisations can likewise benefit from receiving clear metrics on trends in their environment.

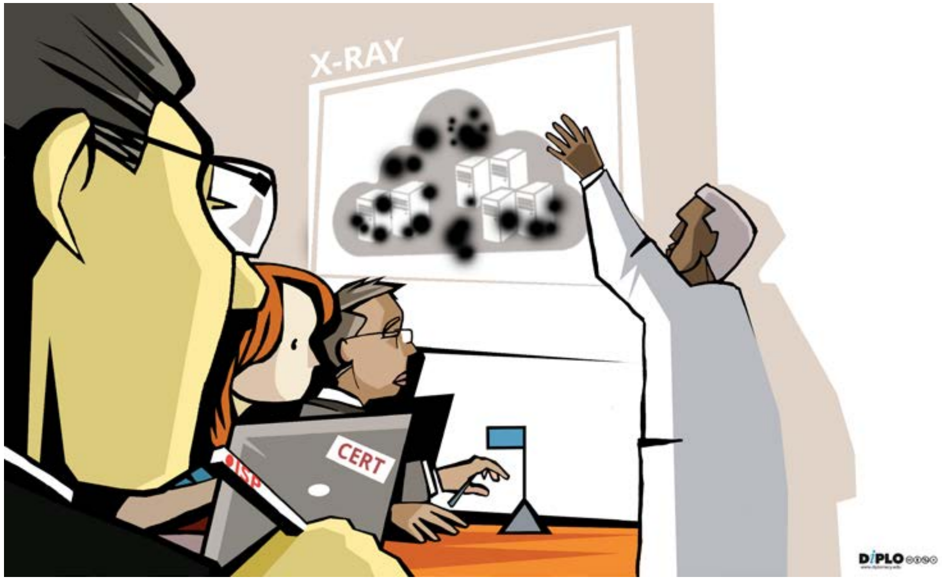
37

p.31-35: Establish a clearing house for gathering systemic risk conditions data in global networks
p.36-40: Produce and present trusted metrics about systemic risk conditions
p.41-44: Assist with cyber-risk mitigation and keep score of successes

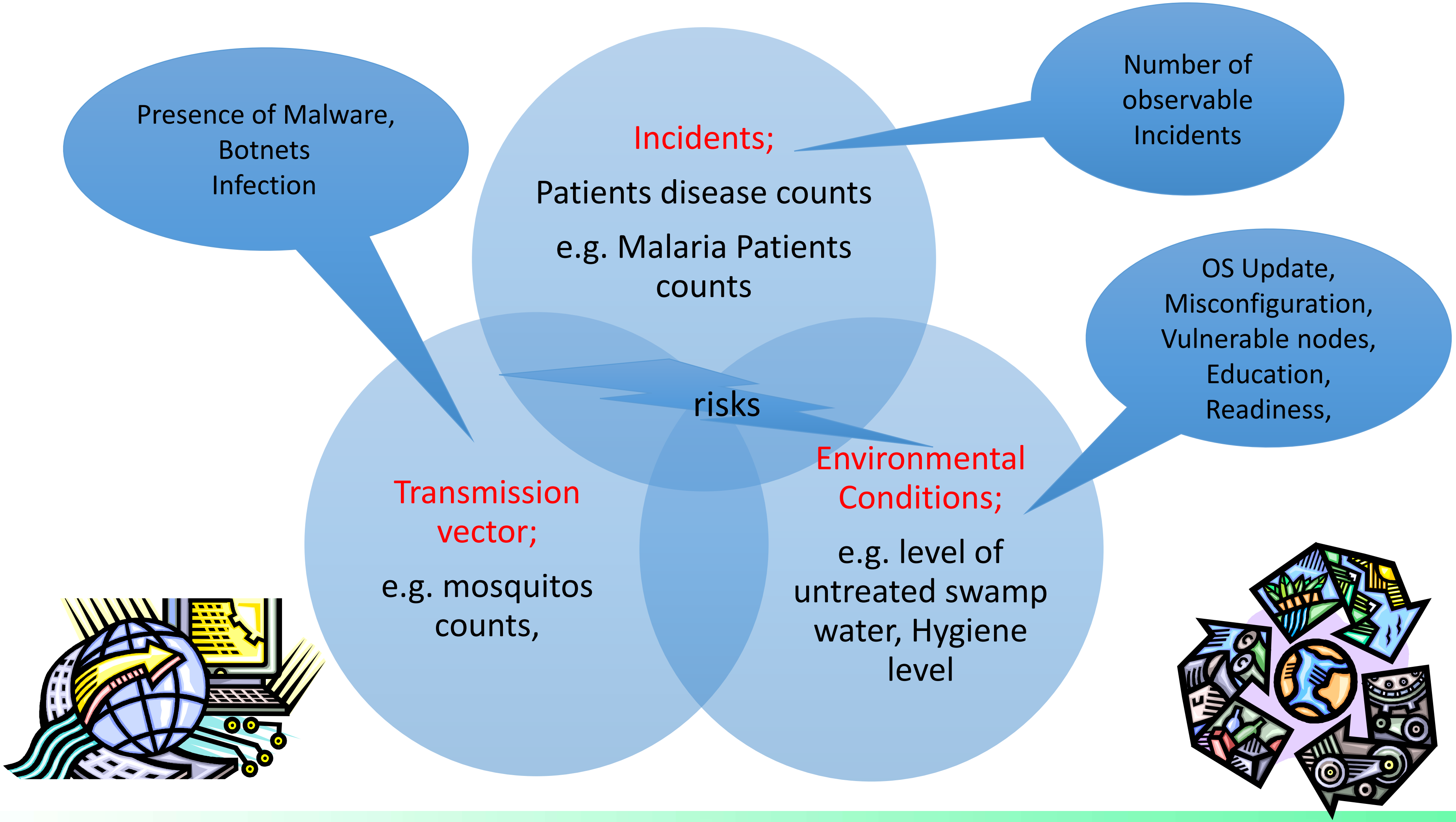
Key Questions

- Do you know the state of your cyber ecosystem health of your country?

- Do you know how to improve it? And it’s impact?



Applying Public Healthcare approach into Cyber



Presence of Malware,
Botnets
Infection

Incidents;

Patients disease counts

e.g. Malaria Patients counts

Number of observable Incidents

risks

Transmission vector;

e.g. mosquitos counts,

Environmental Conditions;

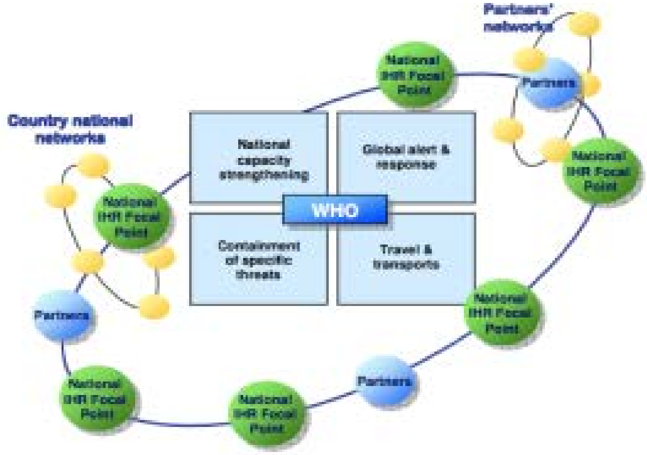
e.g. level of untreated swamp water, Hygiene level

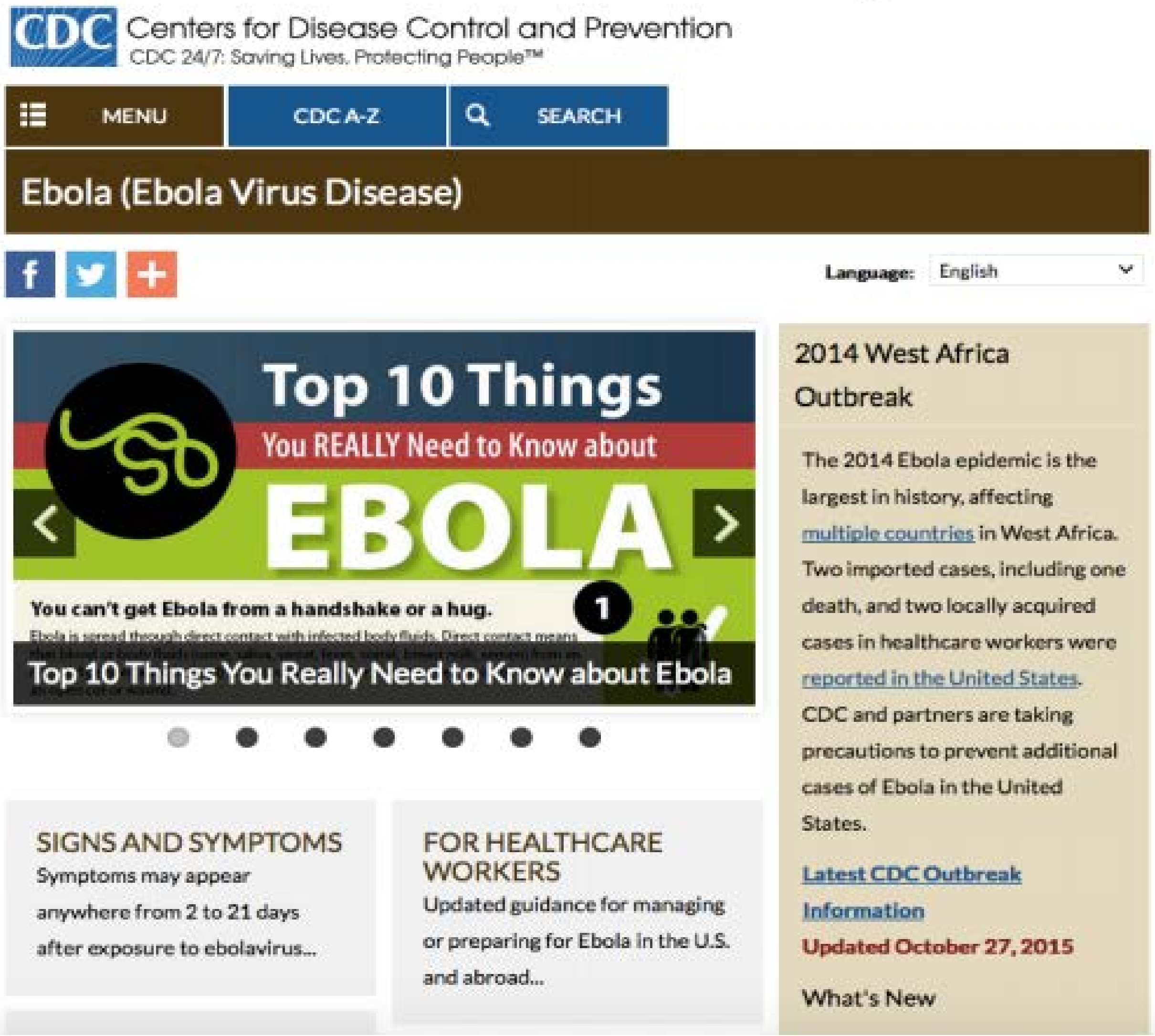
OS Update,
Misconfiguration,
Vulnerable nodes,
Education,
Readiness,

Lack of understanding of State of health, risks and measurement for Cyber Ecosystem

Public healthcare analogy

igure 3.1
nternational public health security: a global network of national health systems a echnical partners, focused on four major areas of work, coordinated by WHO




CDC
Centers for Disease Control and Prevention
CDC 24/7: Saving Lives. Protecting People™
MENU
CDC A-Z
SEARCH
Language: English

Ebola (Ebola Virus Disease)

Top 10 Things
You REALLY Need to Know about
EBOLA
You can't get Ebola from a handshake or a hug.
1

Top 10 Things You Really Need to Know about Ebola

2014 West Africa Outbreak

The 2014 Ebola epidemic is the largest in history, affecting multiple countries in West Africa. Two imported cases, including one death, and two locally acquired cases in healthcare workers were reported in the United States. CDC and partners are taking precautions to prevent additional cases of Ebola in the United States.

Latest CDC Outbreak Information

Updated October 27, 2015

What's New

SIGNS AND SYMPTOMS

Symptoms may appear anywhere from 2 to 21 days after exposure to ebolavirus...

FOR HEALTHCARE WORKERS

Updated guidance for managing or preparing for Ebola in the U.S. and abroad...

CyberGreen: What we measure

Type	Description
Open DNS	Domain Name System (DNS) is a standard protocol that translates human-friendly host names like www.cybergreen.net into numerical, Internet Protocol (IP) addresses such as 197.222.126.114 DNS can have an amplification factor of up to 179. In other words: 1 Byte turns into 179 Bytes in DDOS traffic.
Open NTP	Network Time Protocol (NTP) is standard protocol for time synchronization for devices on a network, used by servers, mobile devices, endpoints and networking devices from all vendors. NTP has an amplification factor of 556.9.
Open SNMP	Simple Network Management Protocol is for collecting and organizing information about devices on networks, including cable modems, routers, switchers, servers, printers etc. SNMP has an amplification factor of 6.3.
Open SSDP	Simple Service Discovery Protocol (SSDP) is the standard search protocol for Universal Plug and Play (UPnP) UPnP is pervasive - it is enabled by default on home gateways, network printers, webcams, network storage servers, and "smart home" devices such as thermostats, automated assistants and wireless home security systems that are part of the Internet of Things (IoT). SSDP's amplification factor is ~ 30.

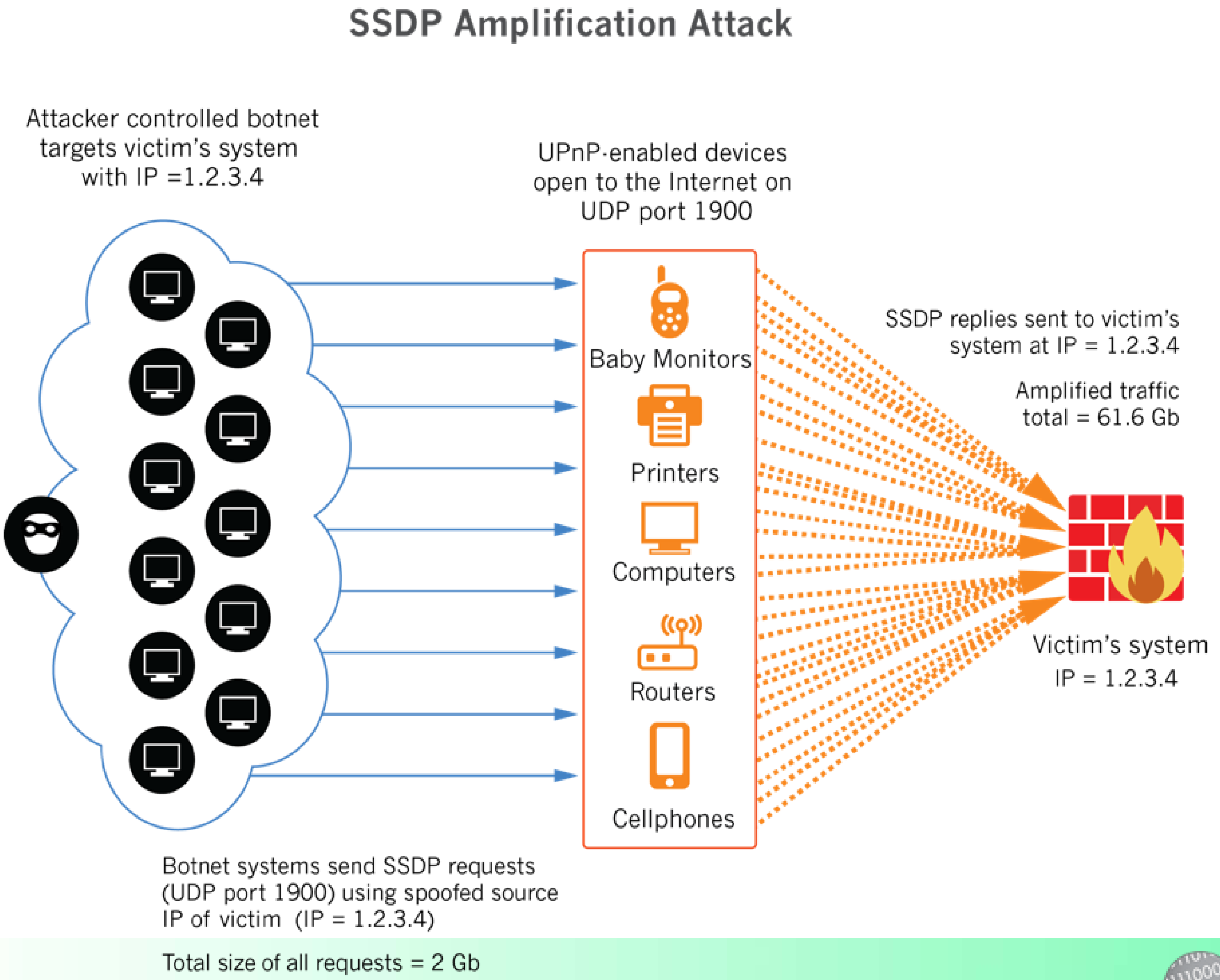
What are open recursive resolvers?

“Open recursive resolvers” are recursive resolvers (DNS servers) that will send a reply to any IP address

- Even about domains for which that DNS server is **not** an authoritative DNS server

Recursion is often on by default when DNS servers are first set up

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



SSDP Amplification Attack

Attacker controlled botnet targets victim's system with IP =1.2.3.4

UPnP-enabled devices open to the Internet on UDP port 1900

Baby Monitors

Printers

Computers

Routers

Cellphones

SSDP replies sent to victim's system at IP = 1.2.3.4

Amplified traffic total = 61.6 Gb

Victim's system IP = 1.2.3.4

Botnet systems send SSDP requests (UDP port 1900) using spoofed source IP of victim (IP = 1.2.3.4)

Total size of all requests = 2 Gb

DNS Open recursive DNS servers

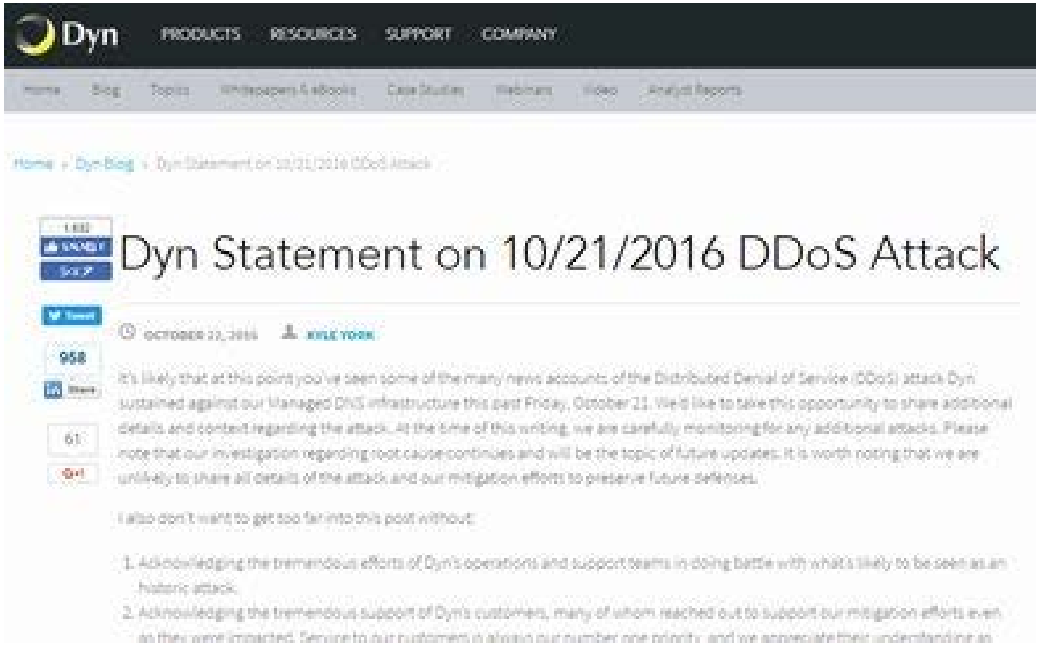
NTP Open NTP servers

SSDP Open SSDP servers

SNMP Open SNMP servers

DDoS attack against DynDNS October 21, 2016

- Mirai Bot infected IoT devices
- Twitter, Spotify, Reddit, netflix, Wall Street Journal, Github… and other major services down



Dyn Statement on 10/21/2016 DDoS Attack

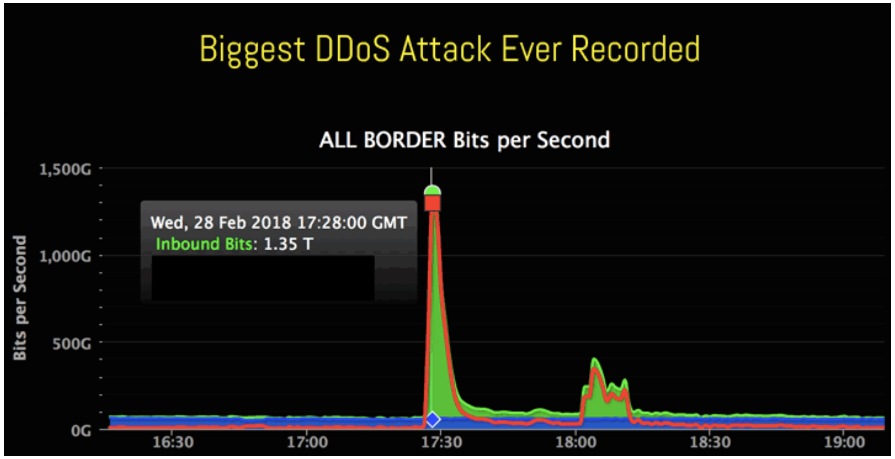
OCTOBER 22, 2016 KYLE YORK

It's likely that at this point you've seen some of the many news accounts of the Distributed Denial of Service (DDoS) attack Dyn sustained against our Managed DNS infrastructure this past Friday, October 21. We'd like to take this opportunity to share additional details and context regarding the attack. At the time of this writing, we are carefully monitoring for any additional attacks. Please note that our investigation regarding root cause continues and will be the topic of future updates. It is worth noting that we are unlikely to share all details of the attack and our mitigation efforts to preserve future defenses.

I also don't want to get too far into this post without:

1. Acknowledging the tremendous efforts of Dyn's operations and support teams in doing battle with what's likely to be seen as an historic attack.
2. Acknowledging the tremendous support of Dyn's customers, many of whom reached out to support our mitigation efforts even as they were impacted. Service to our customers is always our number one priority, and we appreciate their understanding as

DDoS case study : Memecached servers, February, 2018



- The largest recorded attack – peak of 1.35 Tbps
- Weaponized misconfigured memecached servers
- Targeted GitHub
- More than 2x larger than Mirai
- We should expect more massive attacks like this – and we should be prepared

Why do you have to CARE?

Economic Productivity

- Service interruption or failure of business operations relying on network connectivity, particularly for seasonal operations
- Time sensitive operations

Brand

- Loss of reputation with customers and partners

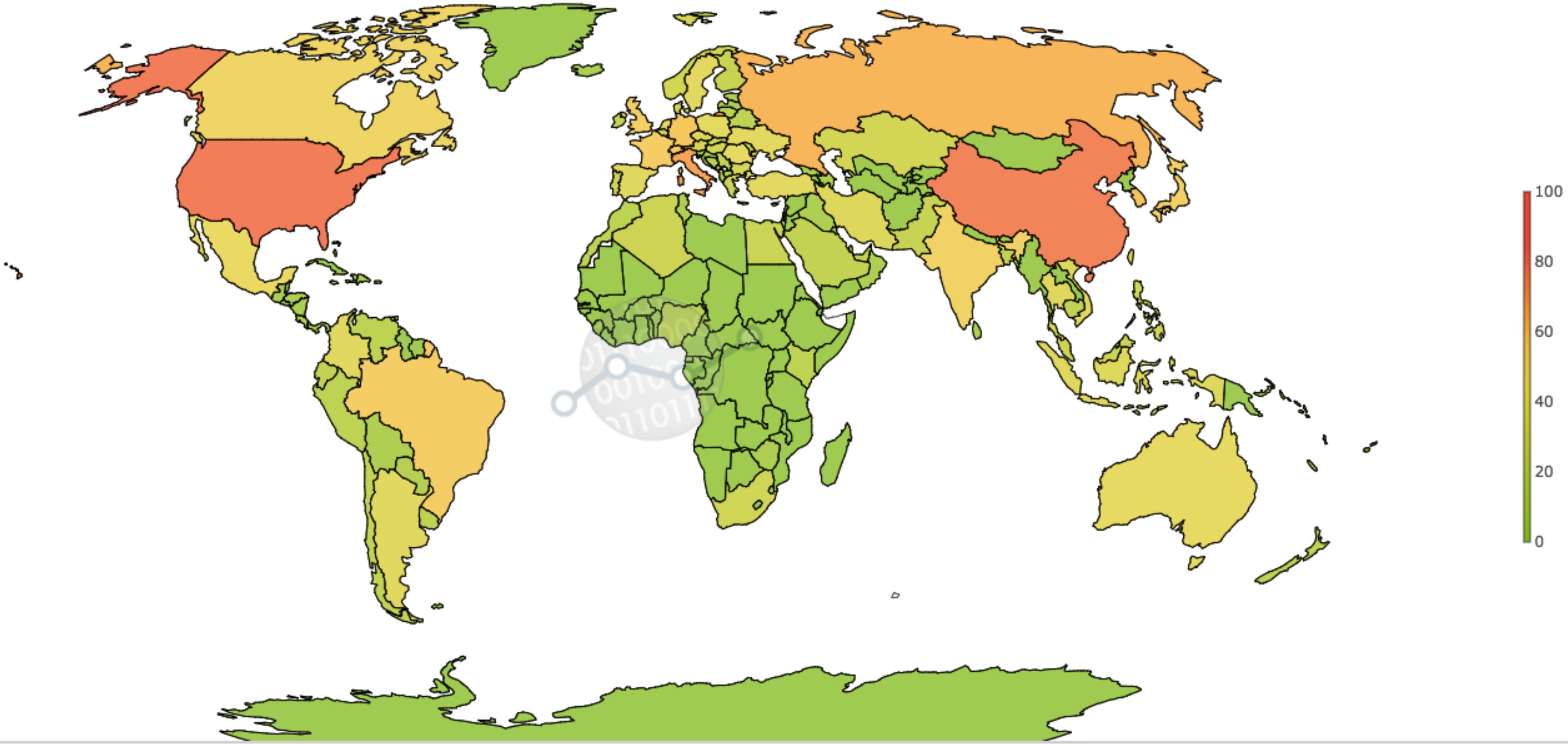
Technical

- Network service interrupted
- Isolation of victim network by network providers from the rest of Internet to mitigate collateral damage to other customers

Financial

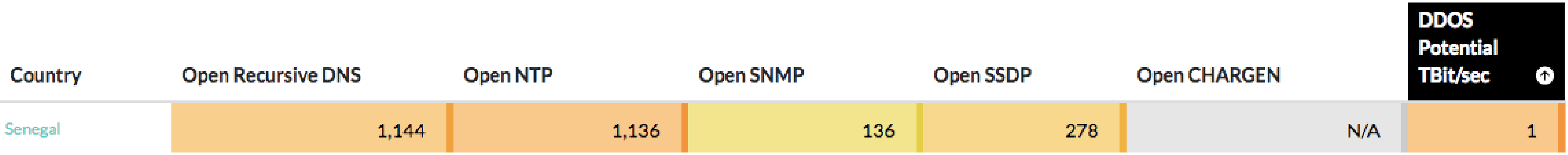
- Loss of business resulting from service interruption
- Cost of specialized DDoS mitigation services

Global View
http://stats.cybergreen.net



Senegal Overview

Week of April 23, 2018 – April 29, 2018

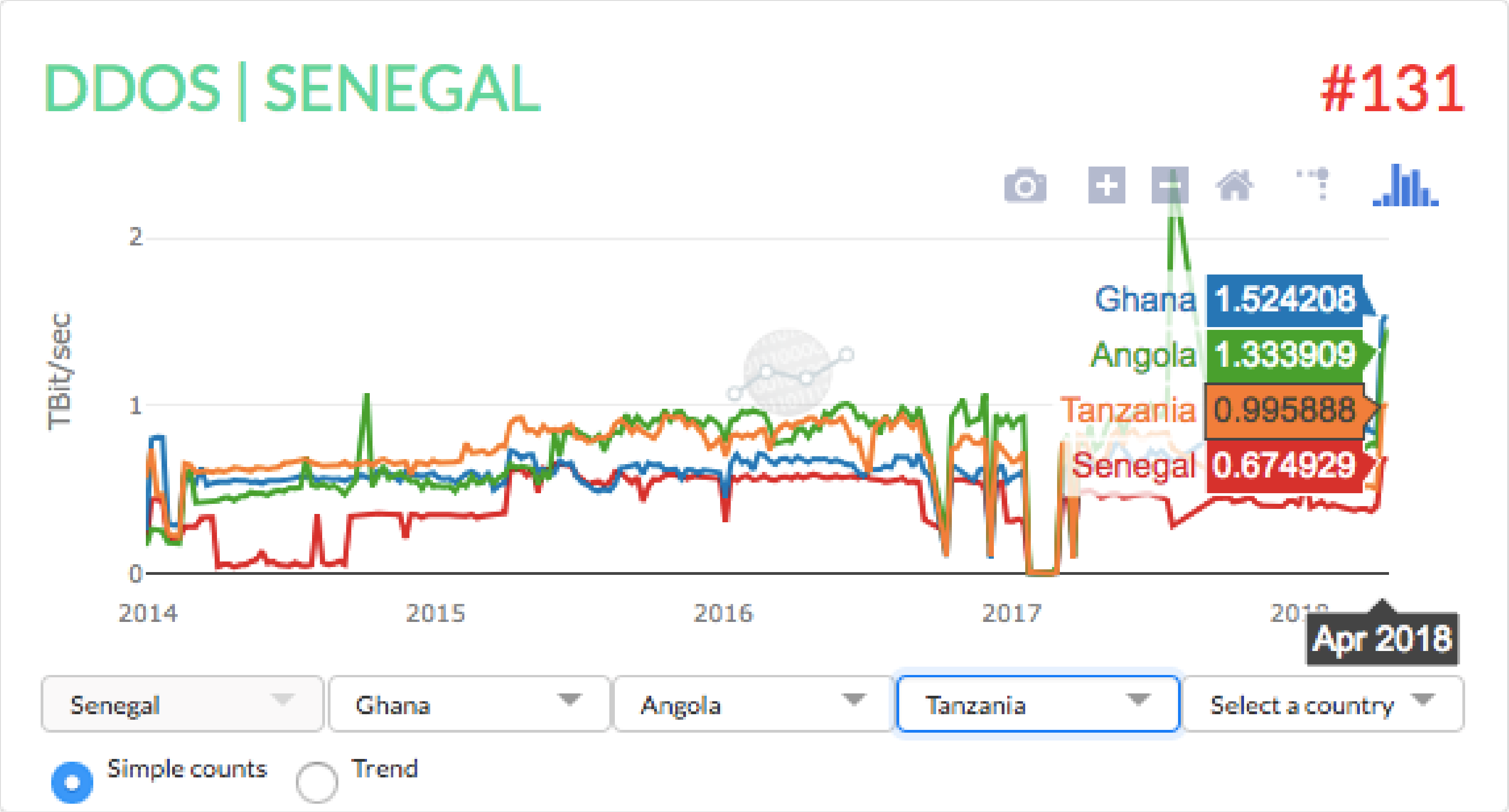


Country	Open Recursive DNS	Open NTP	Open SNMP	Open SSDP	Open CHARGEN	DDOS Potential TBit/sec
Senegal	1,144	1,136	136	278	N/A	1

- Open DNS is the biggest problem area, followed by open NTP

Let’s compare Senegal to other African countries…

Compare with Senegal, Angola, Tanzania, Ghana
Total Potential DDoS Bandwidth



Senegal | Ghana | Angola | Tanzania | Select a country

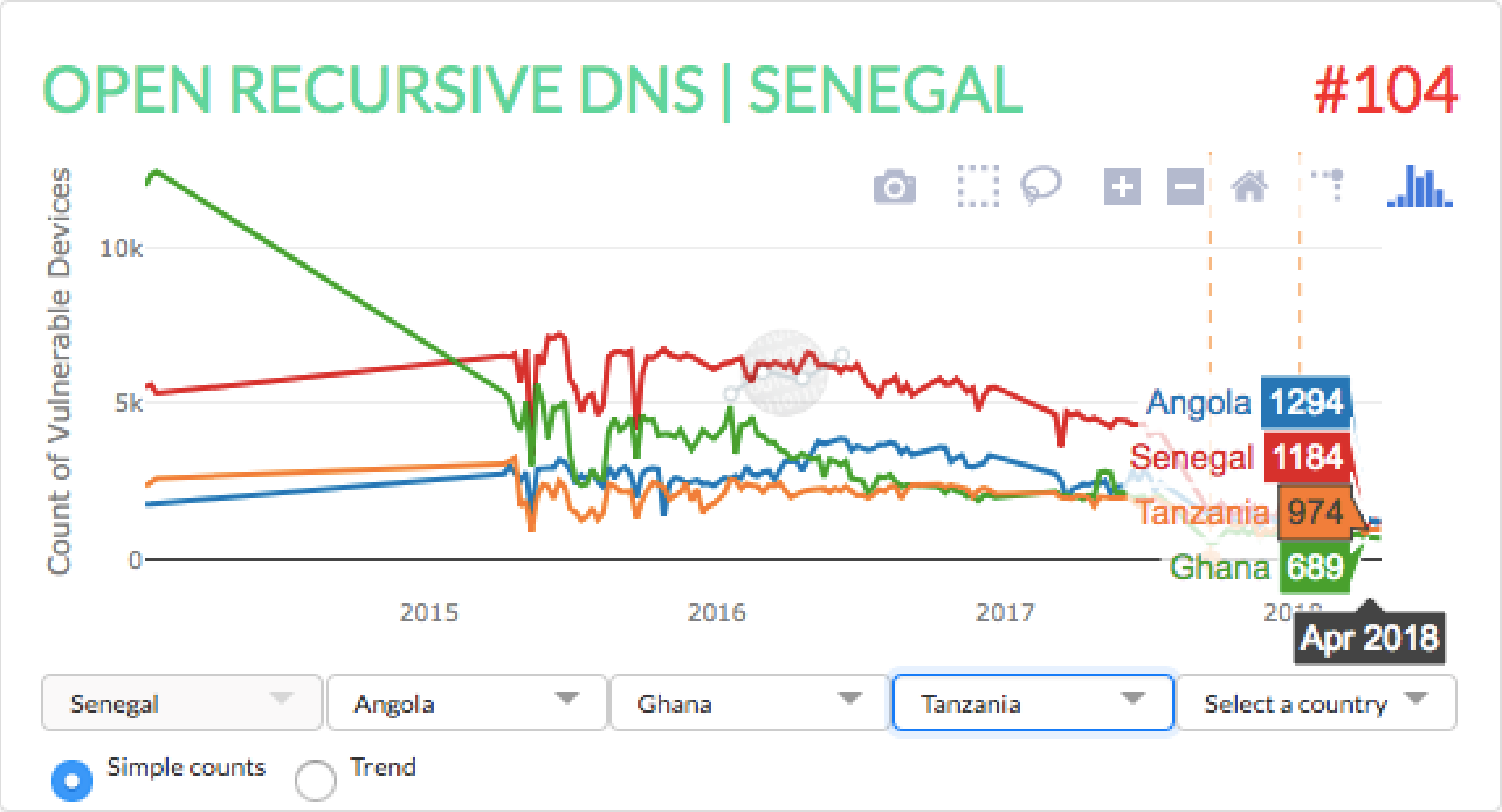
● Simple counts ○ Trend

A note on methodology

CyberGreen's v2.1 metrics report risk to others in terms of "How bad could it be?" This means that CyberGreen v2.1 metrics factor in the scale potential for amplification by protocol by node. Whereas the v2.0 Index is a rank order by the size of the unmet mitigation need, the v2.1 Index is a rank order by the size of the DDoS that could be mounted from the country, the AS, or the alternate entity should all of their nodes currently available to attackers were to be used in a single attack. In short, the v2.1 Index measures "offensive potential" — with the obvious caveat that we do not mean intentional offense but rather the degree to which the country, the AS, or the alternate entity can be made to engage in offense whether it wanted to or not.

Note: This formula for offensive potential does not take into account maximum upstream speeds of the observed unit. Our metrics experts at CyberGreen are currently discussing development of metric Version 2.1.5 to address this.

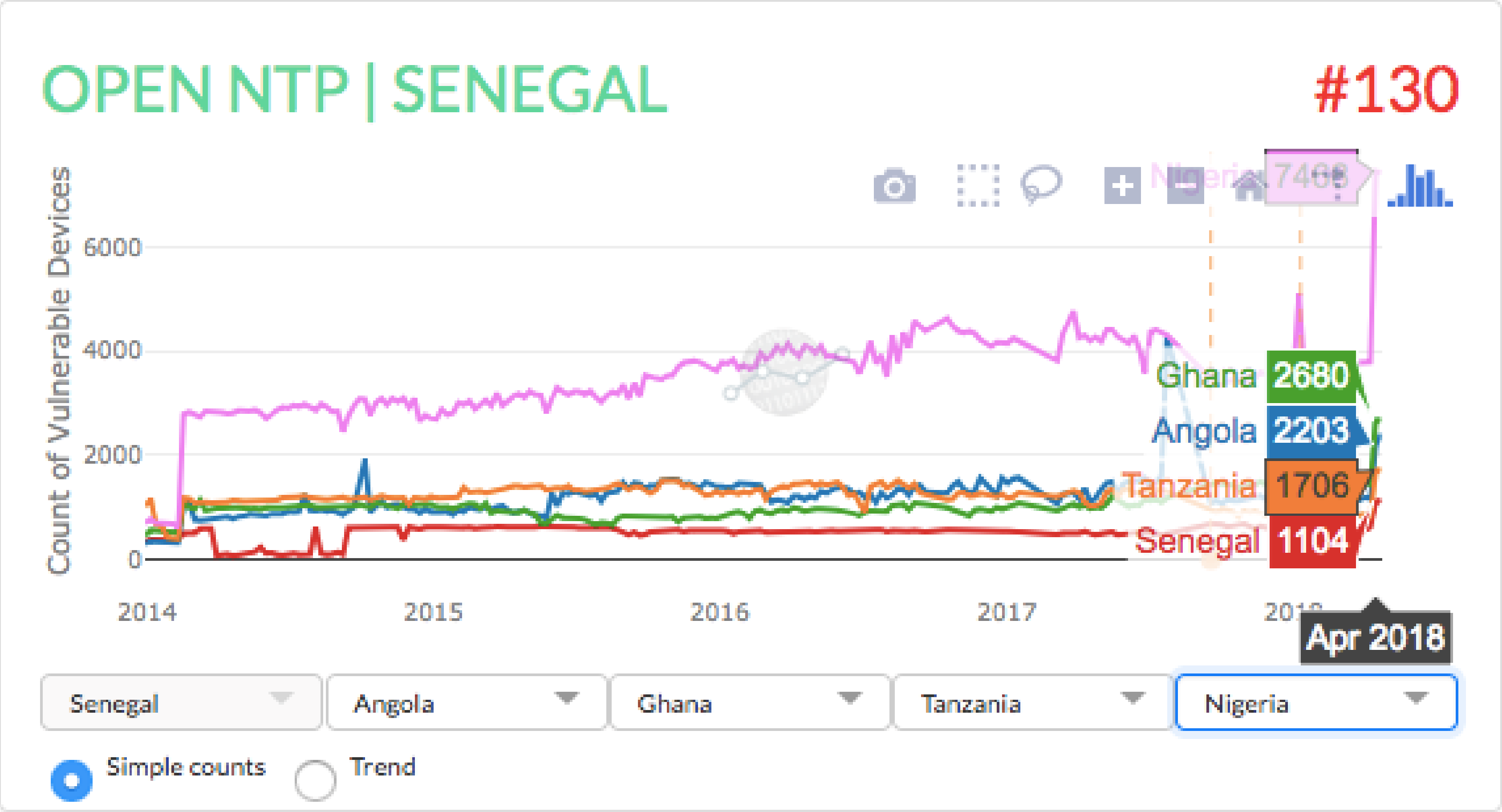
Compare with Senegal, Angola, Tanzania, Ghana
Open DNS



CyberGreen

Compare with Senegal, Angola, Tanzania, Ghana, Nigeria

Open NTP



OPEN NTP | SENEGAL

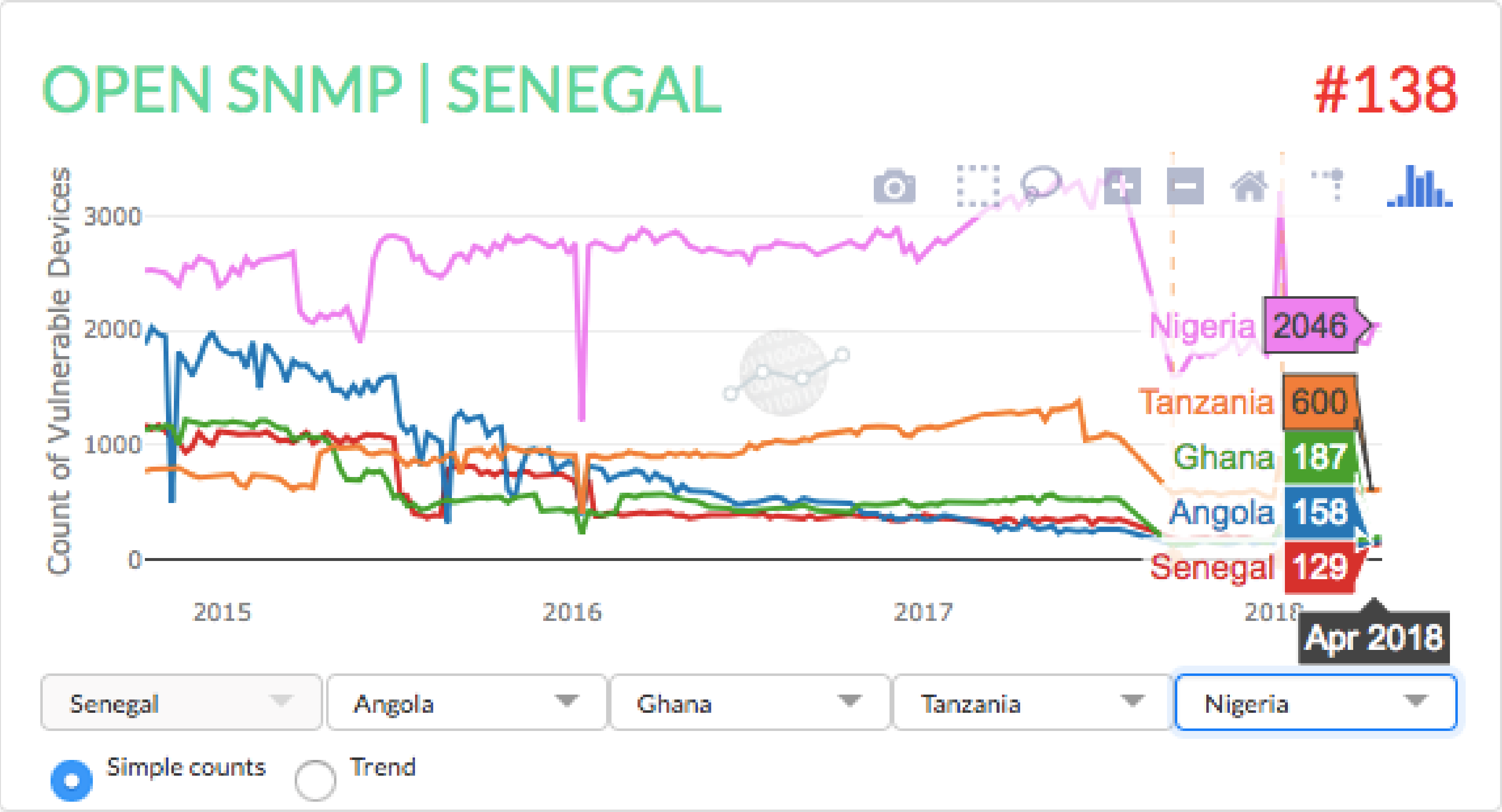
#130

Senegal ▾ | Angola ▾ | Ghana ▾ | Tanzania ▾ | Nigeria ▾

● Simple counts ○ Trend

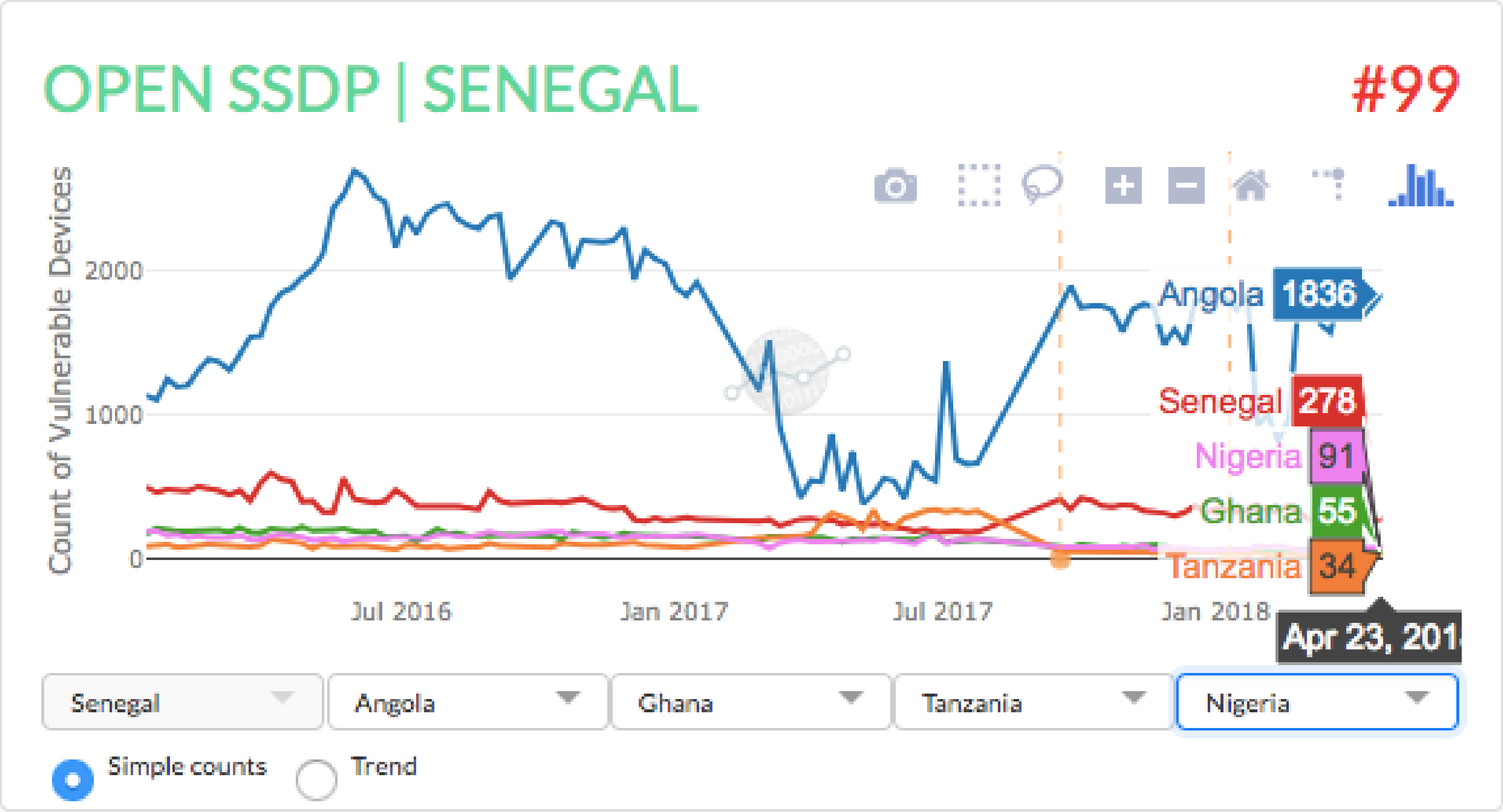
Compare with Senegal, Angola, Tanzania, Ghana, Nigeria

Open SNMP



Compare with Senegal, Angola, Tanzania, Ghana, Nigeria

Open SSDP



ASNs/ISPs in Senegal

So let’s look at Senegal’s ISPs

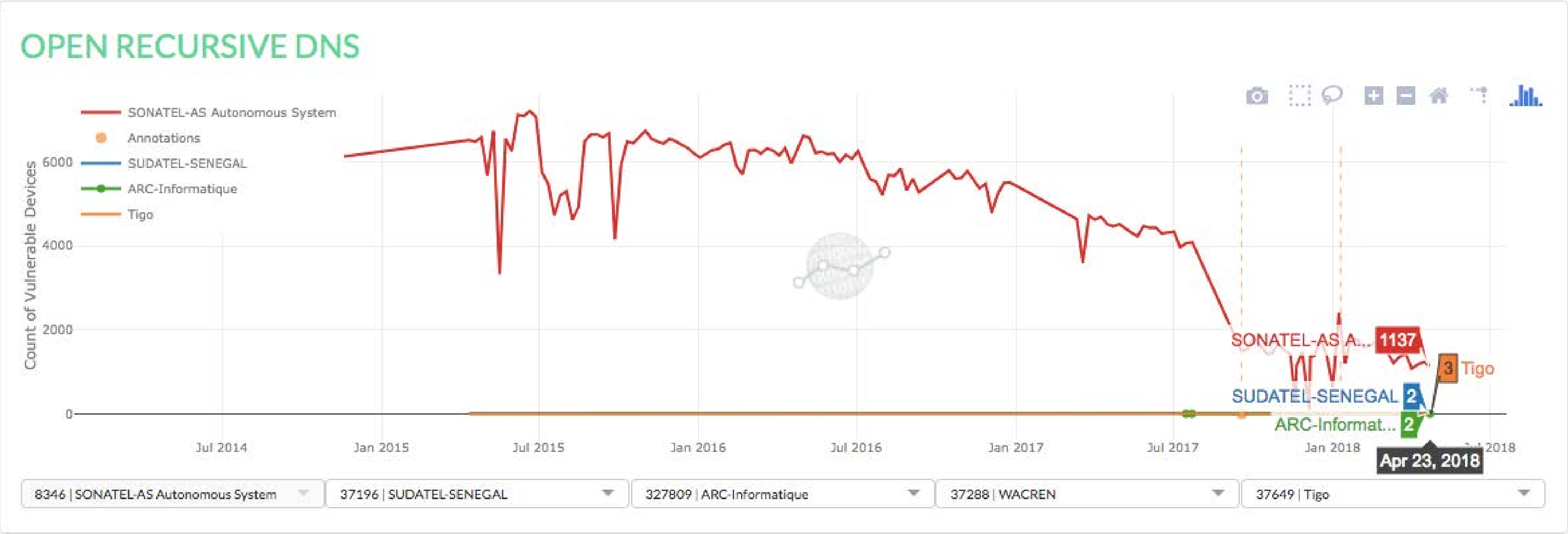
- An Autonomous System Number (ASN) is a number used by network operators to uniquely identify an independent IP network that has its own routing policies
- Senegal has 10 ASNs assigned to 4 Network Operators (most of whom are ISPs)
- And not all are equal…

Let us examine performance of best practice deployment of network equipment

In each case let's ask:

- What has caused an improvement
- What has caused a worsening of "polluted" deployments

Comparison across 4 Senegalese ASNs
Open DNS



8346 | SONATEL-AS Autonomous System

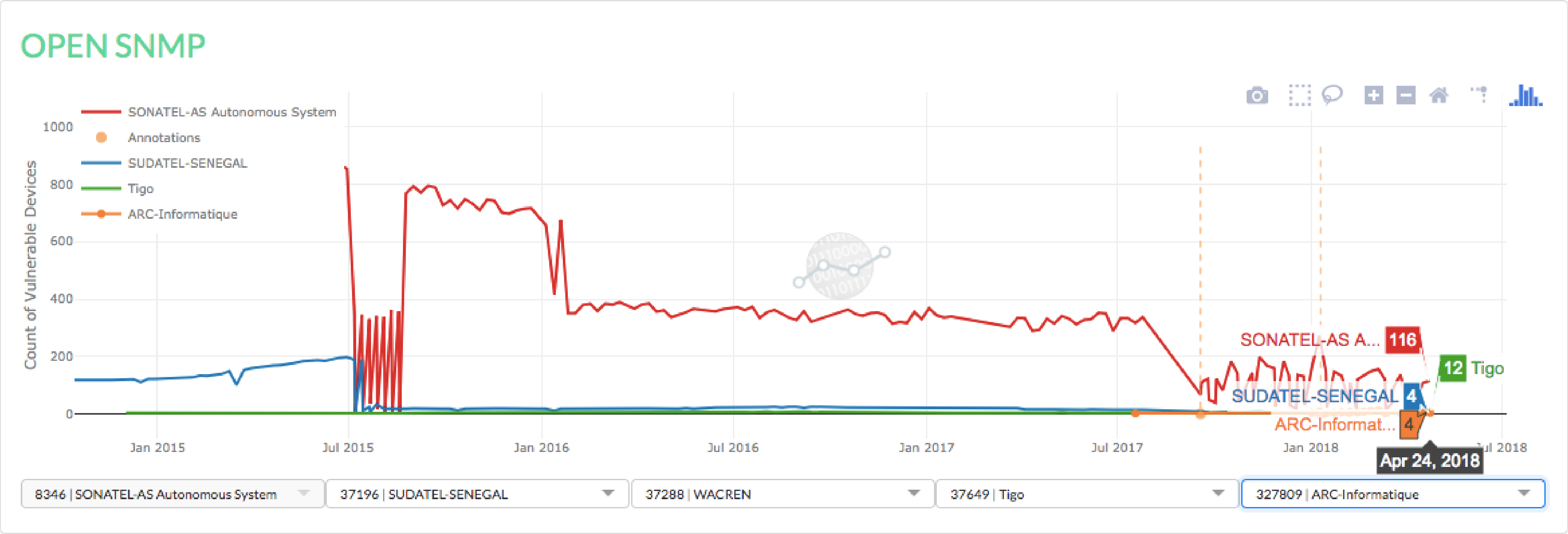
37196 | SUDATEL-SENEGAL

327809 | ARC-Informatique

37288 | WACREN

37649 | Tigo

Comparison across 4 Senegalese ASNs
Open SNMP



8346 | SONATEL-AS Autonomous System

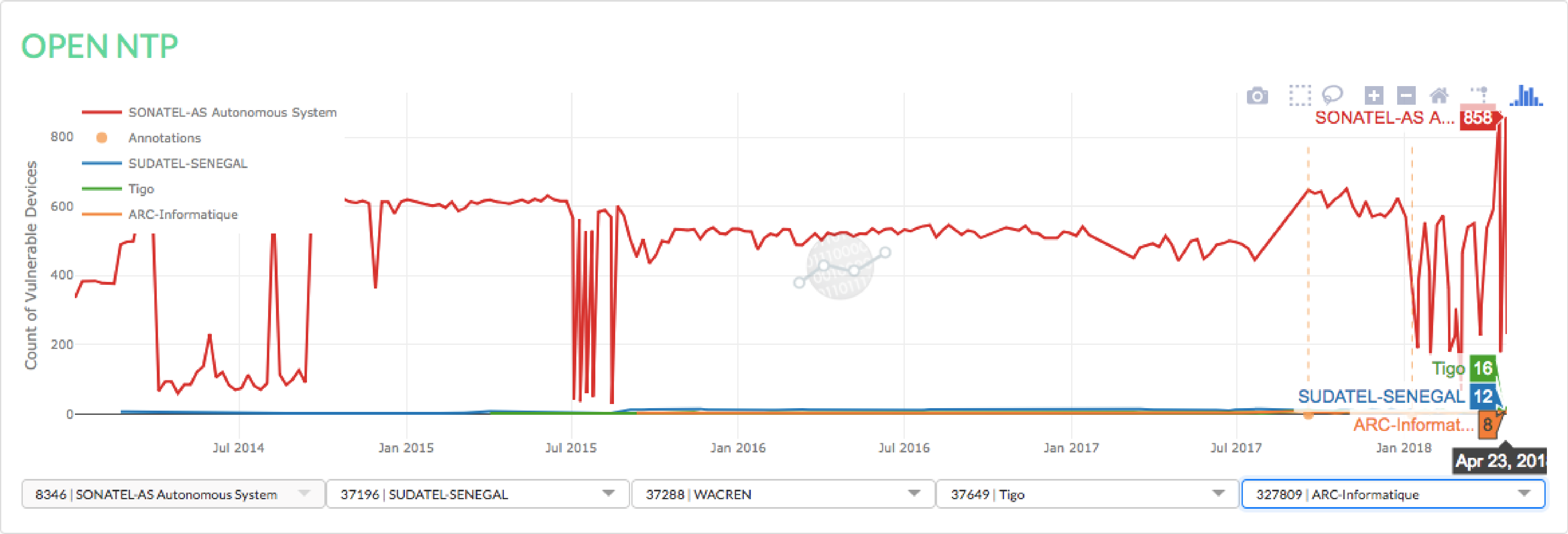
37196 | SUDATEL-SENEGAL

37288 | WACREN

37649 | Tigo

327809 | ARC-Informatique

Comparison across 4 Senegalese ASNs
Open NTP



8346 | SONATEL-AS Autonomous System

37196 | SUDATEL-SENEGAL

37288 | WACREN

37649 | Tigo

327809 | ARC-Informatique

What can be done?

Download Open SSDP

Download Open NTP

Download Open DNS

Download SpamBot

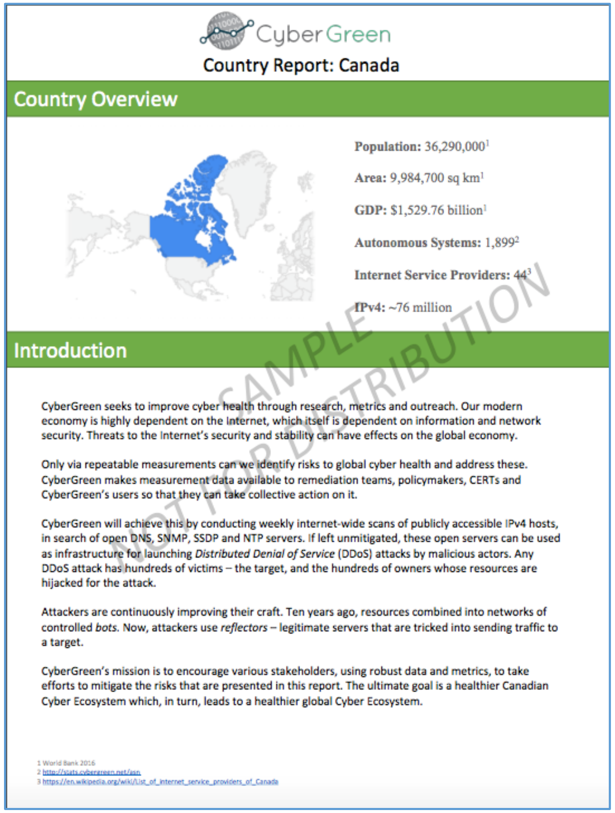
Download CyberGreen Mitigation Materials at

http://www.cybergreen.net/mitigation/

Mitigation approaches:

- How to identify your vulnerable servers/devices across your network
- How to find hosts running under risk conditions
- Step-by-step actions (e.g. update devices, reconfiguration, block certain protocols, disable services, implement certain BCPs)
- How to verify your fix

Country level analysis report



CyberGreen

Country Report: Canada

Country Overview

Population: 36,290,000[1]

Area: 9,984,700 sq km[1]

GDP: $1,529.76 billion[1]

Autonomous Systems: 1,899[2]

Internet Service Providers: 44[3]

IPv4: ~76 million

Introduction

CyberGreen seeks to improve cyber health through research, metrics and outreach. Our modern economy is highly dependent on the Internet, which itself is dependent on information and network security. Threats to the Internet's security and stability can have effects on the global economy.

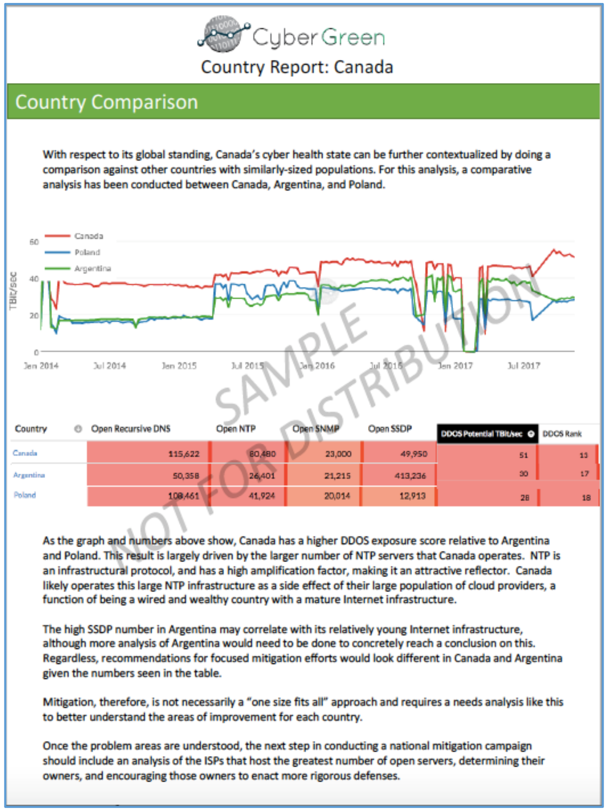
Only via repeatable measurements can we identify risks to global cyber health and address these. CyberGreen makes measurement data available to remediation teams, policymakers, CERTs and CyberGreen's users so that they can take collective action on it.

CyberGreen will achieve this by conducting weekly internet-wide scans of publicly accessible IPv4 hosts, in search of open DNS, SNMP, SSDP and NTP servers. If left unmitigated, these open servers can be used as infrastructure for launching *Distributed Denial of Service* (DDoS) attacks by malicious actors. Any DDoS attack has hundreds of victims – the target, and the hundreds of owners whose resources are hijacked for the attack.

Attackers are continuously improving their craft. Ten years ago, resources combined into networks of controlled *bots*. Now, attackers use *reflectors* – legitimate servers that are tricked into sending traffic to a target.

CyberGreen's mission is to encourage various stakeholders, using robust data and metrics, to take efforts to mitigate the risks that are presented in this report. The ultimate goal is a healthier Canadian Cyber Ecosystem which, in turn, leads to a healthier global Cyber Ecosystem.

[1] World Bank 2016
[2] http://stats.cybergreen.net/asn
[3] https://en.wikipedia.org/wiki/List_of_internet_service_providers_of_Canada



CyberGreen

Country Report: Canada

Country Comparison

With respect to its global standing, Canada's cyber health state can be further contextualized by doing a comparison against other countries with similarly-sized populations. For this analysis, a comparative analysis has been conducted between Canada, Argentina, and Poland.

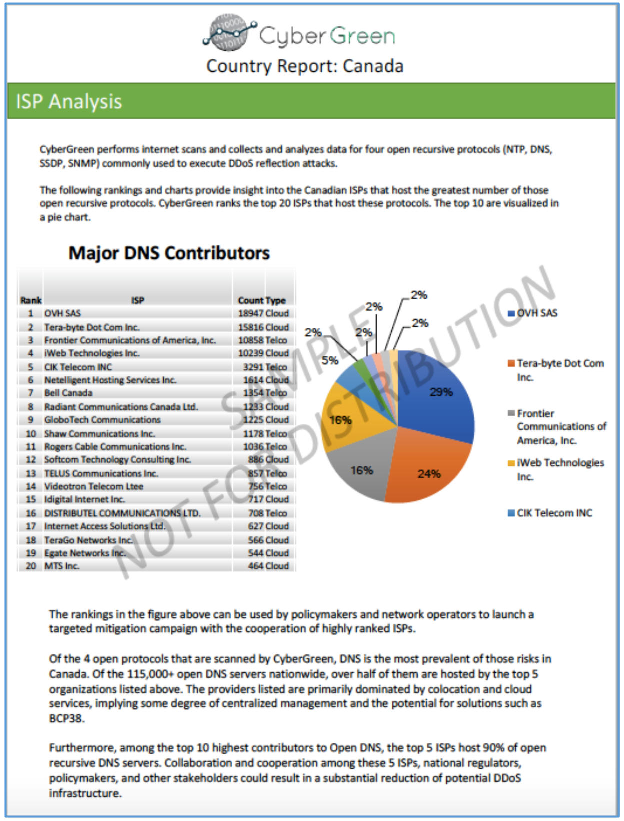
Country	Open Recursive DNS	Open NTP	Open SNMP	Open SSDP	DDOS Potential TBit/sec	DDOS Rank
Canada	115,622	80,480	23,000	49,950	51	13
Argentina	50,358	26,401	21,215	413,236	30	17
Poland	108,461	41,924	20,014	12,913	28	18

As the graph and numbers above show, Canada has a higher DDOS exposure score relative to Argentina and Poland. This result is largely driven by the larger number of NTP servers that Canada operates. NTP is an infrastructural protocol, and has a high amplification factor, making it an attractive reflector. Canada likely operates this large NTP infrastructure as a side effect of their large population of cloud providers, a function of being a wired and wealthy country with a mature Internet infrastructure.

The high SSDP number in Argentina may correlate with its relatively young Internet infrastructure, although more analysis of Argentina would need to be done to concretely reach a conclusion on this. Regardless, recommendations for focused mitigation efforts would look different in Canada and Argentina given the numbers seen in the table.

Mitigation, therefore, is not necessarily a "one size fits all" approach and requires a needs analysis like this to better understand the areas of improvement for each country.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open servers, determining their owners, and encouraging those owners to enact more rigorous defenses.



CyberGreen

Country Report: Canada

ISP Analysis

CyberGreen performs internet scans and collects and analyzes data for four open recursive protocols (NTP, DNS, SSDP, SNMP) commonly used to execute DDoS reflection attacks.

The following rankings and charts provide insight into the Canadian ISPs that host the greatest number of those open recursive protocols. CyberGreen ranks the top 20 ISPs that host these protocols. The top 10 are visualized in a pie chart.

Major DNS Contributors

Rank	ISP	Count	Type
1	OVH SAS	18947	Cloud
2	Tera-byte Dot Com Inc.	15816	Cloud
3	Frontier Communications of America, Inc.	10858	Telco
4	iWeb Technologies Inc.	10239	Cloud
5	CIK Telecom INC	3291	Telco
6	Netelligent Hosting Services Inc.	1614	Cloud
7	Bell Canada	1354	Telco
8	Radiant Communications Canada Ltd.	1233	Cloud
9	GloboTech Communications	1225	Cloud
10	Shaw Communications Inc.	1178	Telco
11	Rogers Cable Communications Inc.	1036	Telco
12	Softcom Technology Consulting Inc.	886	Cloud
13	TELUS Communications Inc.	857	Telco
14	Videotron Telecom Ltee	756	Telco
15	Idigital Internet Inc.	717	Cloud
16	DISTRIBUTEL COMMUNICATIONS LTD.	708	Telco
17	Internet Access Solutions Ltd.	627	Cloud
18	TeraGo Networks Inc.	566	Cloud
19	Egate Networks Inc.	544	Cloud
20	MTS Inc.	464	Cloud

The rankings in the figure above can be used by policymakers and network operators to launch a targeted mitigation campaign with the cooperation of highly ranked ISPs.

Of the 4 open protocols that are scanned by CyberGreen, DNS is the most prevalent of those risks in Canada. Of the 115,000+ open DNS servers nationwide, over half of them are hosted by the top 5 organizations listed above. The providers listed are primarily dominated by colocation and cloud services, implying some degree of centralized management and the potential for solutions such as BCP38.

Furthermore, among the top 10 highest contributors to Open DNS, the top 5 ISPs host 90% of open recursive DNS servers. Collaboration and cooperation among these 5 ISPs, national regulators, policymakers, and other stakeholders could result in a substantial reduction of potential DDoS infrastructure.

The public policy challenge

Market failures are resulting in network operators and device manufacturers not being incentivized to ensure improved cyber security practices in their operations.

The result is a large global base of vulnerable computers, modems/routers and Internet of Things devices which can be manipulated by Cyber criminals.

Communications regulators and/or CERTS should:

Utilize publicly available data on network risk indicators to engage ISPs to encourage better device deployment processes and operational decisions.

Encourage the adoption of the Internet Society's Mutually Agreed Norms for Routing Security, or MANRS (https://www.manrs.org) by network operators.

CyberGreen

Thank you!

Yurie Ito

yito@cybergreen.net

NBIP nationale
beheersorganisatie
internet
providers

Ing.Octavia de Weerdt

Director

www.NBIP.nl

Linked in

NBIP NaWas

How a joint effort approach is efficiently fighting DDoS attacks in the NL cyberspace

05/07/2018

Who we are

Who we are

Sector initative started in 2002

- Lawful Interception (LI) compliancy solution for the lawful interception Act (the NL Telecommunications Act)
- Smarter together
- Independent not-for-profit foundation

DDoS attacks increasingly complex after 2013

Where to start?

NBIP nationale beheersorganisatie internet providers

Anti DDoS protection

One anti DDoS solution

- Detect
- Mitigate
- Analyse and Report

NaWas (Nationale Wasstraat) in 2014 is a NBIP initiative.

- The NaWas is able to mitigate any DDoS attack
- Available as a service.
- Cooperative model

2018 and beyond

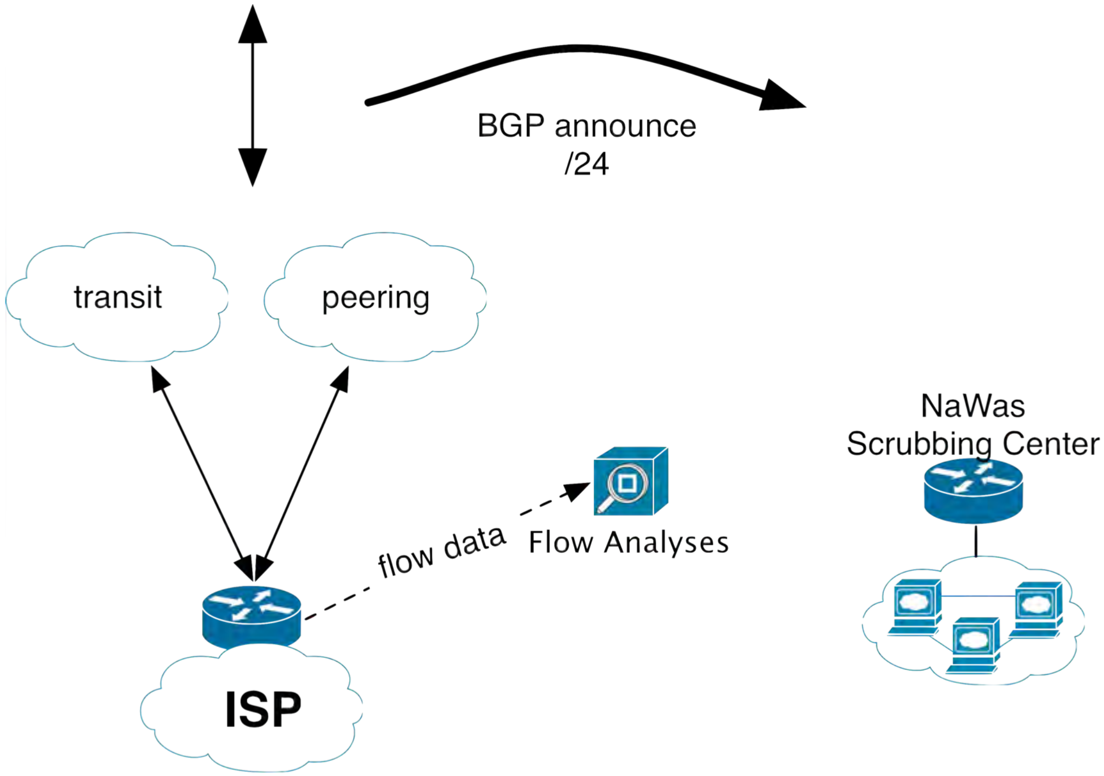
- Continuity services for AS owners with their own solution in place
- 2nd scrubbing center operational in fall 2018
- Distributed model
- First European members
- Mature services compliant with all (Privacy) european demands

DDoS detection

- by the customer
- flood
- application attack

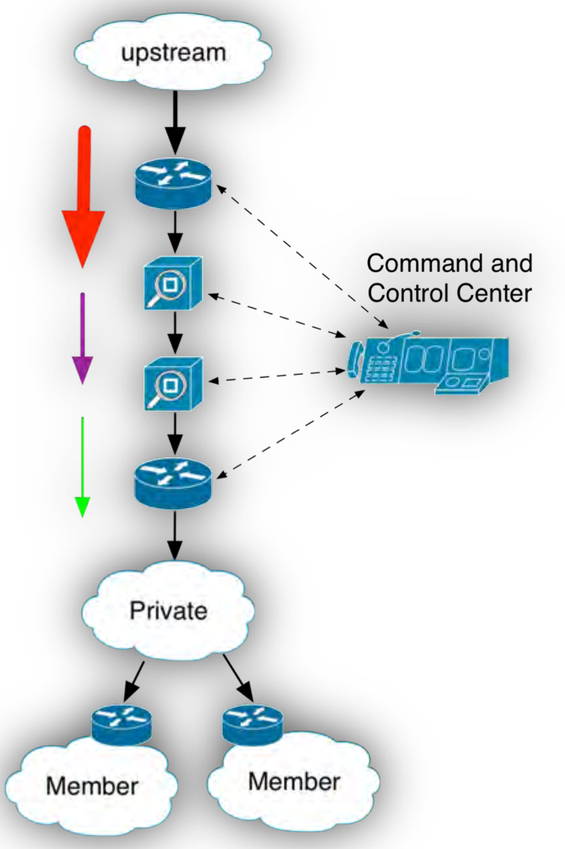
DDoS Defender

- thresholds
- type of traffic
- flowdata
- packets



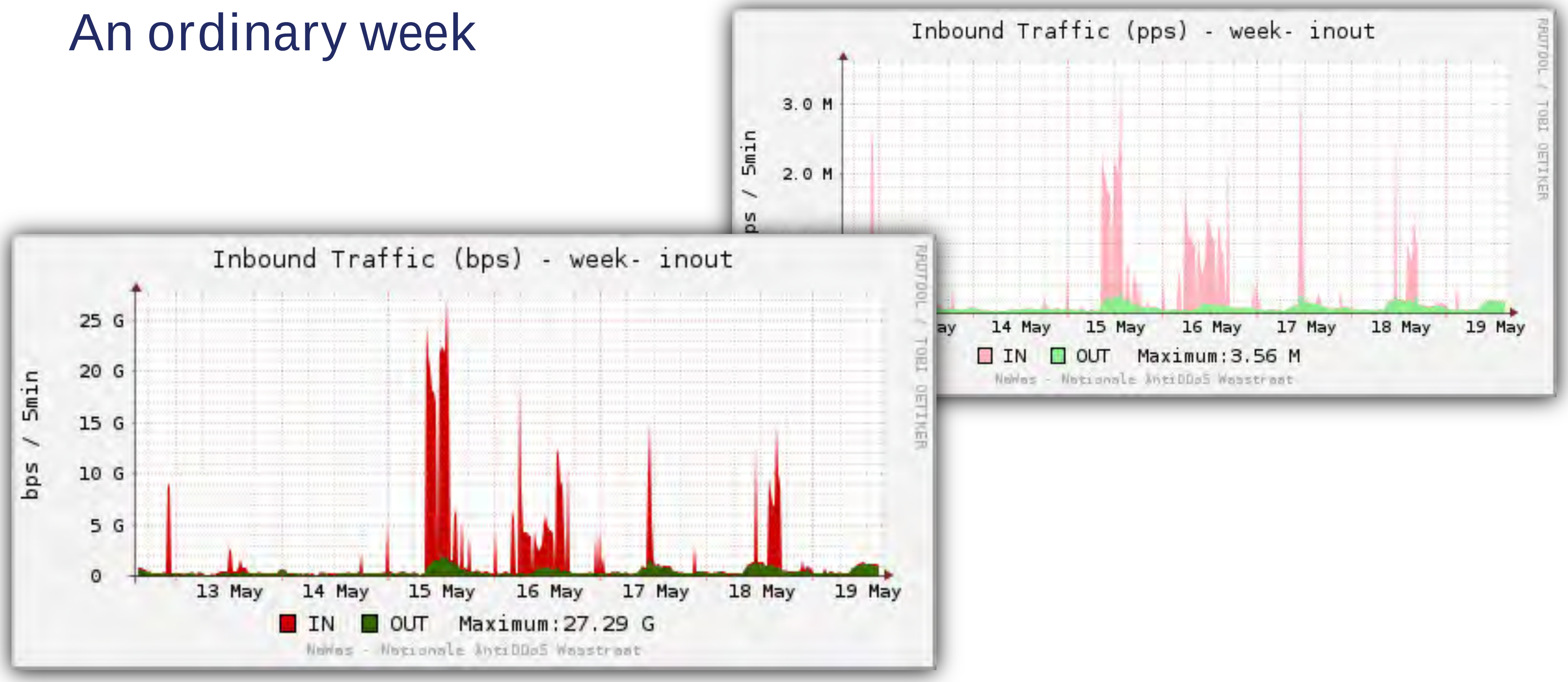
DDoS mitigation

- BGP advertisement of more specific prefix
- multiple devices
- UDP, TCP, floods, application layer

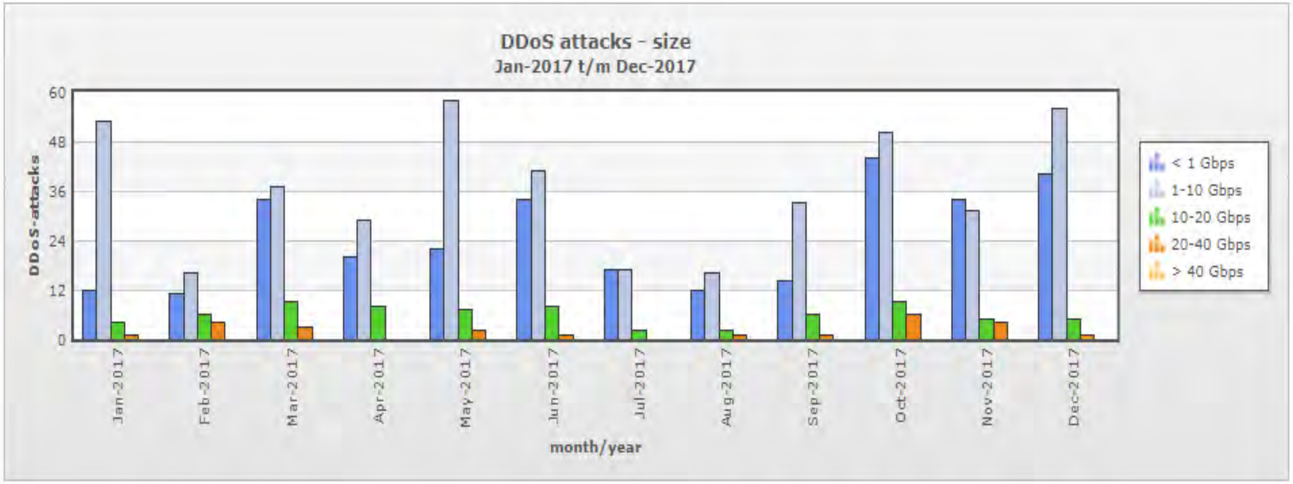


DDoS mitigation

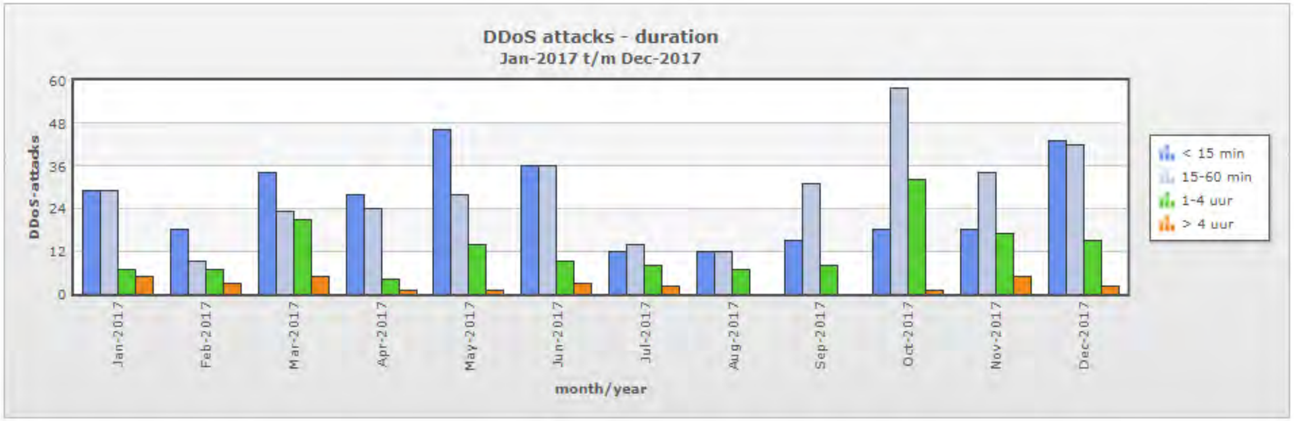
An ordinary week



DDoS 2017 Facts and figures (1)

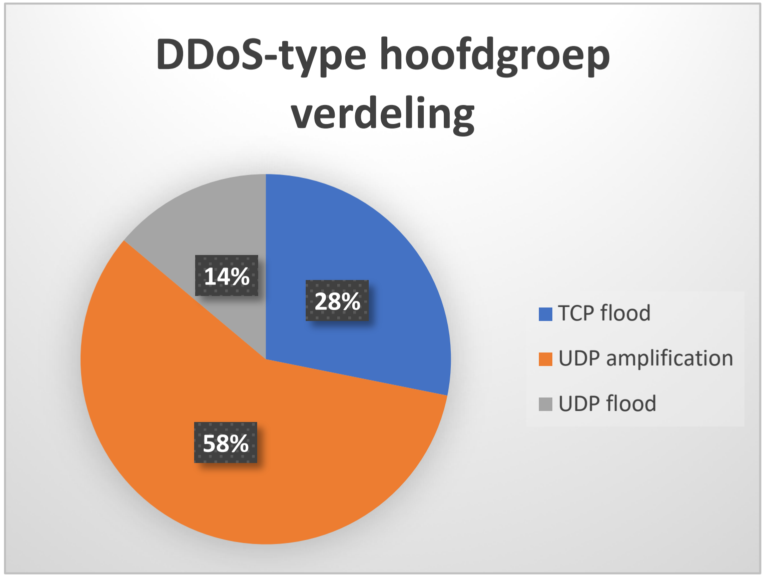


- Most attacks between 1 and 10 Gbps
- Average of 3 attacks a day

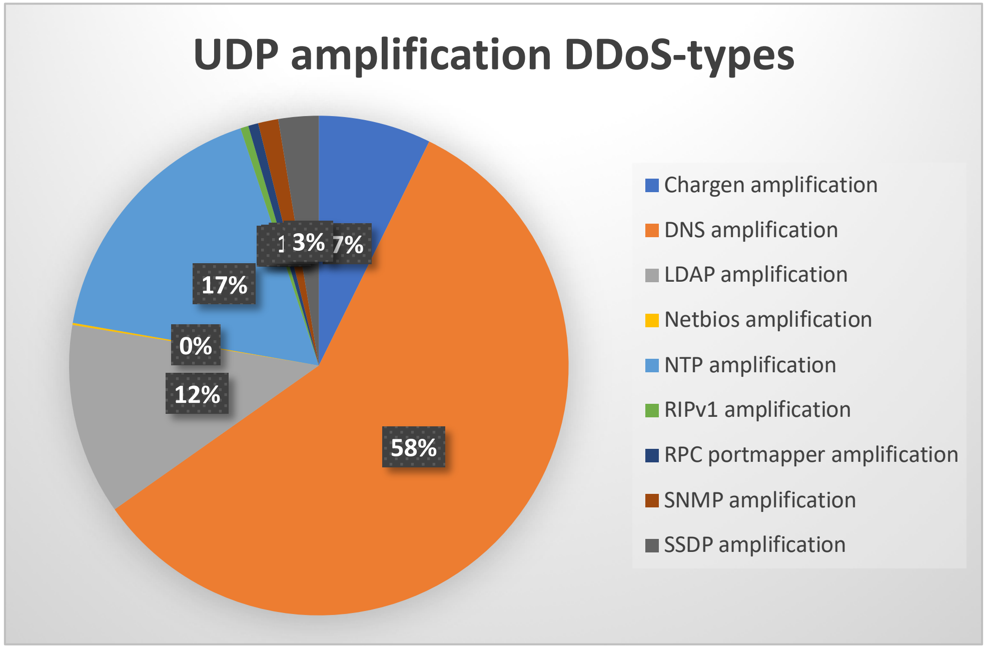


- Most of the attacks < 60 minutes
- Few attacks of 4 hours (longest attack= 23 hours)

DDoS 2017 facts and figures (2)



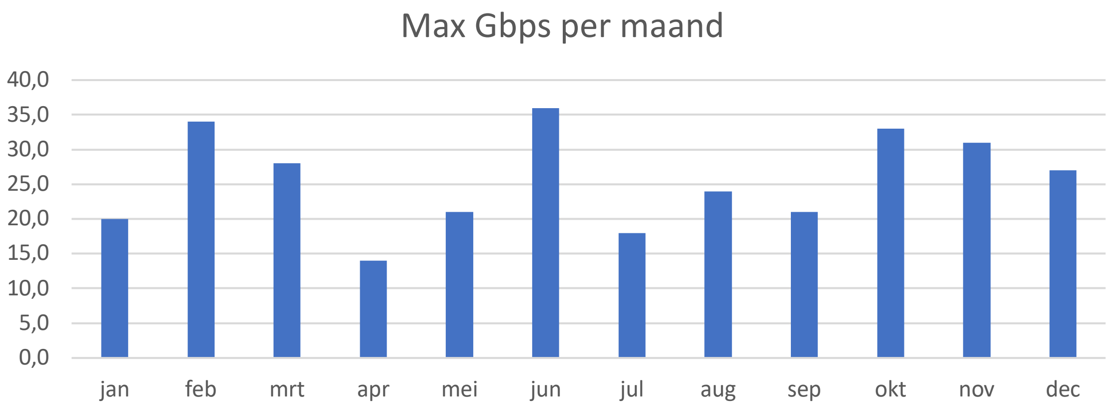
UDP amplification is the most “popular” attack

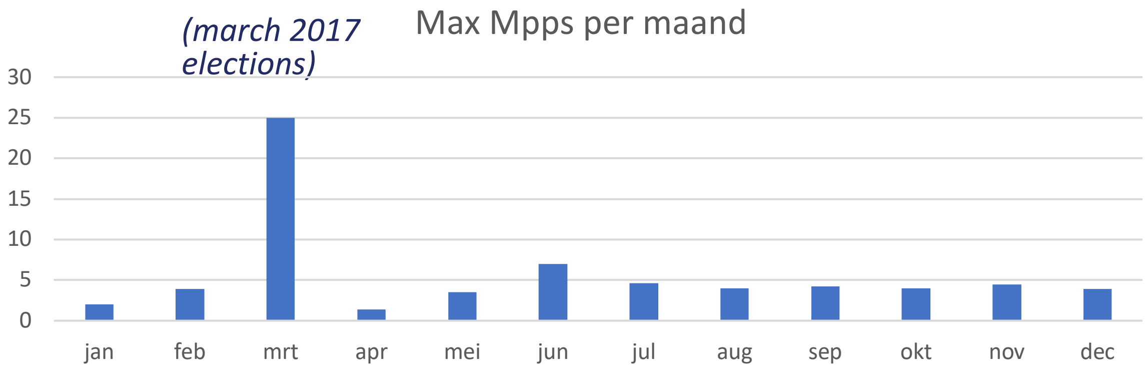


UDP amplification through DNS

NBIP nationale beheersorganisatie internet providers

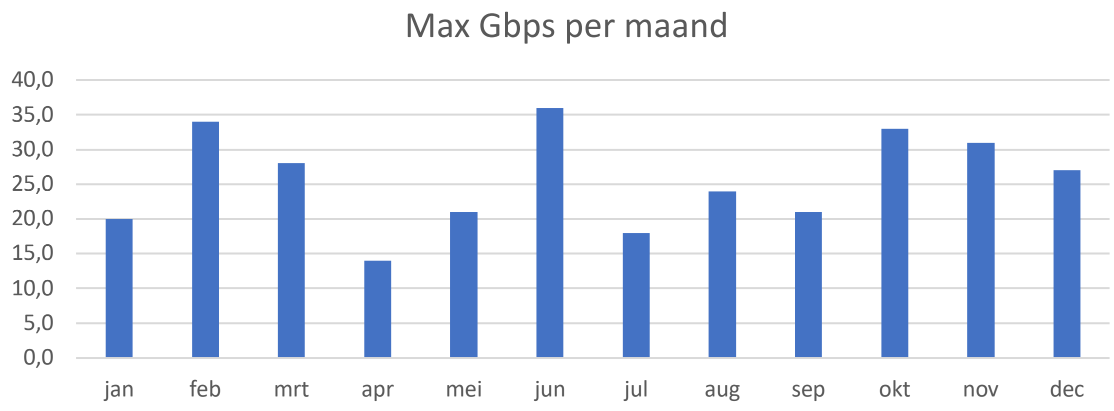
DDoS 2017 facts and figures (3)



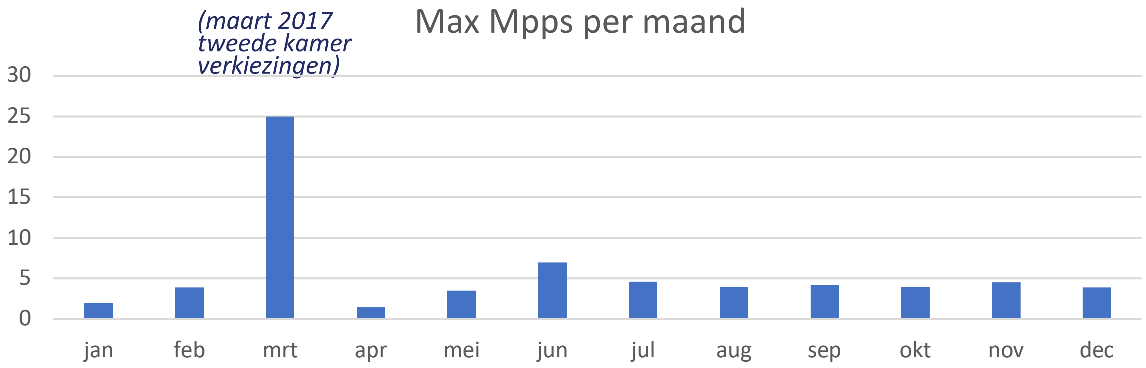


NBIP nationale beheersorganisatie internet providers

DDoS 2017 facts and figures (3)



Max Gbps per maand



Max Mpps per maand

(maart 2017 tweede kamer verkiezingen)

Anti DDoS facts and figures 2017

Register to get the full 2017 report

https://www.nbip.nl/2018/04/21/trends-and-figures-of-2017/

Knowledge Sharing

R&D projects together with Unversities
https://www.ddos-patterns.net

Succes keys

- (Vendor) independent
- Protection as a service
- Share the knowledge
- Connect everybody
- Trusted party

Together.
Smarter and stronger

Date

Trust by Design: The Internet of Things

Security and privacy of smart-home devices and services

Internet Society

Kevin G. Chege

ISOC

The number of IoT devices and systems connected to the Internet will be more than

2.5x the global population

by 2020 (Gartner).

As more and more devices are connected, privacy and security risks increase.

And most consumers don't even know it.

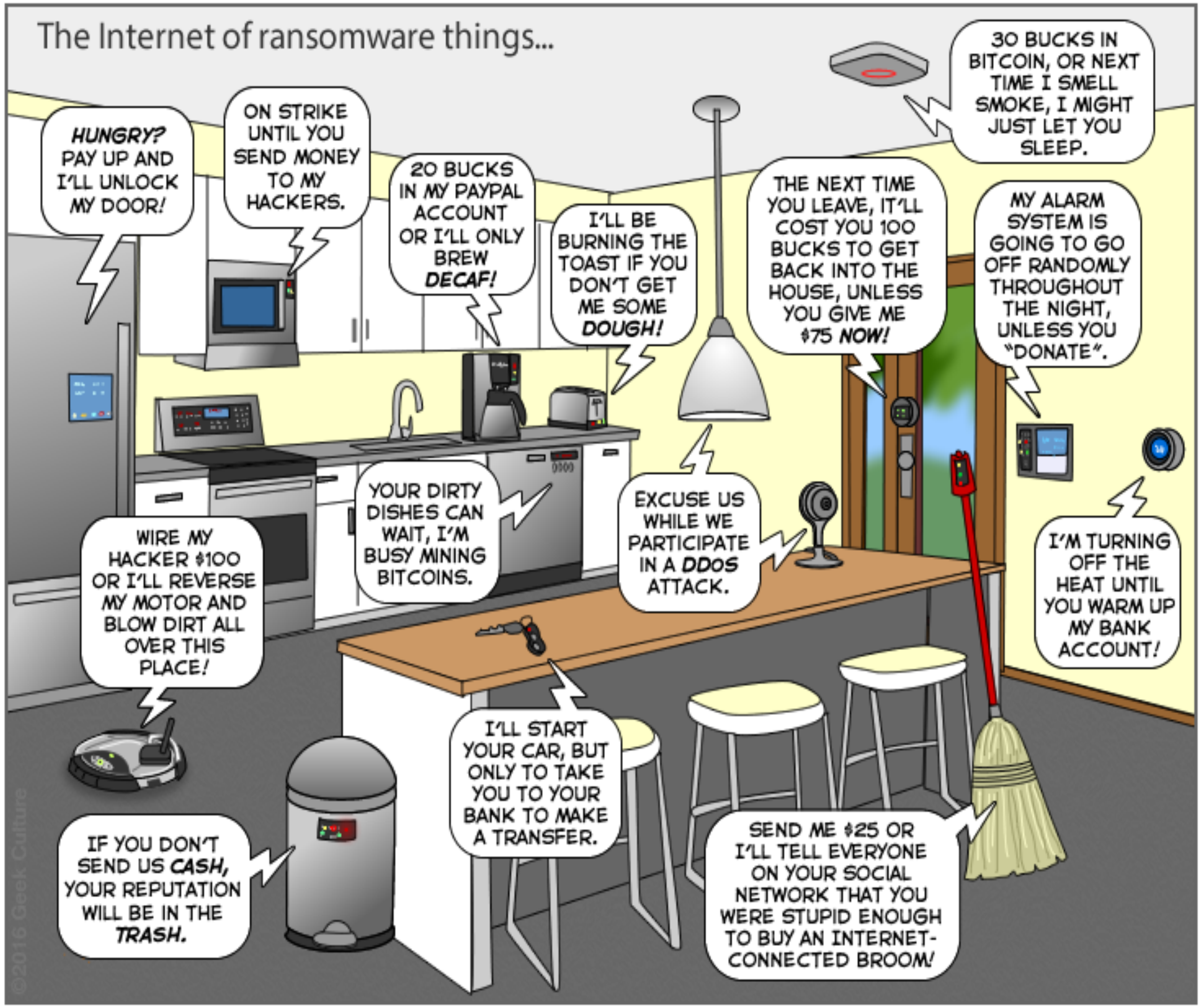
What type of risks?

Unlocking doors, turning on cameras, shutting down critical systems and theft of personal property.

People's safety or the safety of their family might even be at risk.

Large IoT-based attacks, such as the Mirai botnet in 2016, have crippled global access to high-profile Internet services for several hours.

The Joy of Tech™ by Nitrozac & Snaggy


The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture

You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

The challenges we face

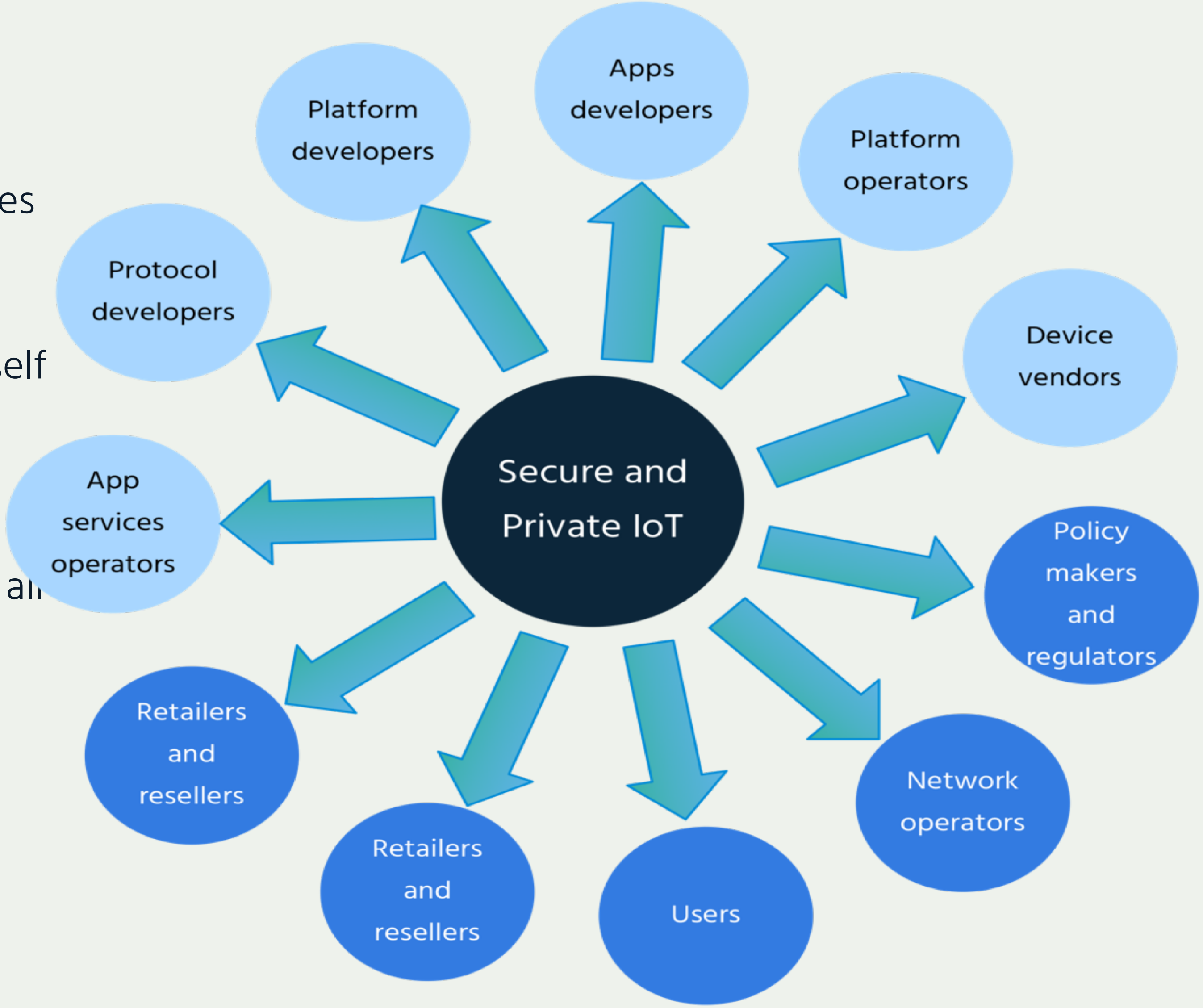
A connected world offers the promise of convenience, efficiency and insight, but creates a platform for shared risk.

Many of today’s IoT devices are rushed to market with little consideration for basic security and privacy protections.

Who is responsible?

Developers and users of IoT devices and systems have a collective obligation to ensure they do not expose others and the Internet itself to potential harm.

We need a collective approach, addressing security challenges on all fronts.



The Internet Society is working for a better Internet.

- We want manufacturers and suppliers of consumer IoT devices and services to adopt security and privacy guidelines to protect the Internet and consumers from cyber threats.
- We want to educate users on the importance of secure IoT devices and work with stakeholders involved in technology and security to better inform their communities on IoT.

Online Trust Alliance (OTA) IoT Trust Framework

- Provides a set of actions and principles to raise the level of security for IoT devices and related services to protect consumers and the privacy of their data
- More than 100+ stakeholders from industry, government and consumer advocates contributed to the Framework
- Stands apart from other IoT-related Frameworks with its comprehensive focus on security, privacy and lifecycle issues, as well as a holistic view of the entire system
- Please visit the ISOC Booth for a copy!

https://otalliance.org/iot/

Actionable principles in eight categories for manufacturers, developers and service providers

Authentication	Encryption	Security	Updates
Privacy	Disclosures	Control	Communications

IoT Framework Principles: It is a collective responsibility

IoT vendors and their supply chain

Distribution channels

Policymakers and governments

Consumer testing and product review organizations

Consumers and enterprises

Are you doing something in IoT in the African region?

- Are you doing research into the field of IoT or developing IoT products?
- Please let us know through the ISOC chapters
- This info will help us coordinate efforts in IoT and know what types of IoT devices are being developed in the region

Thank you.

chege@isoc.org

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120

M^3AAWG

MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP

Transnational Anti-Abuse Working Group (AAWG) Development

Jesse Sowell, PhD

M^3AAWG Senior Advisor
Vice-Chair of Growth and Develop Directing Outreach
Cybersecurity Fellow; Stanford Center for International Security and Cooperation (CISAC)
Honorary Lecturer; University College London; Science, Technology, Engineering and Public Policy (STEaPP)

GFCE @ Africa Internet Summit 2018
Dakar, Senegal
7 May 2018

Academic Anti-Abuse Research
Speaker Bio

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Interdisciplinary Research

- ➔ Internet operations
- ➔ Industrial political economy
- ➔ Operations strategy

MIT
Massachusetts Institute of Technology

CISAC
Center for International Security and Cooperation

High-Level Research Statement

I study the non-state institutions the ensure the Internet stays glued together in a secure and stable way

STE@PP
Applied in Focus. Global in Reach.

Operational Epistemic Communities

Knowledge-policy interface between conventional top-down state actors and bottom-up capabilities and capacity in operator communities

The Bush School
OF GOVERNMENT & PUBLIC SERVICE
TEXAS A&M UNIVERSITY

[1] Adapted from an early definition by MAPS

Introduction to Anti-Abuse

Anti-Abuse and Attribution
Prescriptive Ethos

“abuse is what customers complain about”[2]

“all information exchanges on the Internet *should be consensual*, and unless you choose to receive [traffic] from a third party, you should not *have to* accept it”[1]

Just because there is a *legitimate route* to a destination doesn’t mean all traffic *using that route* is legitimate

Provides a ***prescriptive ethos***, but doesn’t help with ***practical application***

[1] Adapted from an early definition by MAPS

[2] Definition offered by Dave Crocker

M^{3}AAWG Overview

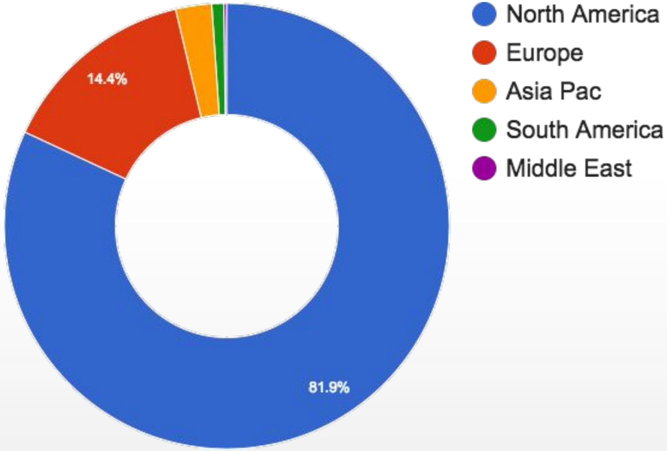
Who is M^3AAWG?

Constituencies and Demographics

MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP

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

- ➔ 200 member orgs "worldwide"
- ➔ 300-400 conference participants
- ➔ technology-neutral, *non-political* working body focusing on operational issues of Internet abuse
  - – Supporting technologies
  - – Industry collaboration
  - – Informing Public Policy

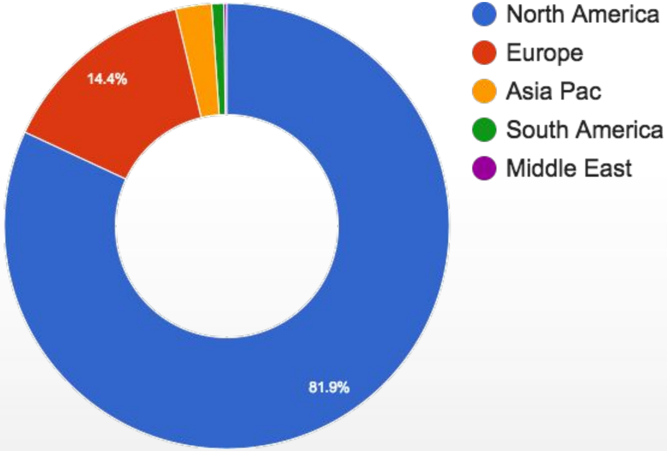


Who is M³AAWG?
We Need AP Contributions

M³AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP

"The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation"

- ➔ 200 member orgs "worldwide"
- ➔ 300-400 conference participants
- ➔ technology-neutral, *non-political* working body focusing on operational issues of Internet abuse
  - – Supporting technologies
  - – Industry collaboration
  - – Informing Public Policy



Too many US voices

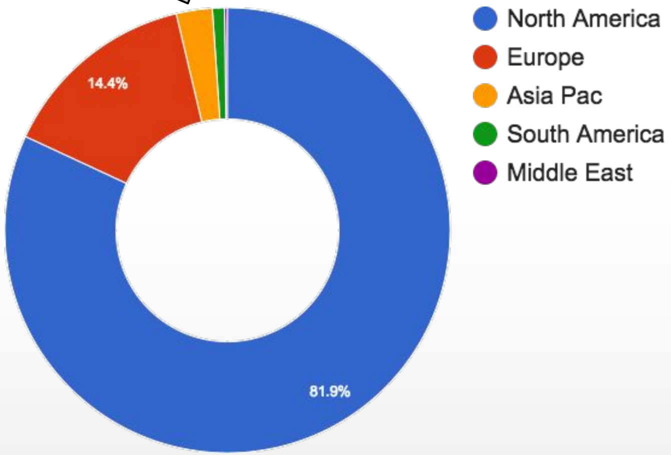
Who is M³AAWG?
We Need AP Contributions

M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

"The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation"

- ➔ 200 member orgs "worldwide"
- ➔ 300-400 conference participants
- ➔ technology-neutral, *non-political* working body focusing on operational issues of Internet abuse
  - – Supporting technologies
  - – Industry collaboration
  - – Informing Public Policy

Not enough global voices, not enough **AF voices!**



Too many US voices

What Does M^{3}AAWG Do?

Distill Industry Knowledge into BCPs

The “M” *cubed*:

- ➔ Messaging: abuse on any messaging platform, from e-mail to SMS texting
- ➔ Malware: abuse is often just a symptom and vector for viruses and malicious code
- ➔ Mobile: addressing messaging and malware issues emerging on mobile as an increasingly ubiquitous platform

Develop and Publish:

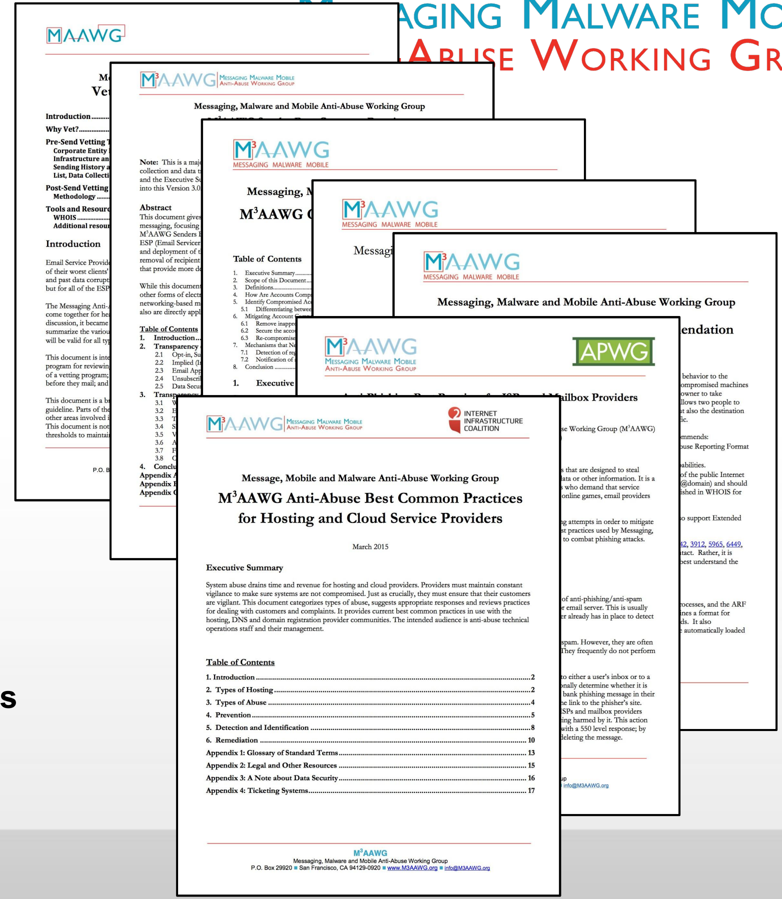
- ➔ Best practice papers
- ➔ Position statements
- ➔ Training and educational videos

Public Policy and Industry Guidelines

https://www.m3aawg.org/for-the-industry/published-comments

The Anti-Bot Code of Conduct for Internet Service Providers

https://www.m3aawg.org/abcs-for-ISP-code



M^{3}AAWG Messaging Malware Mobile Anti-Abuse Working Group

INTERNET INFRASTRUCTURE COALITION

Message, Mobile and Malware Anti-Abuse Working Group

M^{3}AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers

March 2015

Executive Summary

System abuse drains time and revenue for hosting and cloud providers. Providers must maintain constant vigilance to make sure systems are not compromised. Just as crucially, they must ensure that their customers are vigilant. This document categorizes types of abuse, suggests appropriate responses and reviews practices for dealing with customers and complaints. It provides current best common practices in use with the hosting, DNS and domain registration provider communities. The intended audience is anti-abuse technical operations staff and their management.

Table of Contents

M^{3}AAWG
Messaging, Malware and Mobile Anti-Abuse Working Group
P.O. Box 29920 ■ San Francisco, CA 94129-0920 ■ www.M3AAWG.org ■ info@M3AAWG.org

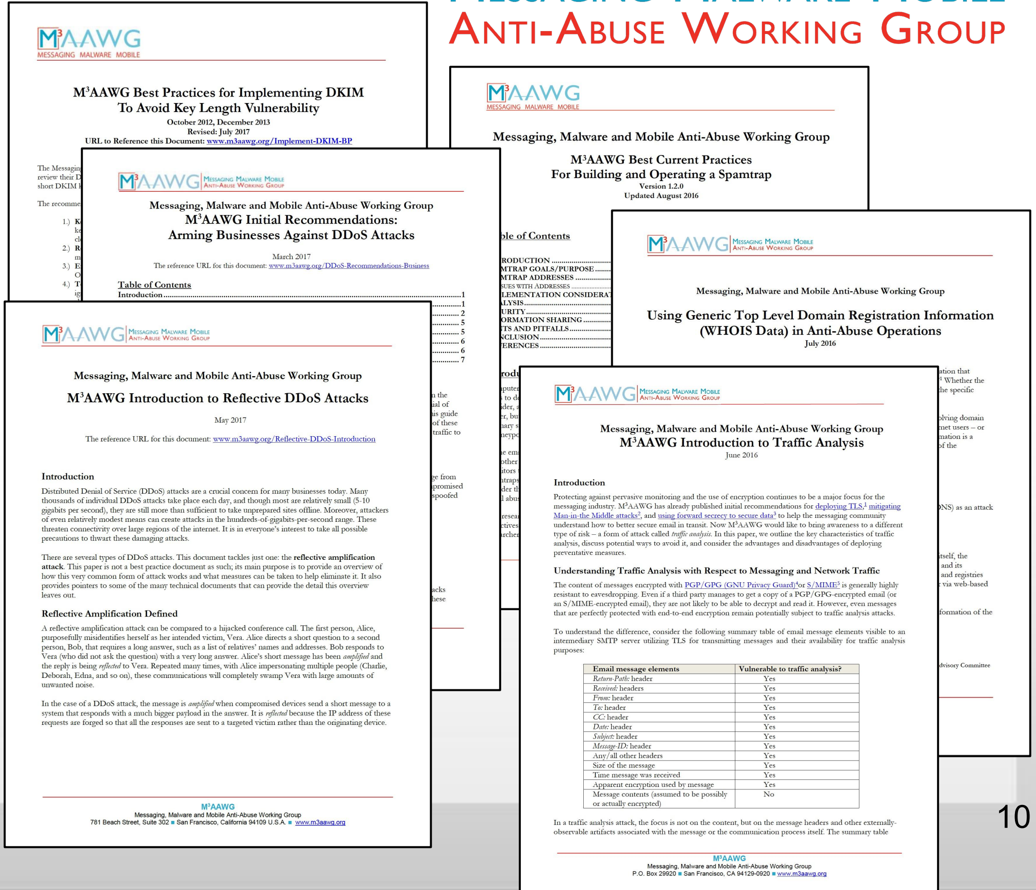
What Does M^3AAWG Do?

Distill Industry Knowledge into BCPs

Latest BCPs

M³AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP

- ➔ M^3AAWG Best Practices for Implementing DKIM to Avoid Key Length Vulnerability
- ➔ M^3AAWG Best Practices Introduction to Reflective DDOS Attacks
- ➔ M^3AAWG Initial Best Practices: Arming Businesses Against DDOS Attacks
- ➔ M^3AAWG Best Current Practices For Building and Operating a Spamtrap, Ver. 1.2.0
- ➔ Using Generic Top Level Domain Registration Information (WHOIS Data) in Anti-Abuse Operations
- ➔ M^3AAWG Introduction to Traffic Analysis



M³AAWG Best Practices for Implementing DKIM
To Avoid Key Length Vulnerability
October 2012, December 2013
Revised: July 2017
URL to Reference this Document: www.m3aawg.org/Implement-DKIM-BP

Messaging, Malware and Mobile Anti-Abuse Working Group
M³AAWG Initial Recommendations:
Arming Businesses Against DDoS Attacks
March 2017
The reference URL for this document: www.m3aawg.org/DDoS-Recommendations-Business

Table of Contents
Introduction 1

Messaging, Malware and Mobile Anti-Abuse Working Group
M³AAWG Best Current Practices
For Building and Operating a Spamtrap
Version 1.2.0
Updated August 2016

Messaging, Malware and Mobile Anti-Abuse Working Group
Using Generic Top Level Domain Registration Information
(WHOIS Data) in Anti-Abuse Operations
July 2016

Messaging, Malware and Mobile Anti-Abuse Working Group
M³AAWG Introduction to Reflective DDoS Attacks
May 2017
The reference URL for this document: www.m3aawg.org/Reflective-DDoS-Introduction

Introduction

Distributed Denial of Service (DDoS) attacks are a crucial concern for many businesses today. Many thousands of individual DDoS attacks take place each day, and though most are relatively small (5-10 gigabits per second), they are still more than sufficient to take unprepared sites offline. Moreover, attackers of even relatively modest means can create attacks in the hundreds-of-gigabits-per-second range. These threaten connectivity over large regions of the internet. It is in everyone's interest to take all possible precautions to thwart these damaging attacks.

There are several types of DDoS attacks. This document tackles just one: the **reflective amplification attack**. This paper is not a best practice document as such; its main purpose is to provide an overview of how this very common form of attack works and what measures can be taken to help eliminate it. It also provides pointers to some of the many technical documents that can provide the detail this overview leaves out.

Reflective Amplification Defined

A reflective amplification attack can be compared to a hijacked conference call. The first person, Alice, purposefully misidentifies herself as her intended victim, Vera. Alice directs a short question to a second person, Bob, that requires a long answer, such as a list of relatives' names and addresses. Bob responds to Vera (who did not ask the question) with a very long answer. Alice's short message has been *amplified* and the reply is being *reflected* to Vera. Repeated many times, with Alice impersonating multiple people (Charlie, Deborah, Edna, and so on), these communications will completely swamp Vera with large amounts of unwanted noise.

In the case of a DDoS attack, the message is *amplified* when compromised devices send a short message to a system that responds with a much bigger payload in the answer. It is *reflected* because the IP address of these requests are forged so that all the responses are sent to a targeted victim rather than the originating device.

M³AAWG
Messaging, Malware and Mobile Anti-Abuse Working Group
781 Beach Street, Suite 302 ■ San Francisco, California 94109 U.S.A. ■ www.m3aawg.org

Messaging, Malware and Mobile Anti-Abuse Working Group
M³AAWG Introduction to Traffic Analysis
June 2016

Introduction

Protecting against pervasive monitoring and the use of encryption continues to be a major focus for the messaging industry. M³AAWG has already published initial recommendations for deploying TLS,[1] mitigating Man-in-the Middle attacks[2], and using forward secrecy to secure data[3] to help the messaging community understand how to better secure email in transit. Now M³AAWG would like to bring awareness to a different type of risk – a form of attack called *traffic analysis*. In this paper, we outline the key characteristics of traffic analysis, discuss potential ways to avoid it, and consider the advantages and disadvantages of deploying preventative measures.

Understanding Traffic Analysis with Respect to Messaging and Network Traffic

The content of messages encrypted with PGP/GPG (GNU Privacy Guard)[4]or S/MIME[5] is generally highly resistant to eavesdropping. Even if a third party manages to get a copy of a PGP/GPG-encrypted email (or an S/MIME-encrypted email), they are not likely to be able to decrypt and read it. However, even messages that are perfectly protected with end-to-end encryption remain potentially subject to traffic analysis attacks.

To understand the difference, consider the following summary table of email message elements visible to an intermediary SMTP server utilizing TLS for transmitting messages and their availability for traffic analysis purposes:

Email message elements	Vulnerable to traffic analysis?
Return-Path: header	Yes
Received: headers	Yes
From: header	Yes
To: header	Yes
CC: header	Yes
Date: header	Yes
Subject: header	Yes
Message-ID: header	Yes
Any/all other headers	Yes
Size of the message	Yes
Time message was received	Yes
Apparent encryption used by message	Yes
Message contents (assumed to be possibly or actually encrypted)	No

In a traffic analysis attack, the focus is not on the content, but on the message headers and other externally-observable artifacts associated with the message or the communication process itself. The summary table

M³AAWG
Messaging, Malware and Mobile Anti-Abuse Working Group
P.O. Box 29920 ■ San Francisco, CA 94129-0920 ■ www.m3aawg.org

What Does M^{3}AAWG Do?

Who Do We Work With?

Unsolicited Commercial Enforcement Net

➔ Operation Safety Net

FIRST

➔ Anti-abuse business case and outreach

Internet Society

➔ Provided training material

i^{2}Coalition

➔ Hosting BCP

EastWest Institute

➔ Outreach and Transnational Policy Engagement

Anti-Phishing Working Group (APWG)

➔ Anti-Phishing Best Practices for ISPs and Mailbox Providers

LAC-AAWG

➔ **Updating and developing BCPs to reflect LAC dynamics**

JP-AAWG Development

➔ **Working with regional orgs and industry partners**

AF-AAWG Development

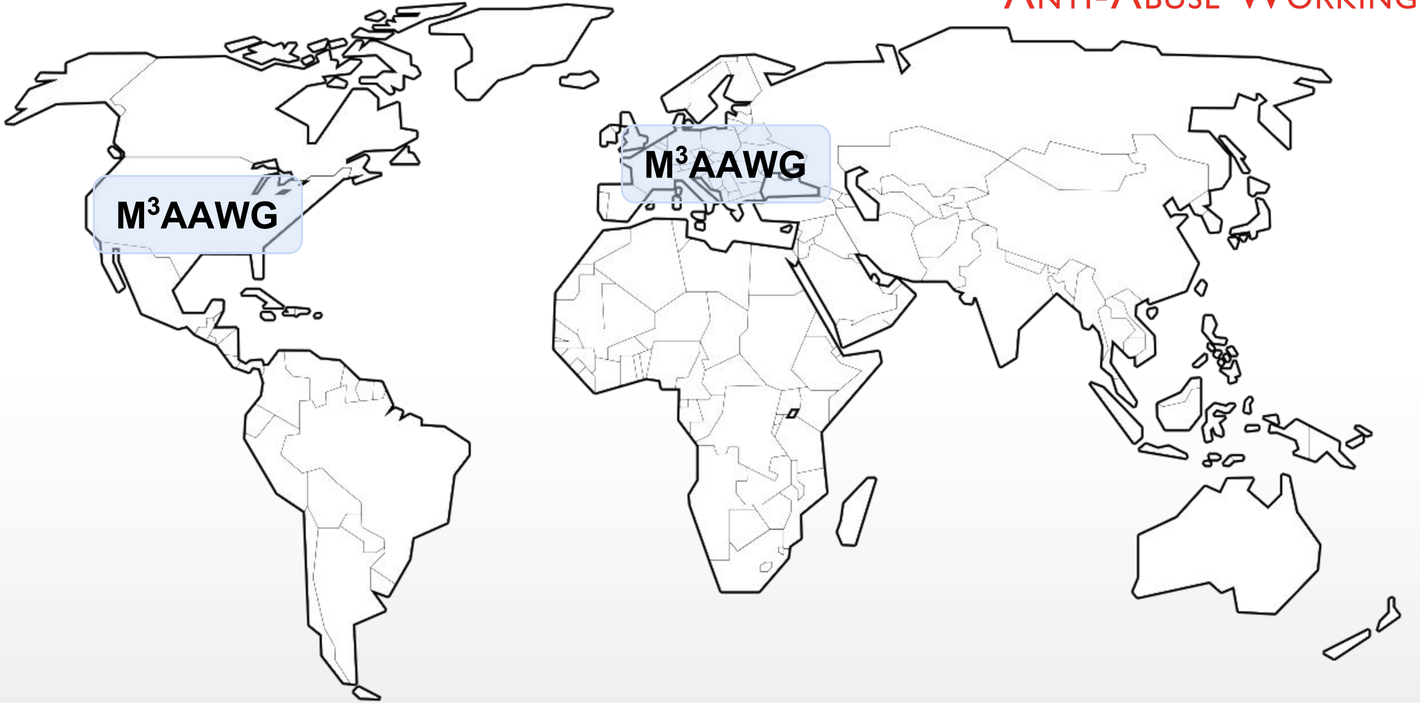
➔ **In progress with AfricaCERT**

JP-AAWG

Outreach:
Anti-Abuse Working Group (AAWG)
Development

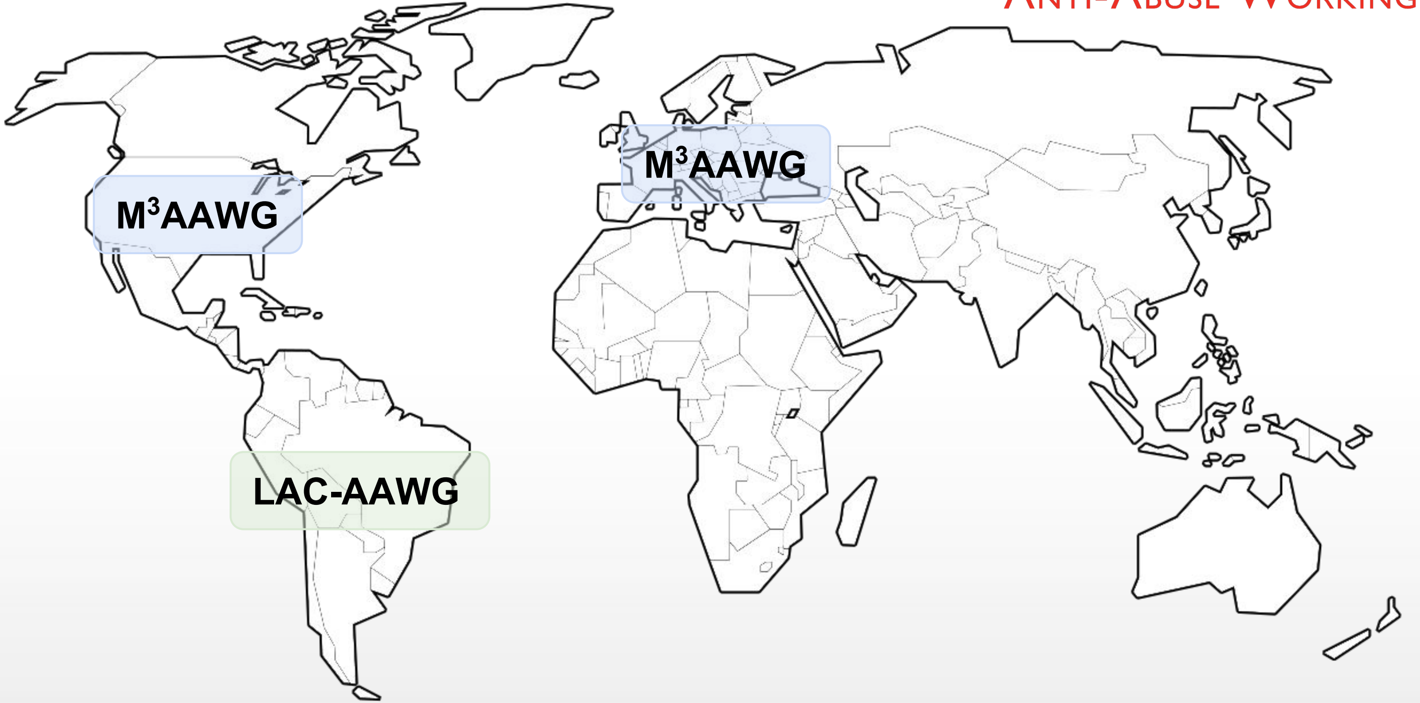
Regional AAWG Development
Contributing to *Peer* Working Groups

M3AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP

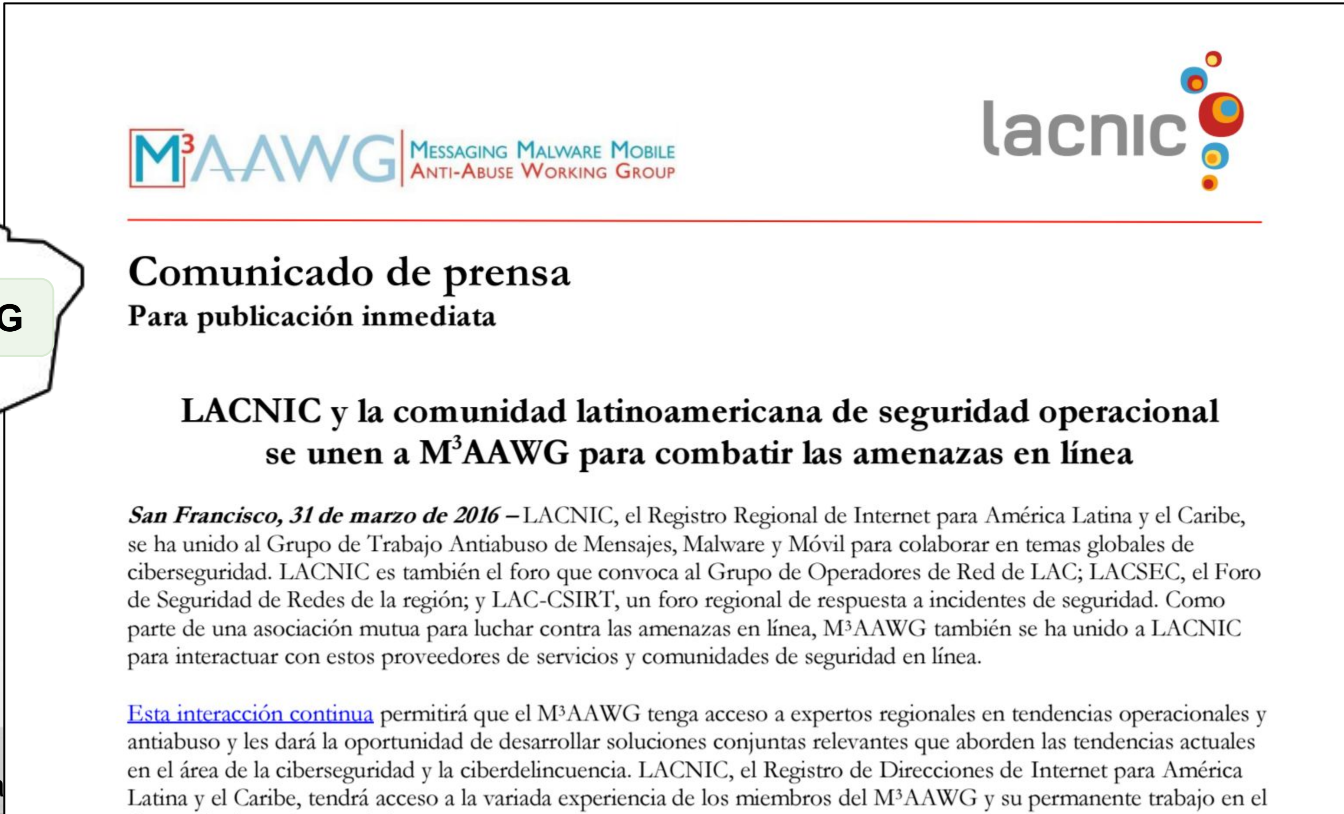


Regional AAWGs Development
Contributing to *Peer* Working Groups

M3AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP



Regional AAWGs Development
Peer Working Group in LAC



Comunicado de prensa

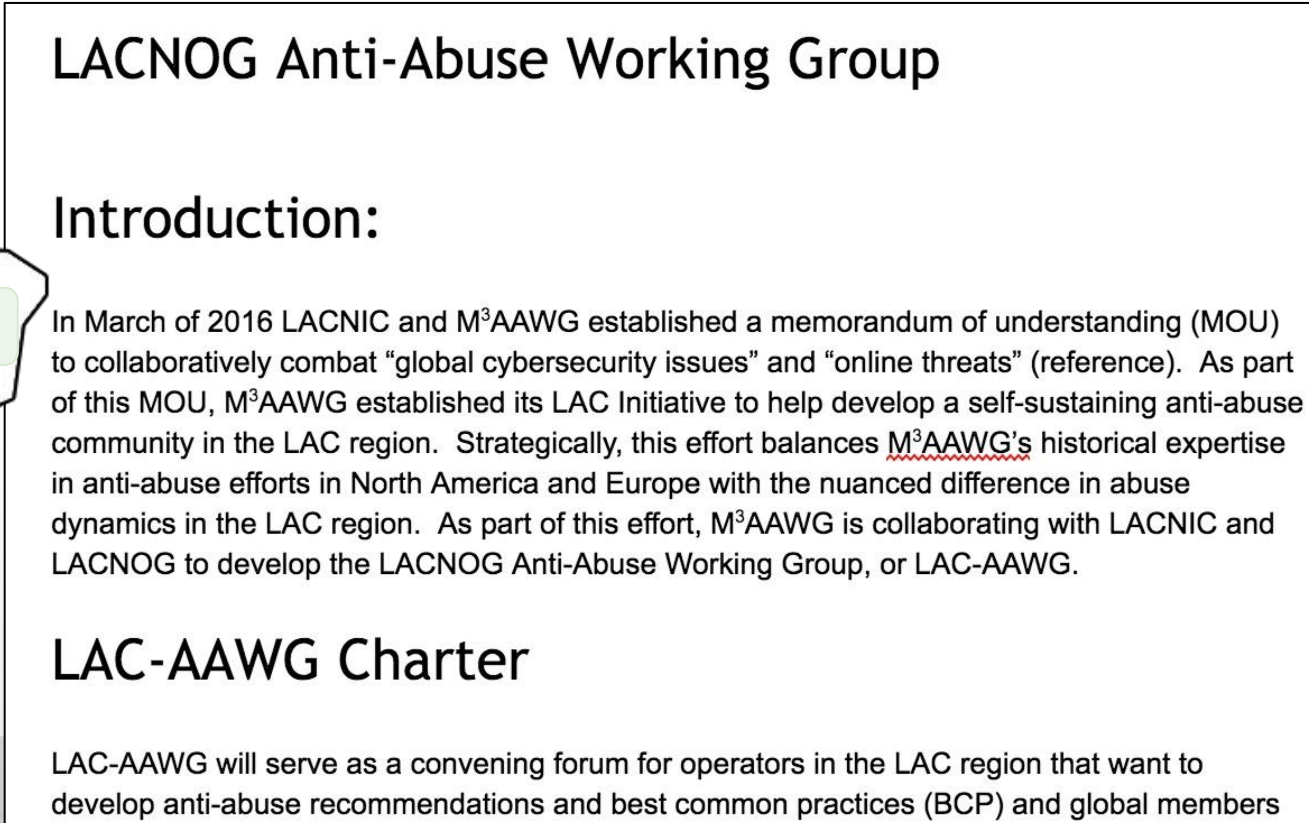
Para publicación inmediata

LACNIC y la comunidad latinoamericana de seguridad operacional se unen a M^{3}AAWG para combatir las amenazas en línea

San Francisco, 31 de marzo de 2016 – LACNIC, el Registro Regional de Internet para América Latina y el Caribe, se ha unido al Grupo de Trabajo Antiabuso de Mensajes, Malware y Móvil para colaborar en temas globales de ciberseguridad. LACNIC es también el foro que convoca al Grupo de Operadores de Red de LAC; LACSEC, el Foro de Seguridad de Redes de la región; y LAC-CSIRT, un foro regional de respuesta a incidentes de seguridad. Como parte de una asociación mutua para luchar contra las amenazas en línea, M^{3}AAWG también se ha unido a LACNIC para interactuar con estos proveedores de servicios y comunidades de seguridad en línea.

Esta interacción continua permitirá que el M^{3}AAWG tenga acceso a expertos regionales en tendencias operacionales y antiabuso y les dará la oportunidad de desarrollar soluciones conjuntas relevantes que aborden las tendencias actuales en el área de la ciberseguridad y la ciberdelincuencia. LACNIC, el Registro de Direcciones de Internet para América Latina y el Caribe, tendrá acceso a la variada experiencia de los miembros del M^{3}AAWG y su permanente trabajo en el

Regional AAWGs Development
Peer Working Group in LAC



LACNOG Anti-Abuse Working Group

Introduction:

In March of 2016 LACNIC and M^{3}AAWG established a memorandum of understanding (MOU) to collaboratively combat "global cybersecurity issues" and "online threats" (reference). As part of this MOU, M^{3}AAWG established its LAC Initiative to help develop a self-sustaining anti-abuse community in the LAC region. Strategically, this effort balances M^{3}AAWG's historical expertise in anti-abuse efforts in North America and Europe with the nuanced difference in abuse dynamics in the LAC region. As part of this effort, M^{3}AAWG is collaborating with LACNIC and LACNOG to develop the LACNOG Anti-Abuse Working Group, or LAC-AAWG.

LAC-AAWG Charter

LAC-AAWG will serve as a convening forum for operators in the LAC region that want to develop anti-abuse recommendations and best common practices (BCP) and global members

Regional AAWGs Development
Peer Working Group in LAC

M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

AAWG Principles and Objectives

Promulgate anti-abuse norms and principles

Further develop regional anti-abuse expertise

- ➔ Anti-abuse research
- ➔ BCPs within and across regions

Convene anti-abuse actors

- ➔ operators
- ➔ public policy
- ➔ LE

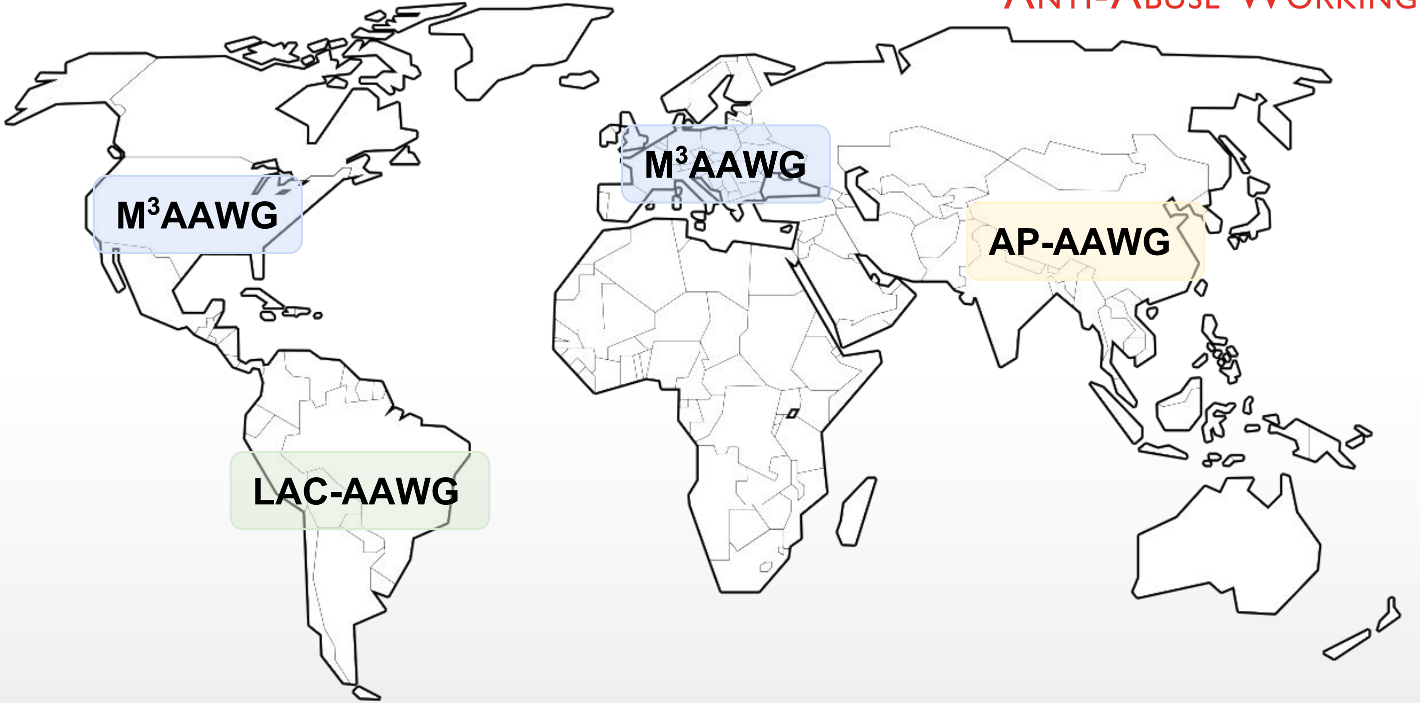
Represent regional anti-abuse expertise

Exchange expertise

- ➔ among operators within the regions
- ➔ globally, among peer regions

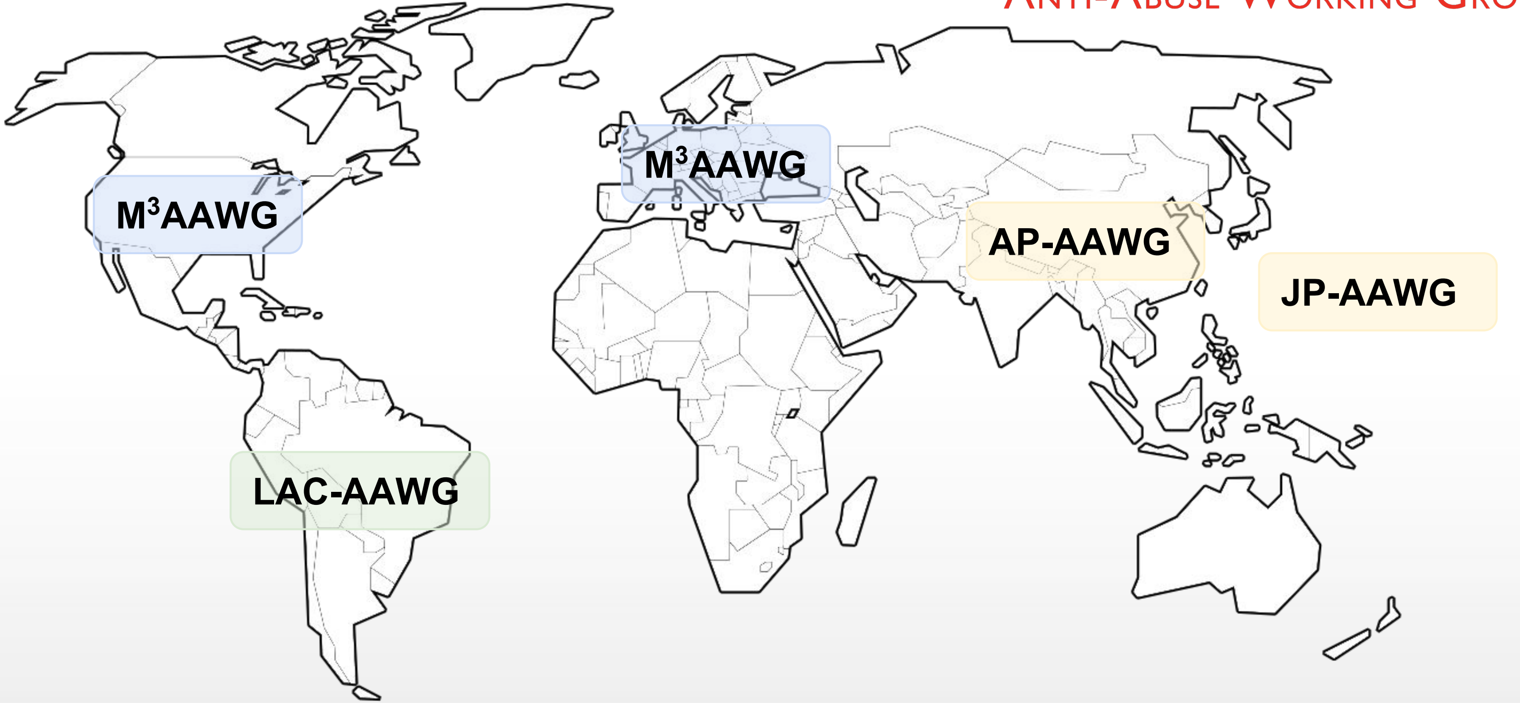
Regional AAWGs Development
Contributing to *Peer* Working Groups

M³AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP



Regional AAWGs Development
Contributing to *Peer* Working Groups

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group



Regional AAWGs Development
Peer Working Group in Japan

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Establishing New Organization

Content Sharing

- ➔ Bringing translated content to Japanese audiences
- ➔ Japanese members translating existing BCPs

Establishing initial membership set

- ➔ 75+ attendees at first two meetings
- ➔ In addition to development team, involvement from Equalitia, Rakuten, SoftBank, and others in region

Government Support for Olympics Milestone

- ➔ Yasuhiko Taniwaki, the Director-General for Information Security has provided endorsement and expressed his desire for cooperative working relationship

JPNIC

twoFive

MIC 総務省 Ministry of Internal Affairs and Communications

CLOUDMARK® Intelligent Threat Protection

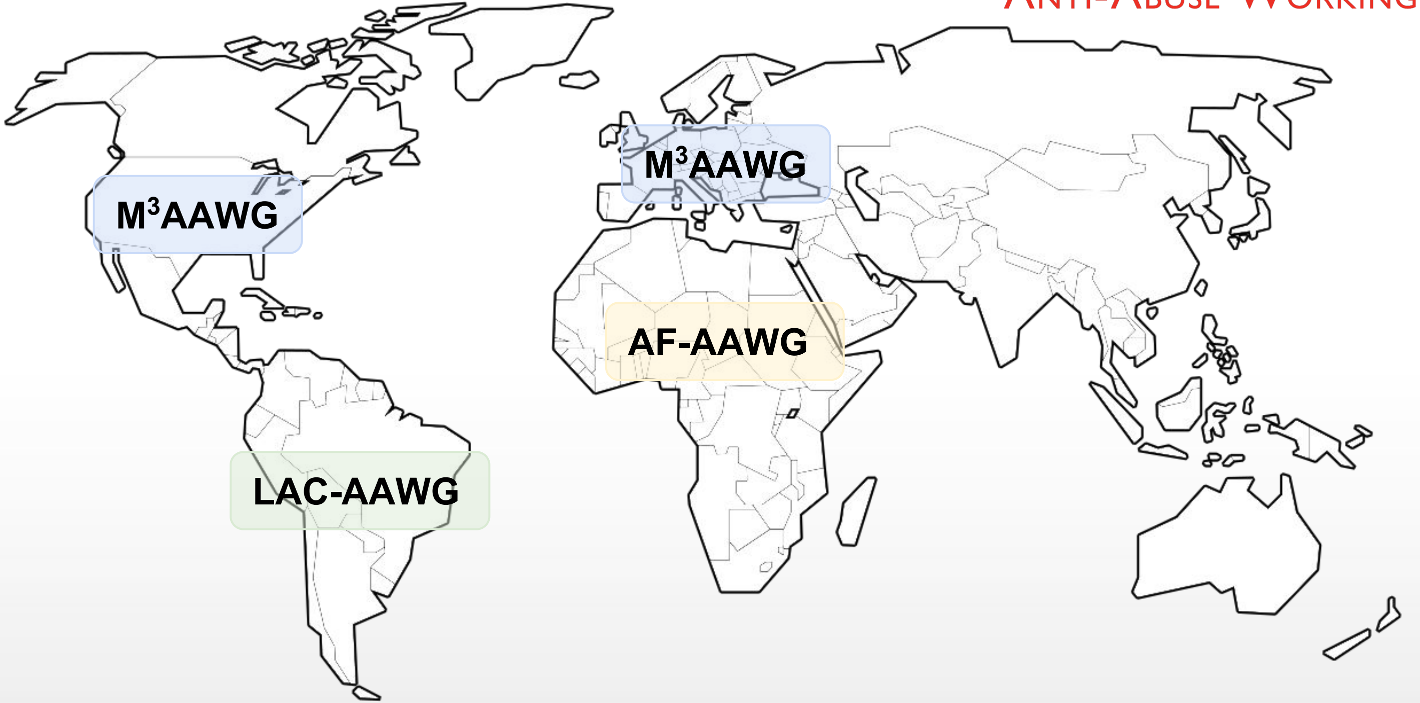
APNIC

IIJ Internet Initiative Japan

Vade Secure Predictive Email Defense

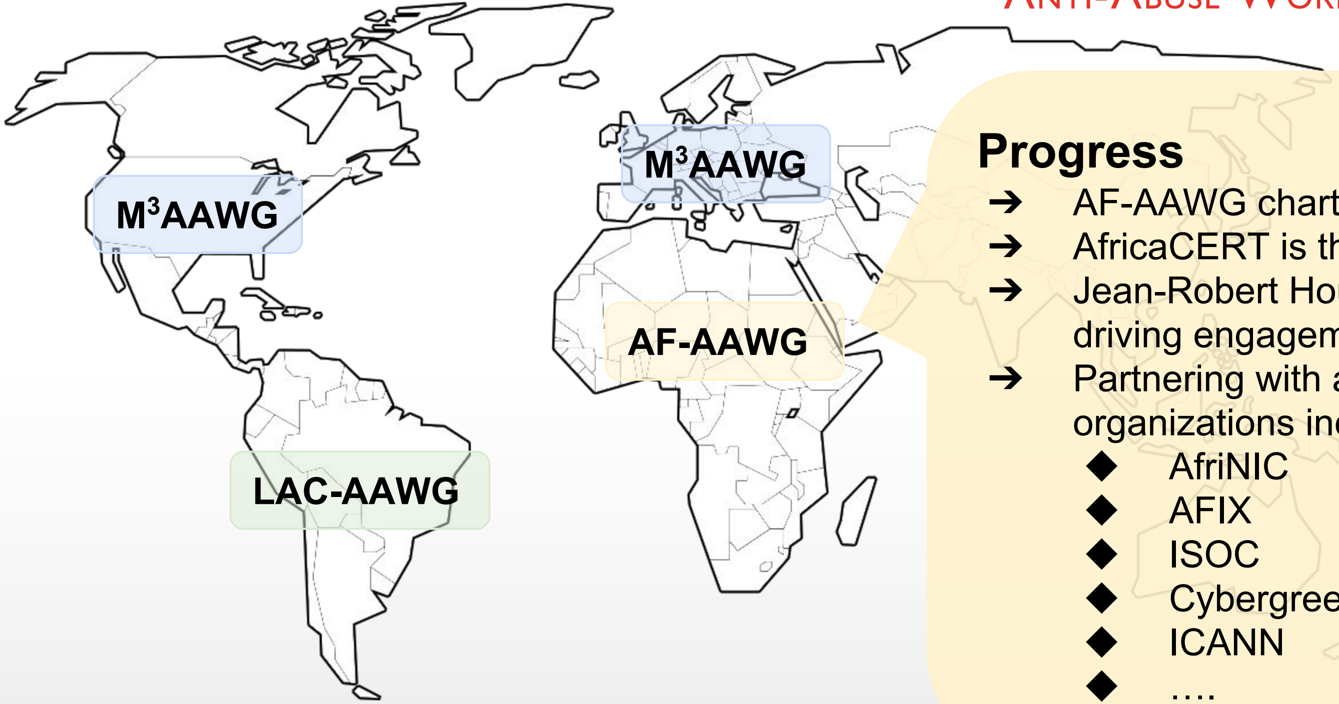
Regional AAWGs Development
Peer Working Group in AF

M3AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP



Regional AAWGs Development
Peer Working Group in AF

M³AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP



Progress

- ➔ AF-AAWG charter drafted
- ➔ AfricaCERT is the home
- ➔ Jean-Robert Hountomy is driving engagement
- ➔ Partnering with a variety of organizations including
  - ◆ AfriNIC
  - ◆ AFIX
  - ◆ ISOC
  - ◆ Cybergreen
  - ◆ ICANN
  - ◆ ….

Questions?
Comments?
Volunteers?!!?

jesse.sowell@gmail.com

MANRS

Mutually Agreed Norms for Routing Security

Michuki Mwangi

mwangi@isoc.org

The Problem

A Routing Security Overview

Routing Incidents are Increasing

In 2017 alone, 14,000 routing outages or attacks – such as hijacking, leaks, and spoofing – led to a range of problems including stolen data, lost revenue, reputational damage, and more.

About 40% of all network incidents are attacks, with the mean duration per incident lasting 19 hours.

Incidents are global in scale, with one operator’s routing problems cascading to impact others.

Routing Incidents Cause Real World Problems

Insecure routing is one of the most common paths for malicious threats.

Attacks can take anywhere from hours to months to recognize.

Inadvertent errors can take entire countries offline, while attackers can steal an individual's data or hold an organization's network hostage.

The Basics: How Routing Works

There are ~60,000 networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach.

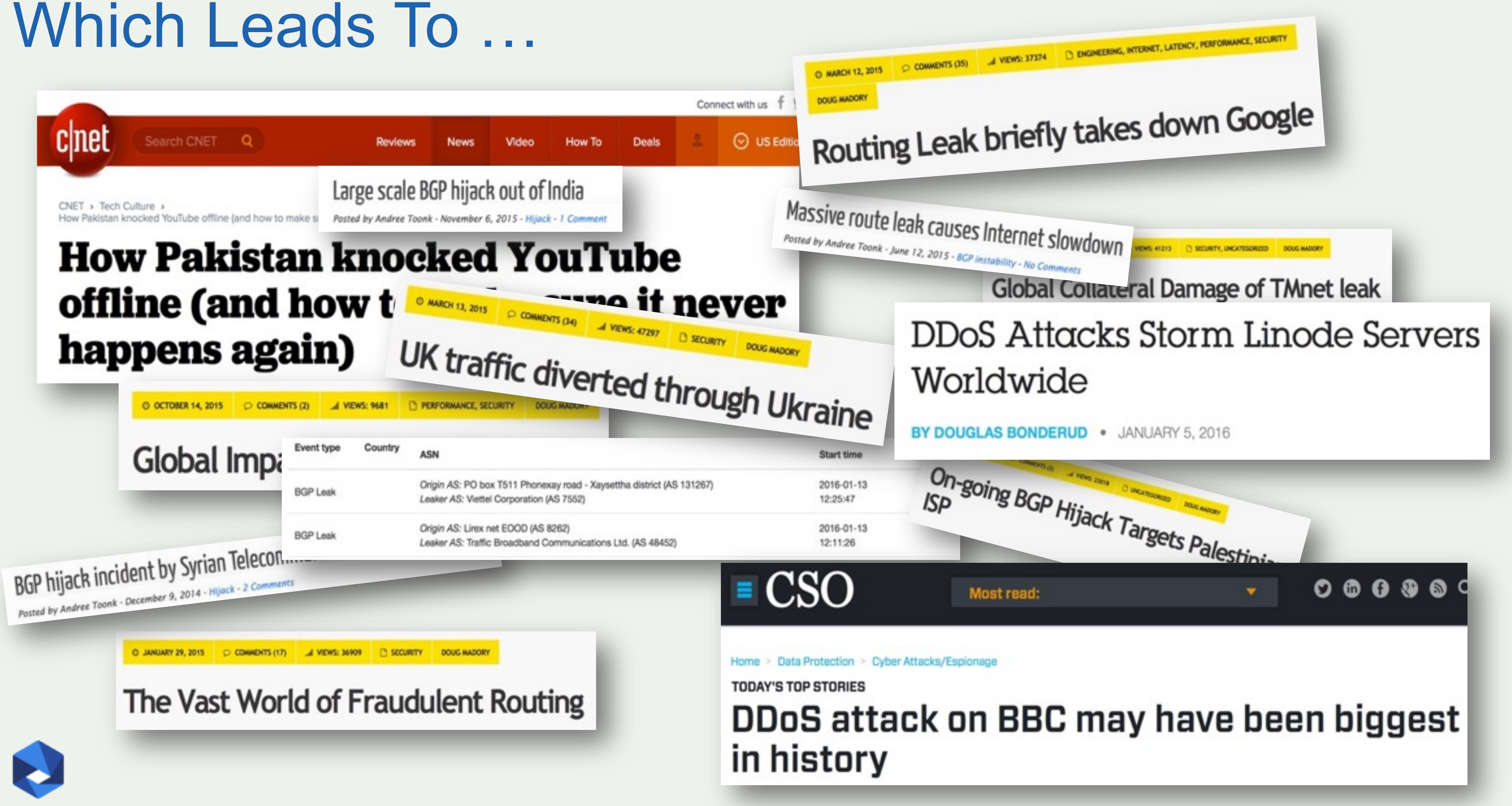
Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

The Honor System: Routing Issues

Border Gateway Protocol (BGP) is based entirely on trust between networks

- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

Which Leads To …



Connect with us

c|net · Search CNET · Reviews · News · Video · How To · Deals · US Editio

CNET › Tech Culture › How Pakistan knocked YouTube offline (and how to make s

How Pakistan knocked YouTube offline (and how t… …sure it never happens again)

Large scale BGP hijack out of India

Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment

MARCH 12, 2015 · COMMENTS (35) · VIEWS: 37374 · ENGINEERING, INTERNET, LATENCY, PERFORMANCE, SECURITY · DOUG MADORY

Routing Leak briefly takes down Google

Massive route leak causes Internet slowdown

Posted by Andree Toonk - June 12, 2015 - BGP instability - No Comments

VIEWS: 41213 · SECURITY, UNCATEGORIZED · DOUG MADORY

Global Collateral Damage of TMnet leak

MARCH 13, 2015 · COMMENTS (34) · VIEWS: 47297 · SECURITY · DOUG MADORY

UK traffic diverted through Ukraine

DDoS Attacks Storm Linode Servers Worldwide

BY DOUGLAS BONDERUD • JANUARY 5, 2016

OCTOBER 14, 2015 · COMMENTS (2) · VIEWS: 9681 · PERFORMANCE, SECURITY · DOUG MADORY

Global Impa

Event type	Country	ASN	Start time
BGP Leak		*Origin AS:* PO box T511 Phonexay road - Xaysettha district (AS 131267) *Leaker AS:* Viettel Corporation (AS 7552)	2016-01-13 12:25:47
BGP Leak		*Origin AS:* Lirex net EOOD (AS 8262) *Leaker AS:* Traffic Broadband Communications Ltd. (AS 48452)	2016-01-13 12:11:26

COMMENTS (2) · VIEWS: 23018 · UNCATEGORIZED · DOUG MADORY

On-going BGP Hijack Targets Palestini ISP

BGP hijack incident by Syrian Telecom

Posted by Andree Toonk - December 9, 2014 - Hijack - 2 Comments

JANUARY 29, 2015 · COMMENTS (17) · VIEWS: 36909 · SECURITY · DOUG MADORY

The Vast World of Fraudulent Routing

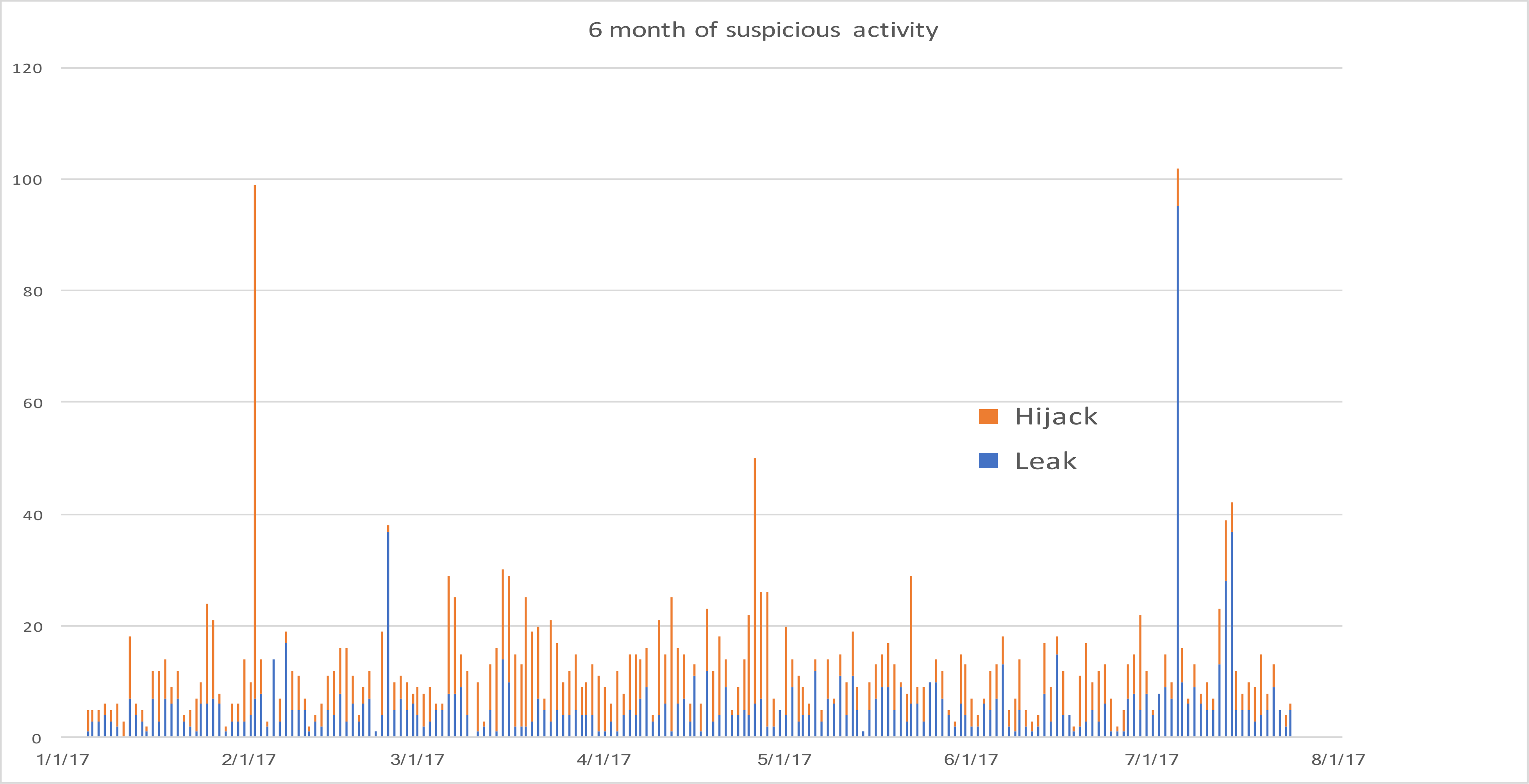
CSO · Most read:

Home > Data Protection > Cyber Attacks/Espionage

TODAY'S TOP STORIES

DDoS attack on BBC may have been biggest in history

No Day Without an Incident



http://bgpstream.com/

The Threats: What’s Happening?

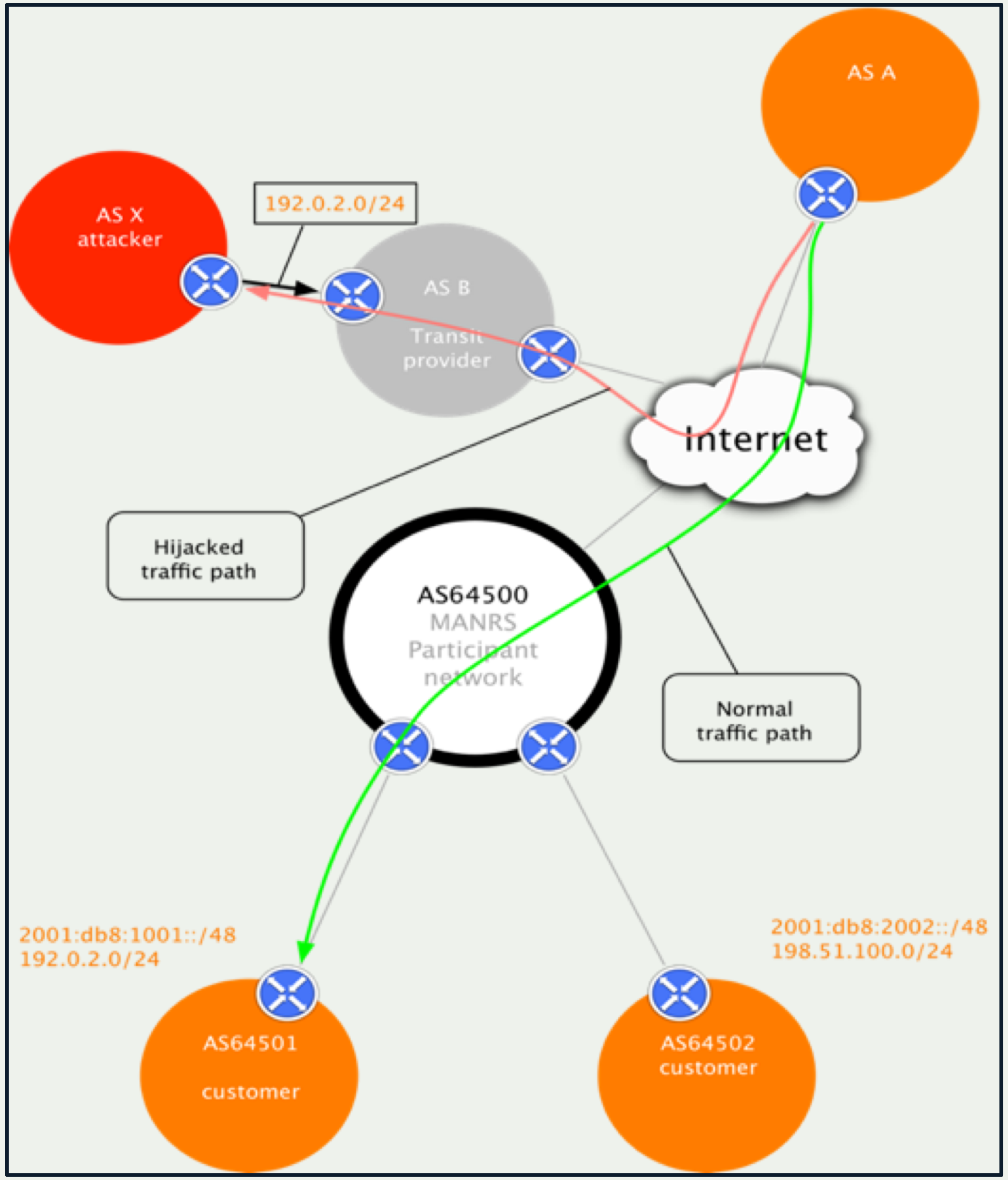
Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	Stronger filtering policies
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	Stronger filtering policies
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks	Source address validation

Prefix/Route Hijacking

Route hijacking, also known as “BGP hijacking” when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretending that a server or network is their client. This routes traffic to a network operator, when another real route is available.

Example: The 2008 YouTube hijack; an attempt to block YouTube through route hijacking led to much of the traffic to YouTube being dropped around the world.

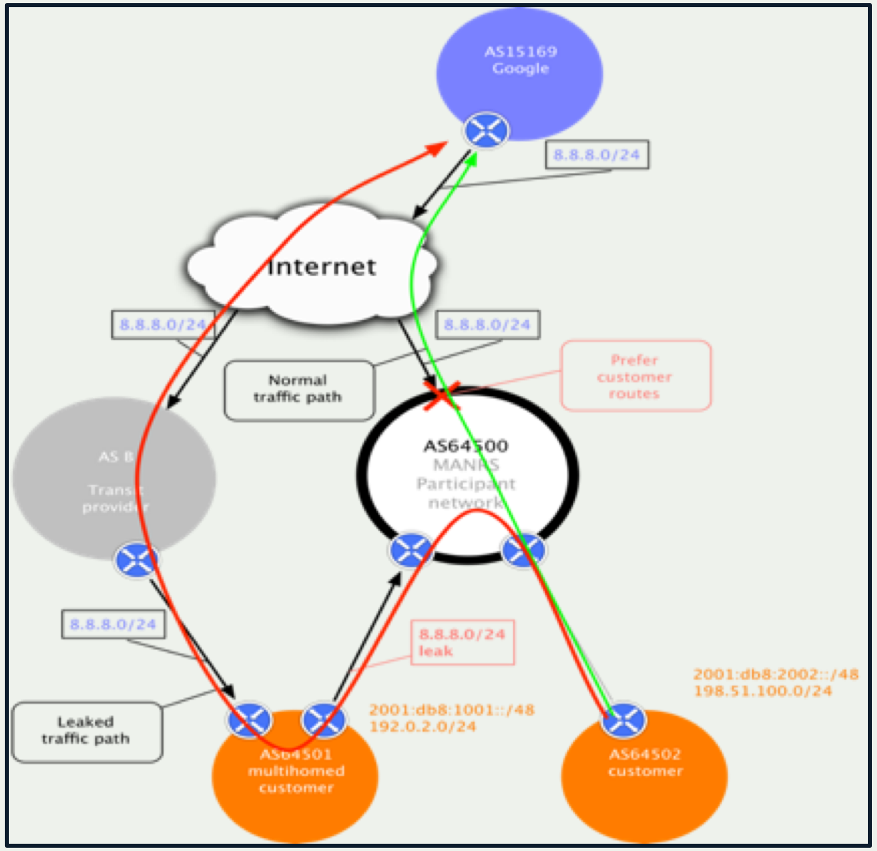
Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting false announcements).



Route Leak

A route leak is a problem where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that is has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers. With one sending traffic now through it to get to the other.

Example: 2015, Malaysia Telecom and Level 3, a major backbone provider. Malaysia Telecom told one of Level 3's networks that it was capable of delivering traffic to anywhere on the Internet. Once Level 3 decided the route through Malaysia Telecom looked like the best option, it diverted a huge amount of traffic to Malaysia Telecom.

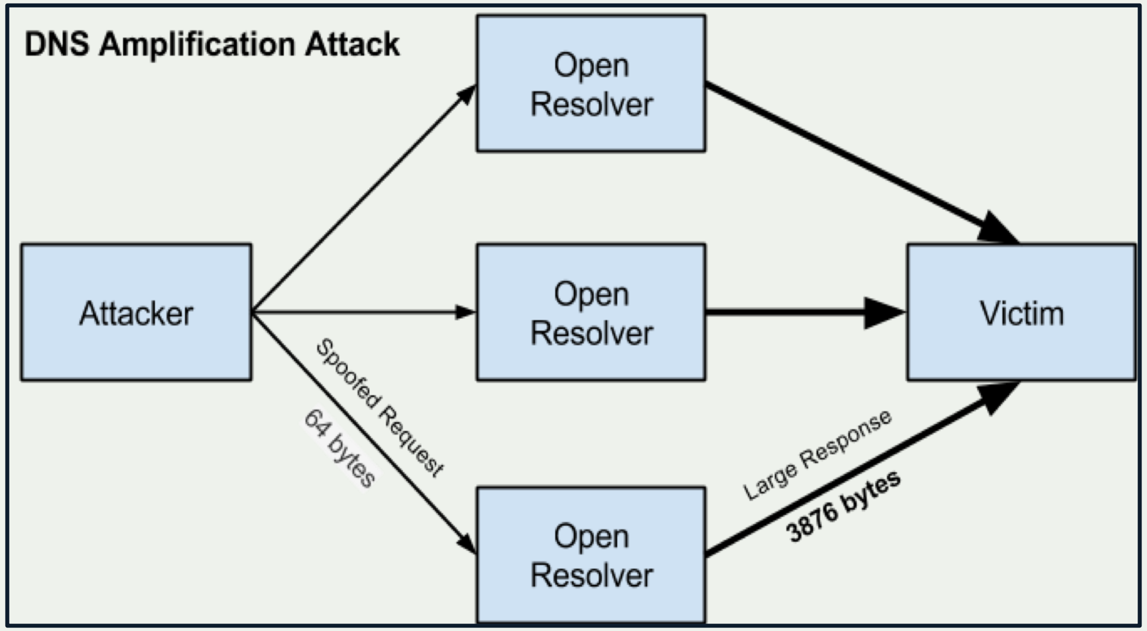


Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting announcements that don't make sense).

IP Address Spoofing

IP address spoofing is used to hide the true identity of the server or to impersonate another server. This technique can be used to amplify an attack.

Example: DNS amplification attack. By sending multiple spoofed requests to different DNS resolvers, an attacker can prompt many responses from the DNS resolver to be sent to a target, while only using one system to attack.



Fix: Source address validation: systems for source address validation can help tell if the end users and customer networks have correct source IP addresses (combined with filtering).

Tools to Help

- Prefix and AS-PATH filtering
- RPKI validator, IRR toolset, IRRPT, BGPQ3
- BGPSEC is standardized

But…

- Not enough deployment
- Lack of reliable data

We need a standard approach to improving routing security.

Collaboration and Consensus

Your security is in someone else's hands. The actions of others directly impact you and your network security (and vice versa).

Why should they help you? You can start by helping them.

Where is the line between good and bad routing security?

We need globally recognized security expectations for all network operators to raise the bar on routing security.

We Are In This Together

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure.

Your network’s safety depends on a routing infrastructure that weeds out bad actors and accidental misconfigurations that wreak havoc on the Internet.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.

The Solution: Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to eliminate the most common routing threats

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

Mutually Agreed Norms for Routing Security

MANRS defines four simple but concrete actions that network operators must implement to dramatically improve Internet security and reliability.

- The first two operational improvements eliminate the root causes of common routing issues and attacks, while the second two procedural steps improve mitigation and decrease the likelihood of future incidents.

MANRS Actions

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

Benefits of Improved Routing Security

Signals an organization’s security-forward posture and can eliminate SLA violations that reduce profitability or cost customer relationships.

Heads off routing incidents, helping networks readily identify and address problems with customers or peers.

Improves a network’s operational efficiency by establishing better and cleaner peering communication pathways, while also providing granular insight for troubleshooting.

Implementing best practices alleviates many routing concerns of security-focused enterprises and other customers.

Everyone Benefits

Joining MANRS means joining a community of security-minded network operators committed to making the global routing infrastructure more robust and secure.

Consistent MANRS adoption yields steady improvement, but we need more networks to implement the actions and more customers to demand routing security best practices.

The more network operators apply MANRS actions, the fewer incidents there will be, and the less damage they can do.

MANRS is an Important Step

Security is a process, not a state. MANRS provides a structure and a consistent approach to solving security issues facing the Internet.

MANRS is the minimum an operator should consider, with low risk and cost-effective actions.

MANRS is not a one-stop solution to all of the Internet's routing woes, but it is an important step toward a globally robust and secure routing infrastructure.

Why join MANRS?

Improve your security posture and reduce the number and impact of routing incidents

Join a community of security-minded operators working together to make the Internet better

Use MANRS as a competitive differentiator

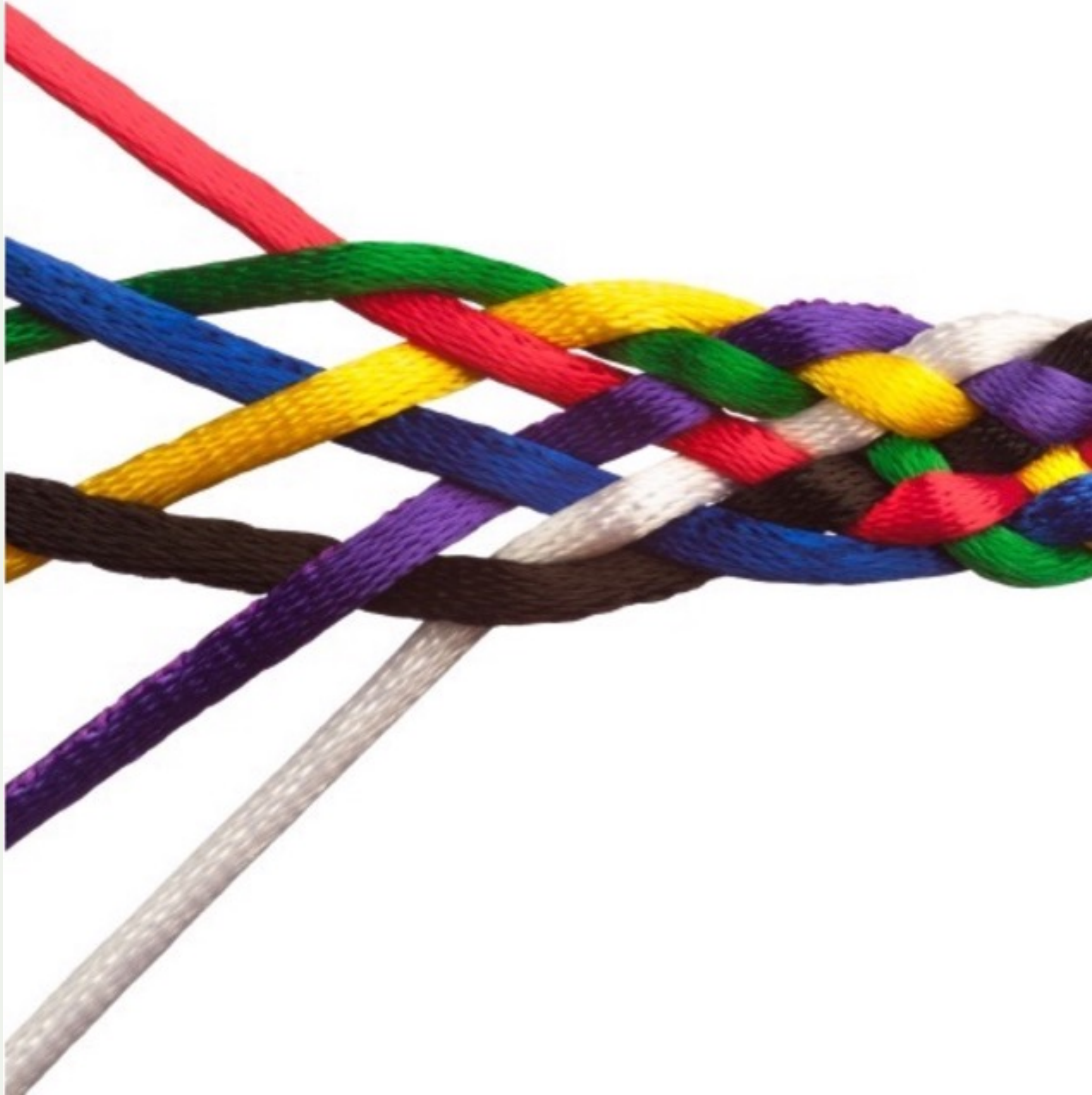
Join Us

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.
- We may ask questions and run tests

Get Involved in the Community

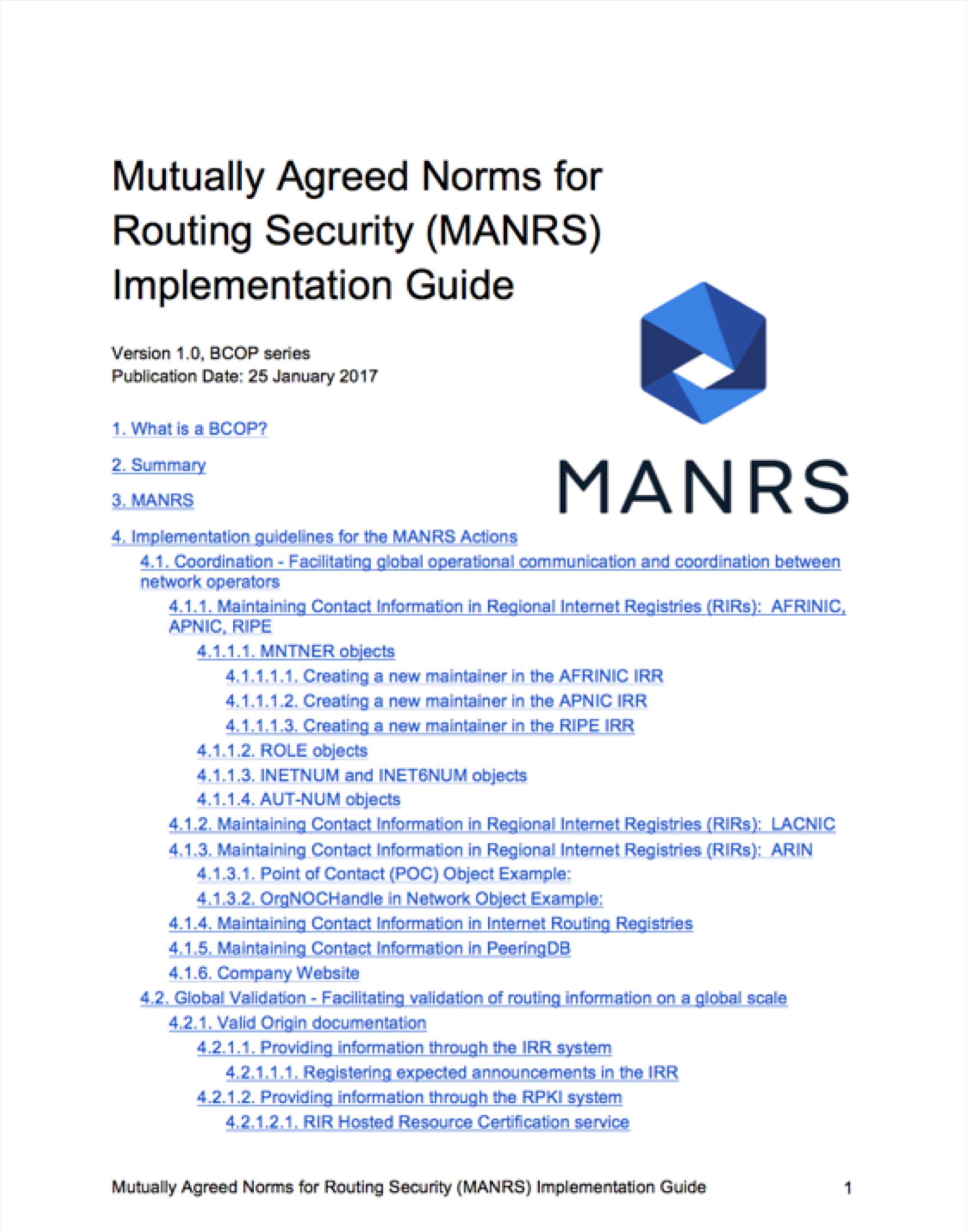
- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the document and promote MANRS objectives



MANRS Implementation Guide

If you’re not ready to join yet, implementation guidance is available to help you.

- Based on Best Current Operational Practices deployed by network operators around the world
- https://www.manrs.org/bcop/



Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

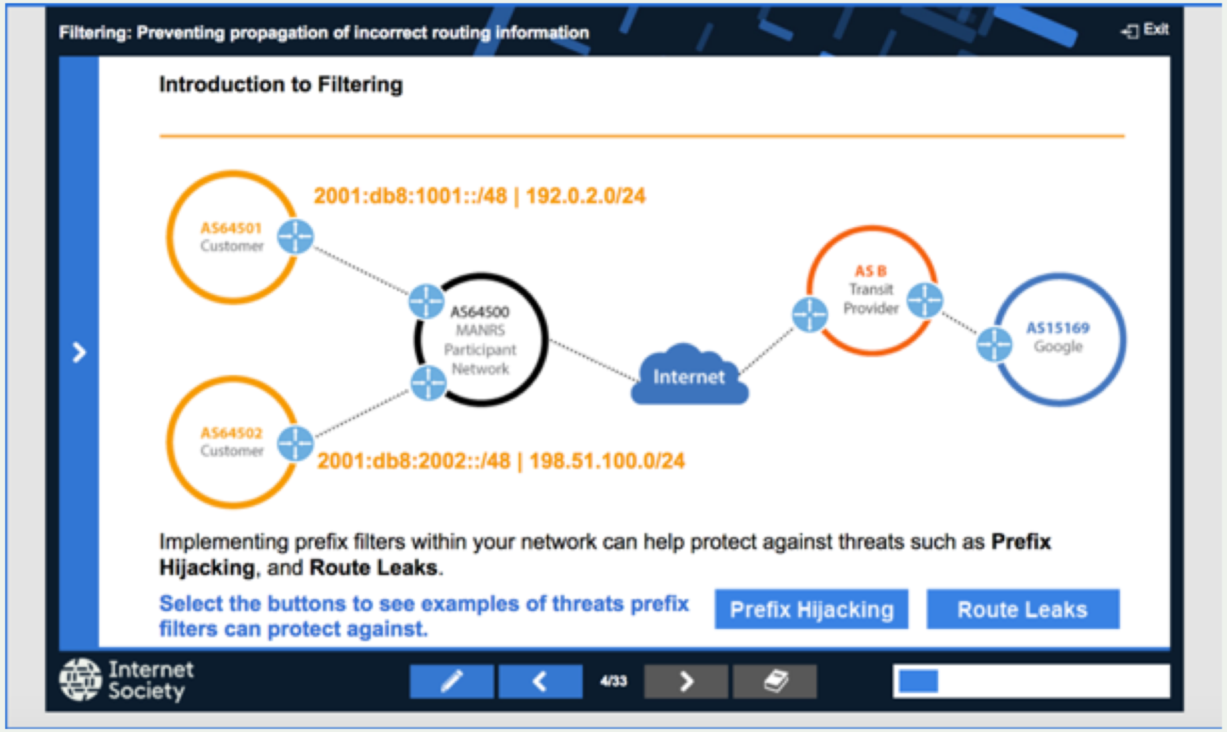
MANRS Training Modules

6 training modules based on information in the Implementation Guide.

Walks through the tutorial with a test at the end of each module.

Working with and looking for partners that are interested in integrating it in their curricula.

https://www.manrs.org/tutorials



Filtering: Preventing propagation of incorrect routing information

Introduction to Filtering

Implementing prefix filters within your network can help protect against threats such as **Prefix Hijacking**, and **Route Leaks**.

Select the buttons to see examples of threats prefix filters can protect against.

What’s Next: MANRS IXP Partnership Programme

There is synergy between MANRS and IXPs

- IXPs form a community with a common operational objective
- MANRS is a reference point with a global presence – useful for building a “safe neighborhood”

How can IXPs contribute?

- Technical measures: Route Server with validation, alerting on unwanted traffic, providing debugging and monitoring tools
- Social measures: MANRS ambassadors, local audit as part of the on-boarding process
- A development team is working on a set of useful actions

LEARN MORE:

https://www.manrs.org

Thank you.

Michuki Mwangi

Mwangi@isoc.org

manrs.org

AFRICA INTERNET SUMMIT'18
DAKAR SENEGAL
29 APRIL - 11 MAY 2018

AfricaCERT
United in promoting cyber security in Africa

Incident Response at Internet Scale

By
Marcus K. G. Adomey

OVERVIEW

❑ Incident Responses

❑ Actions

❑ Core Values

Incident Response

Type of incidents

Type of Issues

- DOS
- Phishing
- Intrusion attempts
- Net Scanning
- Website Intrusion & Malware Propagation

Type of incidents

Statistics of Reported Incident

2014	-	17073	
2015	-	7399	
2016	-	8072	
2017	-	7780	
2018	-	2396	(Jan to April)

Type of incidents

We have noticed

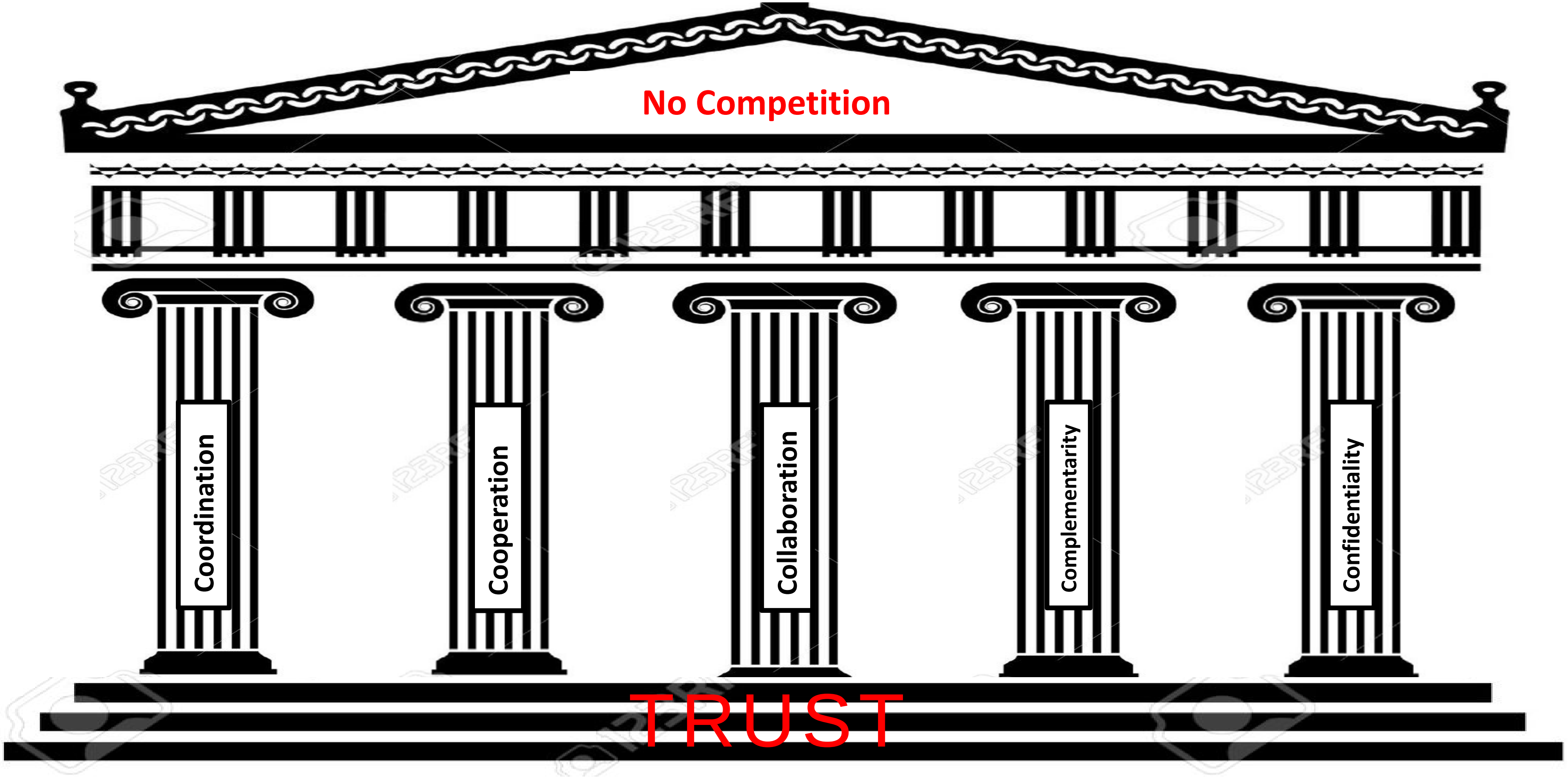
- Non- usage of good cyber hygiene practices
- Default passwords
- Unpatched equipment
- Bad configuration
- Unsecure products
- Most of the time we are the one notifying that something is going on

Actions

- Capacity building for incident management skills at all level
- Capacity building for Policy Makers
- More coordinated approach with stakeholders involved in Internet Health
- Recognitions inspired by the way vendors recognized Security researchers
- Development of incentives to motivate good cyber fitness

Core Values

Core Values



No Competition

Coordination

Cooperation

Collaboration

Complementarity

Confidentiality

TRUST

Thank you