

Что мы знаем о надежности глобальной системы маршрутизации и как сделать ее лучше?

Андрей Робачевский, Internet Society

robachevsky@isoc.org

Глобальная инфраструктура Интернета

Глобальная община

- Мы все используем ее и зависим от нее

Глобальные эффекты

- Ошибки конфигурации, атаки, ложная информация
- Пример: Indosat

Связности и взаимозависимость

- «Входящие» и «исходящие» риски
- Пример: атака на Спамхаус 300Гб/с

Сложность проблемы

Технические факторы

- Технологические решения
- Общее понимание проблемы
- Общее понимание решений

Экономические факторы

- Внешние эффекты (экстерналии), информационная асимметрия

Социальные факторы

- Коллективная ответственность
- Дух сотрудничества

Routing resilience survey

Риски глобальной системы маршрутизации?

Частота происшествий?

- Совещание по измерению надежности системы маршрутизации
<http://www.internetsociety.org/doc/report-routing-resiliency-measurements-workshop>
- Частота зависит от порога фильтрации ложных сигналов

Каков эффект?

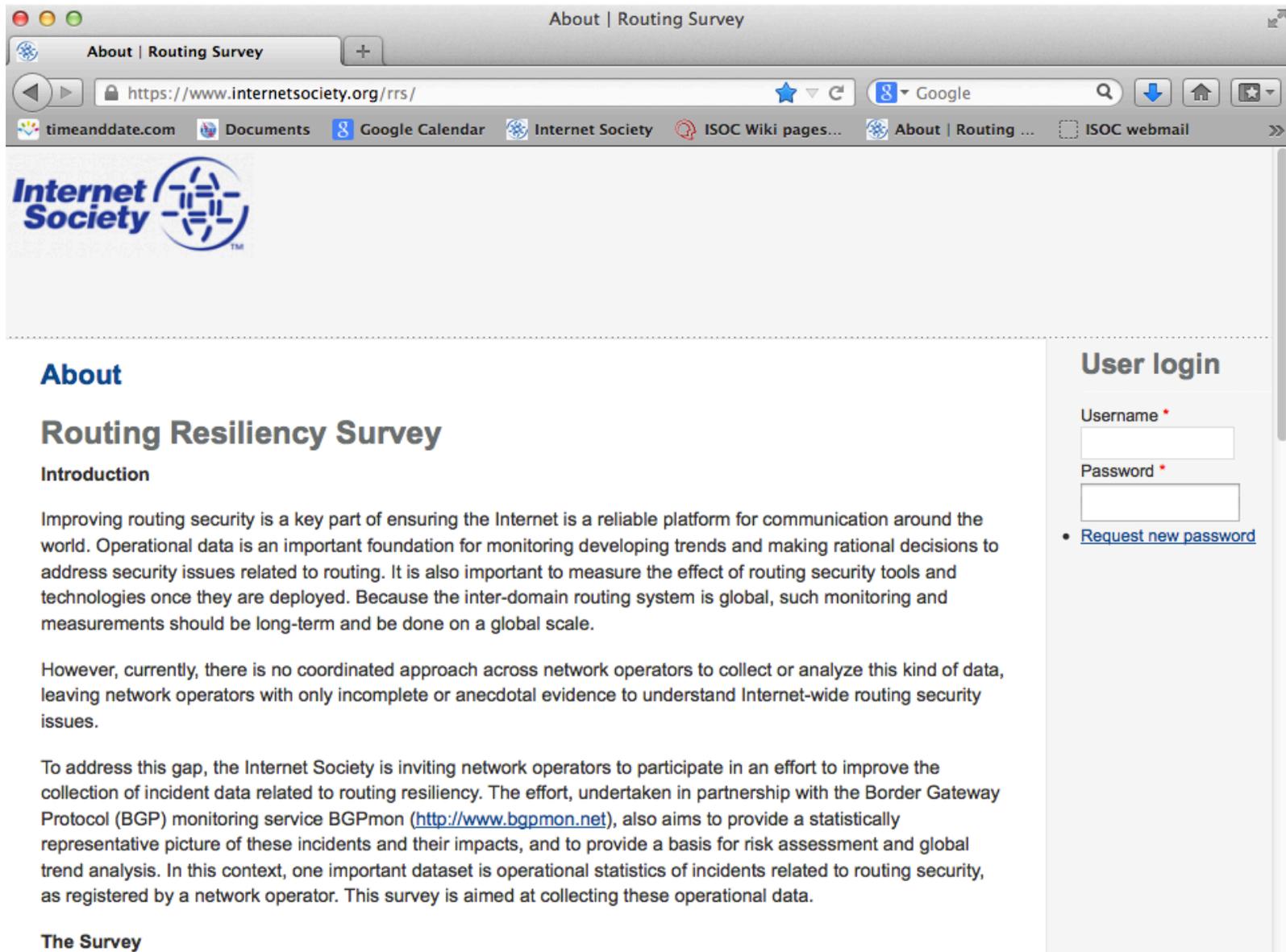
- Данные недоступны, либо отсутствуют, либо не разглашаются
- Оценка рисков основана на догадках

Затрагивает ли это вашу сеть?

- Детектирование инцидентов
- Исключение ложных сигналов
- Оценка эффекта

Адекватно ли защищена ваша сеть?

https://www.internetsociety.org/rrs/



The screenshot shows a web browser window with the title "About | Routing Survey". The address bar displays "https://www.internetsociety.org/rrs/". The browser's bookmark bar includes "timeanddate.com", "Documents", "Google Calendar", "Internet Society", "ISOC Wiki pages...", "About | Routing ...", and "ISOC webmail". The page content features the Internet Society logo at the top left. Below the logo, the heading "About" is followed by "Routing Resiliency Survey" and "Introduction". The main text discusses the importance of routing security and the survey's goal. A "User login" section on the right contains input fields for "Username" and "Password", and a link for "Request new password".

About

Routing Resiliency Survey

Introduction

Improving routing security is a key part of ensuring the Internet is a reliable platform for communication around the world. Operational data is an important foundation for monitoring developing trends and making rational decisions to address security issues related to routing. It is also important to measure the effect of routing security tools and technologies once they are deployed. Because the inter-domain routing system is global, such monitoring and measurements should be long-term and be done on a global scale.

However, currently, there is no coordinated approach across network operators to collect or analyze this kind of data, leaving network operators with only incomplete or anecdotal evidence to understand Internet-wide routing security issues.

To address this gap, the Internet Society is inviting network operators to participate in an effort to improve the collection of incident data related to routing resiliency. The effort, undertaken in partnership with the Border Gateway Protocol (BGP) monitoring service BGPmon (<http://www.bgpmon.net>), also aims to provide a statistically representative picture of these incidents and their impacts, and to provide a basis for risk assessment and global trend analysis. In this context, one important dataset is operational statistics of incidents related to routing security, as registered by a network operator. This survey is aimed at collecting these operational data.

The Survey

User login

Username *

Password *

- [Request new password](#)

Собираемые данные

Информация о сети

- Одноразово, во время регистрации
- Тип сети, связность, использование практик и инструментария для обеспечения безопасности и устранения последствий инцидентов.

Информация о происшествиях, автоматически регистрируемых внешними мониторами

- При первом входе в систему – исторический обзор за последние 6-12 месяцев
- После этого обзор инцидентов обновляется еженедельно
- Мы просим участников классифицировать зарегистрированные события
 - Эффект: severe, moderate, insignificant, not an incident
 - Детектирование: monitoring system, customer call, this alert

Анализ рисков на основе фактических данных

Filter by

Type

Priority
 Critical Warning Notice Info

Include previously classified

Show only Active alerts

Filter

Legend

- Critical
- Warning
- Notice
- Info

ID	Alert Type	Your AS	Your Prefix	Detected Prefix	Origin AS	ASPath	Time (UTC)	Seen By #Probes	Duration	Status	Classify
794	More Specific Announcement by Customer	64500	208.67.220.0/24	208.67.220.0/25	666	1103 271 666	2013-09-19 15:47:35	666	0	active	
734	More Specific Announcement by Customer	64500	128.189.0.0/16	128.189.128.0/18	393249	28247 262781 28329 12989 271 271 271 393249	2013-06-10 14:15:40	8	22:44:20	active	
735	More Specific Announcement by Customer	64500	128.189.0.0/17	128.189.96.0/19	393249	34695 11670 13768 271 393249	2013-06-10 14:15:40	7	22:44:20	active	
736	More Specific Announcement by Customer	64500	207.23.0.0/16	207.23.160.0/19	11105	558 22822 271 11105	2013-04-18 18:58:04	8	22:01:56	active	
737	More Specific Announcement by Customer	64500	207.23.0.0/16	207.23.192.0/19	11105	40387 11537 6509 271 11105	2013-04-18 18:58:04	18	22:01:56	active	
738	More Specific Announcement by Other AS	64500	206.12.24.0/22	206.12.26.0/24	22950	553 680 20965 6509 26806 22950	2013-02-11 02:40:29	11	14:19:31	active	
739	More Specific	271	206.12.24.0/22	206.12.27.0/24	22950	3367 2603 6509 26806	2013-02-11	11	14:19:31	active	

Анализ рисков на основе фактических данных

Filter by

Type

Priority
 Critical Warning Notice Info

Include previously classified

Show only Active alerts

Filter

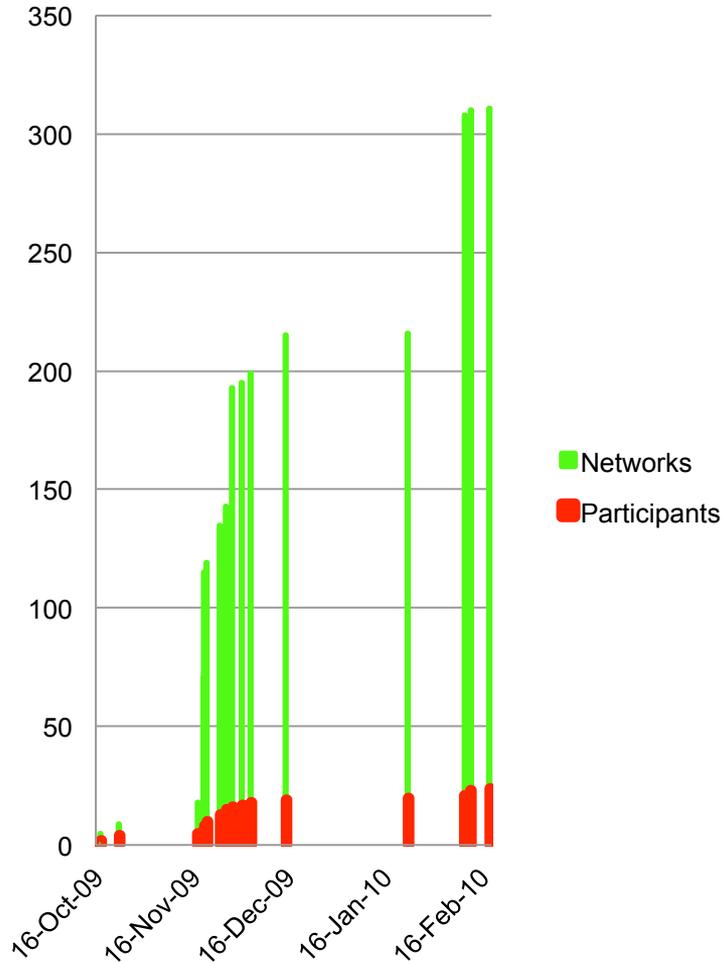
Legend

Critical	Red background
Warning	Yellow background
Notice	Grey background
Info	White background

ID	Alert Type	Your AS	Your Prefix	Detected Prefix	Origin AS	ASPath	Time (UTC)	Seen By #Probes	Duration	Status	Classify
794	More Specific Announcement by Customer	64500	208.67.220.0/24	208.67.220.0/25	666	1103 271 666	2013-09-19 15:47:35	666	0	active	✔
734	More Specific Announcement by Customer	64500	128.189.0.0/16	128.189.128.0/18	393249	28247 262781 28329 2989 271 271 393249	2013-06-10 14:15:40	8	22:44:20	active	➡
735	More Specific Announcement by Customer	64500	128.189.0.0/16	128.189.0.0/17	393249	14695 11070 1376 28329 393249	2013-06-10 14:15:40	8	22:44:20	active	➡
736	More Specific Announcement by Customer	64500	207.23.0.0/16	207.23.160.0/19	11105	558 22822 271 11105	2013-04-18 18:58:04	8	22:01:56	active	➡
737	More Specific Announcement by Customer	64500	207.23.0.0/16	207.23.192.0/19	11105	40387 11537 6509 271 11105	2013-04-18 18:58:04	18	22:01:56	active	➡
738	More Specific Announcement by Other AS	64500	206.12.24.0/22	206.12.26.0/24	22950	553 680 20965 6509 26806 22950	2013-02-11 02:40:29	11	14:19:31	active	✔
739	More Specific Announcement by Other AS	64500	206.12.24.0/22	206.12.27.0/24	22950	3367 2603 6509 26806 22950	2013-02-11 02:40:29	11	14:19:31	active	✔

Check and Classify

Статистика: Участие



>4 months

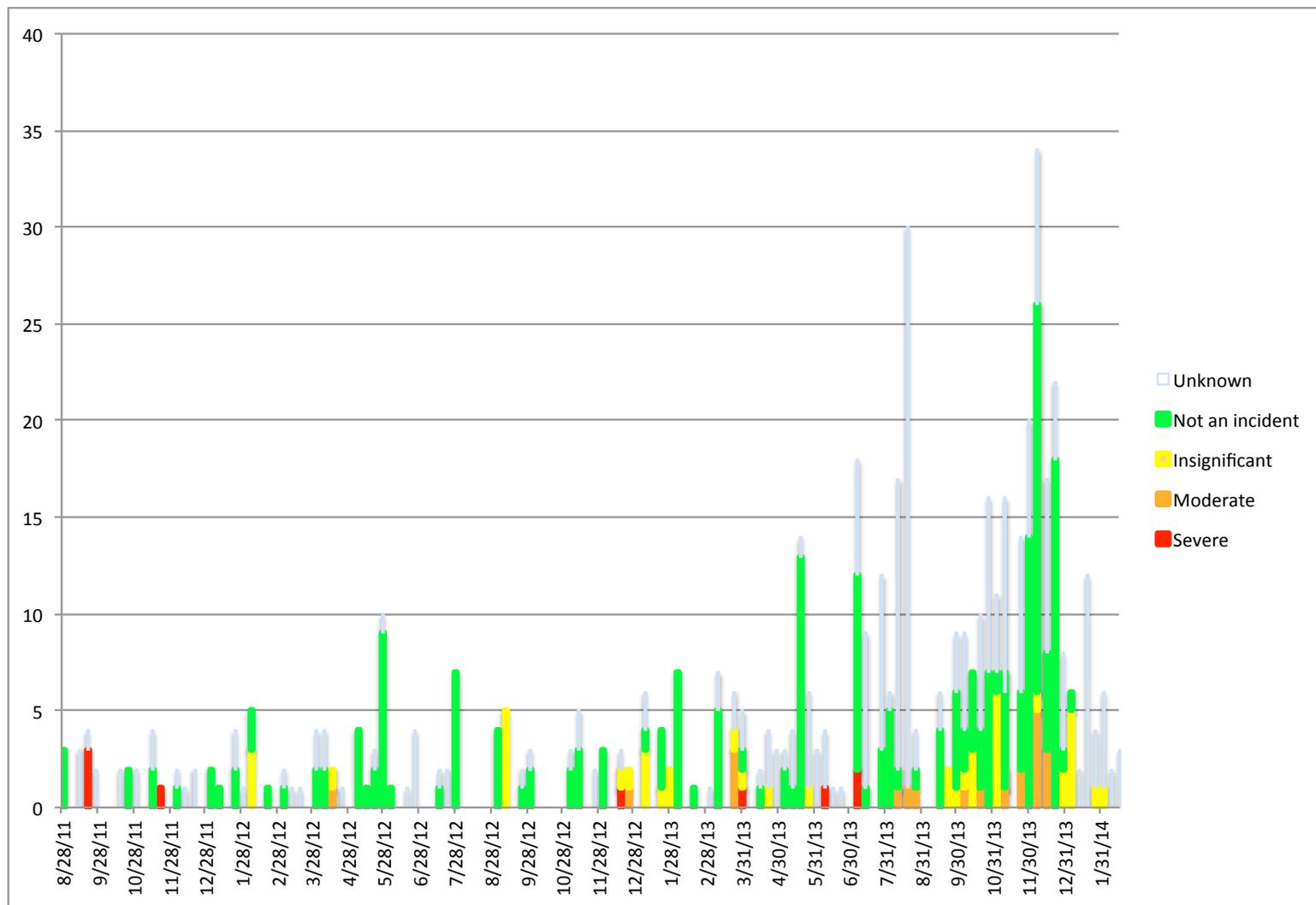
25 participants

311 networks

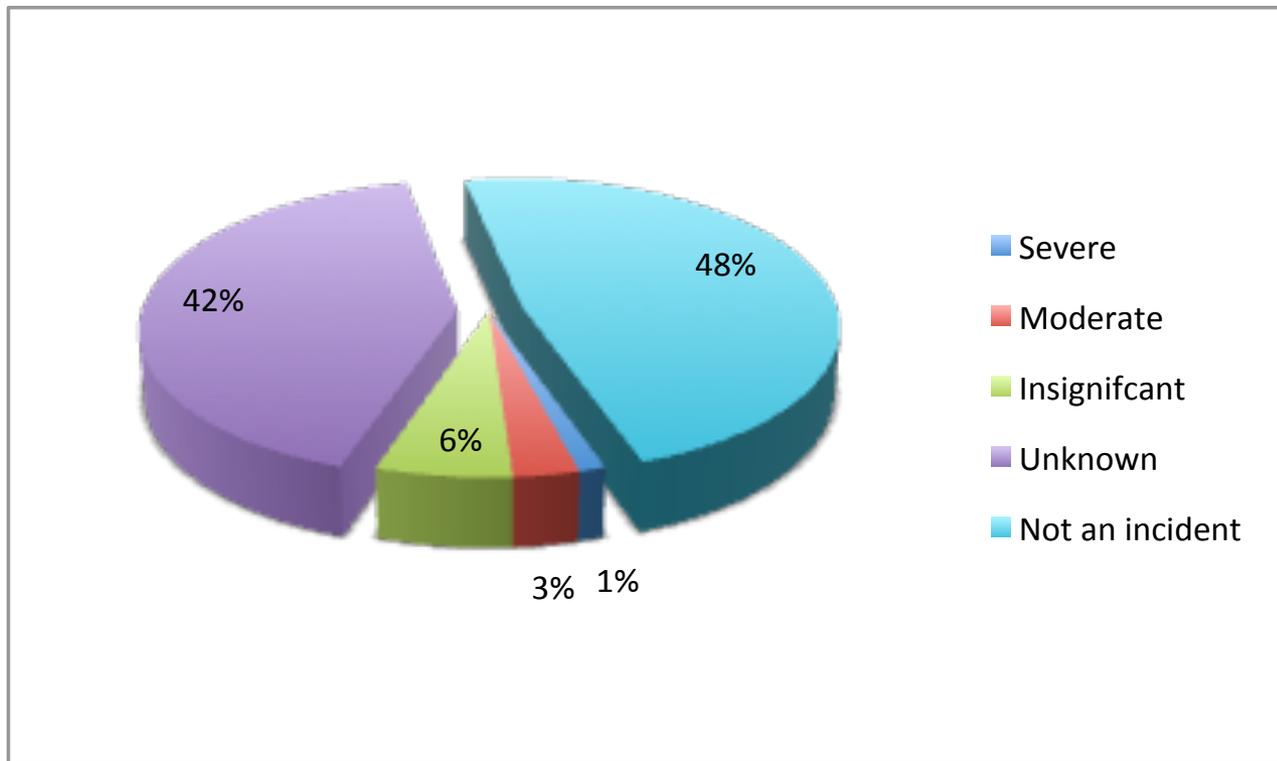
442 events registered

264 events classified

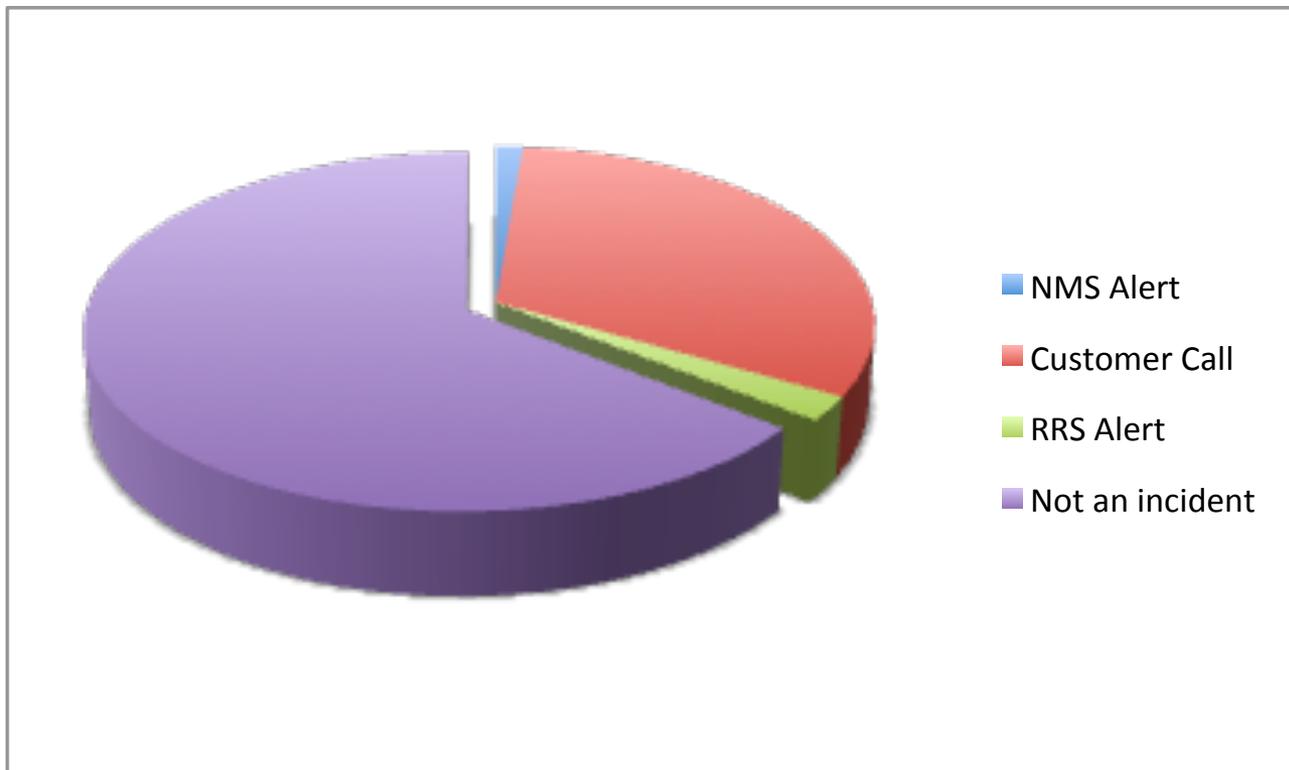
Эффект происшествий на услуги сети



Эффект происшествий (II)



Откуда вы узнали о происшествии?



Хотите поучаствовать?

Проект заканчивается 1 июля, но...

Пожалуйста отправьте заявку по адресу rrs-admin@isoc.org.

В заявке укажите:

- номер вашей автономной системы (AS number) и
- почтовый адрес для получения уведомлений

Вы также можете указать номера автономных систем ваших клиентов для которых вы готовы классифицировать события, относящиеся к их сетям.

Коллективная ответственность и сотрудничество для повышения надежности и безопасности глобальной системы маршрутизации

Цели

- **Представить подход к решению сложных проблем, основанный на принципах и рекомендациях с широкой поддержкой сетевого сообщества**
- **Привлечь внимание к проблеме и побудить к конкретным действиям, которые поддерживаются растущей группой сетевых операторов.**
- **Показать, что отрасль способна взять решение проблемы в свои руки**

«Манифест надежной маршрутизации»

Routing Resilience Manifesto

- Общие принципы

- Взаимозависимость и взаимные действия
- Приверженность передовым практикам
- Привлечение клиентов и пиоров

- Рекомендации, сфокусированные на наиболее насущных проблемах

- Фильтрация BGP
- Анти-спуфинг
- Координация и сотрудничество

Конечный продукт

Вэб-ресурс

Опубликованный документ

**Растущий список операторов, поддерживающих
Манифест**

**Ссылки на практические рекомендации, например
ВСОР, ВСР**

Первая фаза работы

Небольшая группа операторов, работающая над черновым вариантом

ISOC обеспечивает нейтральную платформу и координацию

Рекомендации – 3 четких призыва

- 1. Предотвратить распространение ложной маршрутизационной информации**
- 2. Предотвратить трафик с подложными адресами источника**
- 3. Стимулировать коммуникацию и сотрудничество между сетевыми операторами в глобальном масштабе**

Рекомендации – 3 четких призыва

Prevent propagation of incorrect routing information

Network operators are encouraged to define a clear routing policy and implement a system that ensures correctness of their own announcements and announcements from their customers to adjacent networks with a prefix and as-path granularity. Network operators should be able to communicate to their adjacent networks which announcements are correct.

Рекомендации – 3 четких призыва

Prevent propagation of incorrect routing information

Network operators are encouraged to define a clear routing policy and implement a system that ensures correctness of their own announcements and announcements from their customers to adjacent networks with a prefix and as-path granularity. Network operators should be able to communicate to their adjacent networks which announcements are correct.

Рекомендации – 3 четких призыва

Prevent traffic with spoofed source IP address

Network operators should implement a system that enables source address validation for at least single-homed stub customer networks, their own end-users and infrastructure. Network operators are encouraged to implement filtering to prevent packets with incorrect source IP address from entering and leaving the network.

Рекомендации – 3 четких призыва

Prevent traffic with spoofed source IP address

Network operators should implement a system that enables source address validation for at least single-homed stub customer networks, their own end-users and infrastructure. Network operators are encouraged to implement filtering to prevent packets with incorrect source IP address from entering and leaving the network.

Рекомендации – 3 четких призыва

Facilitate global operational communication and coordination between the network operators

Network operators should maintain globally accessible up-to-date contact information.

Рекомендации – 3 четких призыва

Facilitate global operational communication and coordination between the network operators

Network operators should maintain globally accessible up-to-date contact information.

Следующие шаги

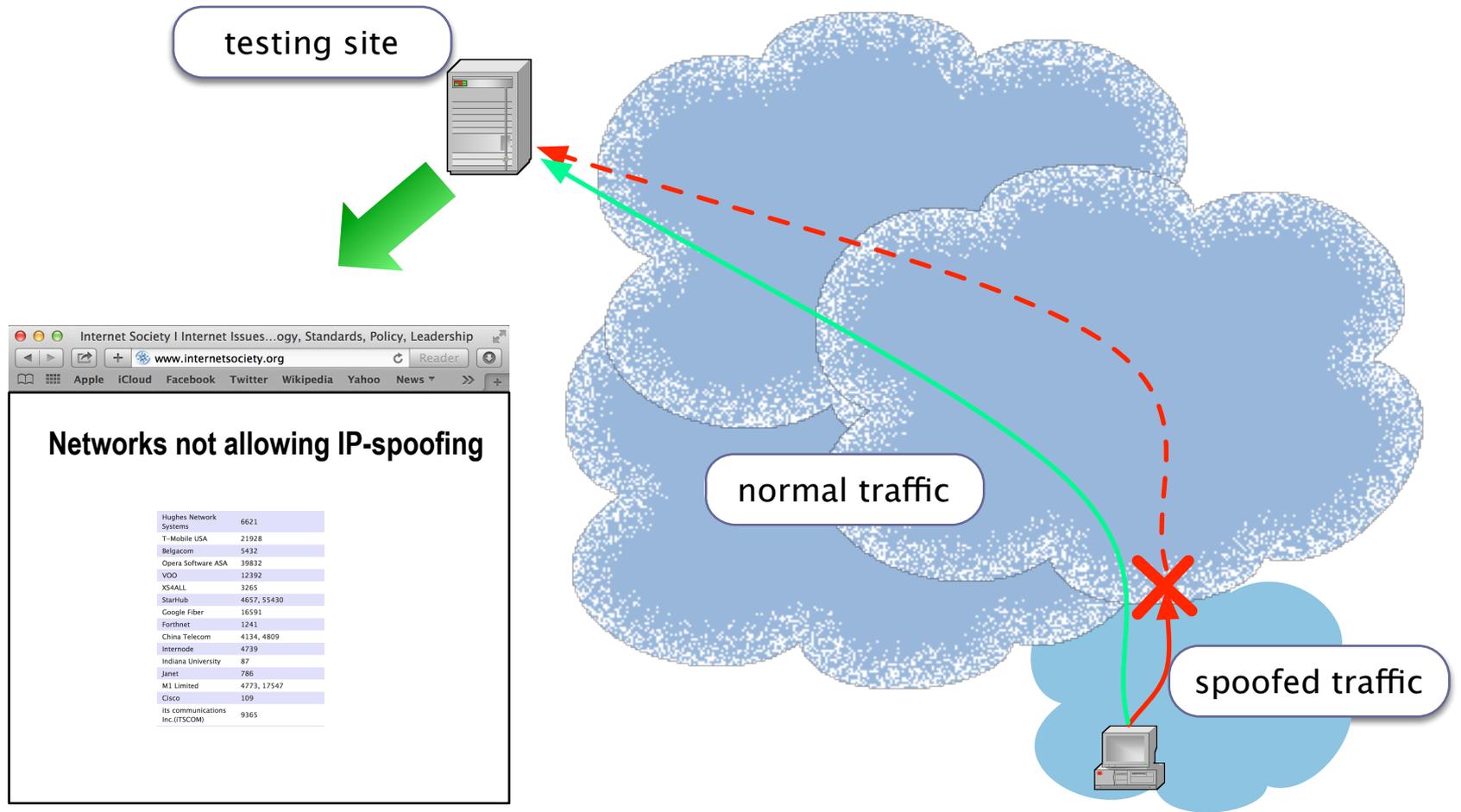
Закончить черновую работу

Более детально обсудить с широким кругом сетевых операторов – если вас заинтересовала эта инициатива – напишите мне или в resilience@isoc.org

Создать вэб-ресурс и изначальную «группу поддержки»

Начать активно продвигать Манифест в глобальном масштабе (списки рассылки, NOG, операторы)

«Движение» анти-спуфинга



Цели

• Привлечь внимание к проблемам и побудить к конкретным действиям, поддерживаемым растущей группой сетевых операторов.

• Показать, что отрасль способна взять решение проблем в свои руки

• Четкий конкретный призыв:

“Мы делаем как минимум это и призываем вас последовать нашему примеру”

The Internet is open, interconnected and interdependent
It's an ecosystem based on collaboration and shared responsibility

ACCESSIBLE | PERMISSION-FREE INNOVATION | GLOBAL REACH



Each network is responsible not only for its own security, but also contributes to the overall security of the medium. The challenge is to create a culture of collective responsibility to make the Internet more secure and resilient.

EXPONENTIAL GROWTH

The Internet has almost **1 billion** hosts
> 500% growth in last years



In 2014, **100 new devices** will connect to the Internet each second. This number is expected to reach **250 devices** per second by 2020.

ATTACKS ON THE RISE

The very same properties of the Internet that underpin its success open up new opportunities for various types of malicious activity.

Accessible → open for attacks and intrusion
Permission-free innovation → Innovative malware
Global reach → Issues are transborder and spread globally

300Gbps is the largest attack recorded to date.
↳ Largest DDoS and spam campaign ever/first in 2013.

55% increase in average attack sizes in 20 months.

265% increase in reflection attacks from Q3 '12 to Q3 '13

28 million DNS requests pose some level of security risk

60 to 70 times Potential for amplification attacks

350% growth In large >200Gbps DDoS attacks from 2012 to 2013

DDoS An acronym for distributed denial of service attack, the most popular is a reflection-based amplification attack. It leverages unprotected servers on the Internet to launch an attack.

INWARD AND OUTWARD RISKS

Risks are not only inward. Compromised networks can be used to launch attacks against other networks and across the Internet.

Common Inward Risks Security perimeter breaches, malware, spam and phishing are examples of inward risks that, if not managed correctly, can compromise a network.

Man in the Middle Attacks Open DNS, SIP and VoIP servers can be used as unifying offices for target attacks.

Reflection and Amplification Attacks Open DNS, SIP and VoIP servers can be used as unifying offices for target attacks.

Routing Hygiene Networks that handle routing arrangements centrally can be used for hijacking or spoofing other resources' traffic. Networks without anti-spoofing measures can be used as a launchpad for attacks.

TECHNOLOGY BUILDING BLOCKS

Key measures that administrators can employ to make their networks and the whole Internet more secure and resilient.

IPsec • Internet Protocol Security

TLB • Transport Layer Security

Kerberos • Network Authentication System

DNSSEC • Domain Name System Security Extensions

DANE • DNS-based Authentication of Named Entities

RPKI • Resource Public Key Infrastructure

TAKE ACTION

The evaluate your network risk profile and assessment. Support actions focusing on global security and resilience.

• Detect, close or protect open resolvers and other potential amplifiers

• Deploy best practices aimed at improving routing hygiene

• Deploy anti-spoofing measures, preventing traffic with spoofed source IP addresses

• Deploy DNSSEC (optional) to secure name resolution for your customers

• Detect and mitigate reflected and compromised devices on your network

• Cooperate with other networks in detection, tracing back and mitigation of attacks

Internet Society

Learn more at
www.internetsociety.org/security

© 2014 Internet Society. All rights reserved. This document is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. For more information, see <http://creativecommons.org/licenses/by-nc-sa/4.0/>.

Заинтересовались?

Напишите нам:

resilience@isoc.org