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?

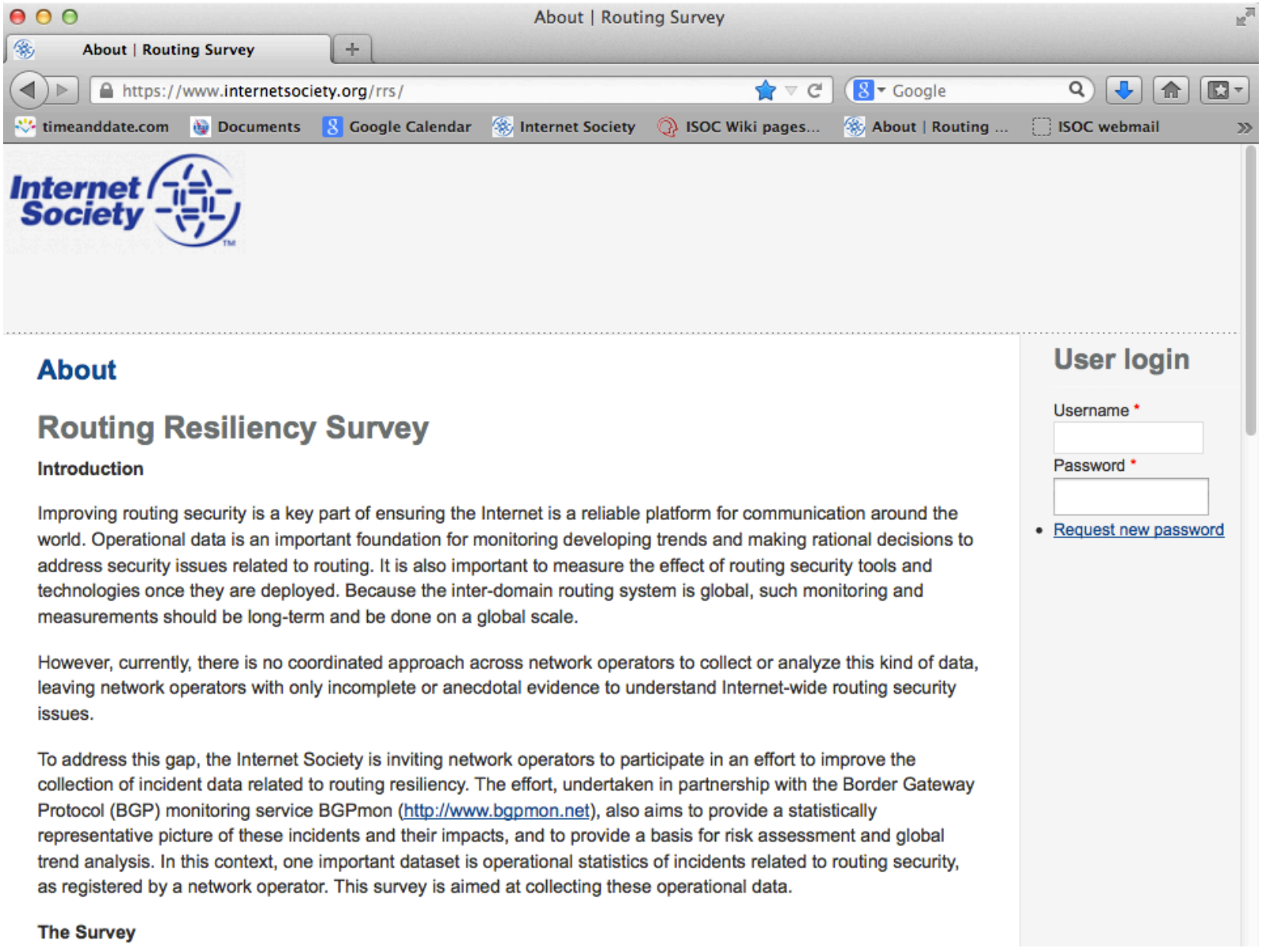
- Данные недоступны, либо отсутствуют, либо не разглашаются
- Оценка рисков основана на догадках

Затрагивает ли это вашу сеть?

- Детектирование инцидентов
- Исключение ложных сигналов
- Оценка эффекта

Адекватно ли защищена ваша сеть?

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



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

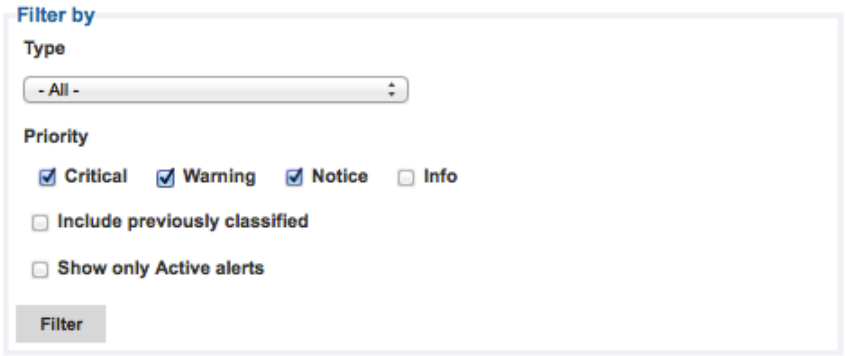
– При первом входе в систему – исторический обзор за последние 6-12 месяцев

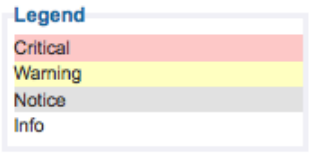
– После этого обзор инцидентов обновляется еженедельно

– Мы просим участников классифицировать зарегистрированные события

- Эффект: severe, moderate, insignificant, not an incident
- Детектирование: monitoring system, customer call, this alert

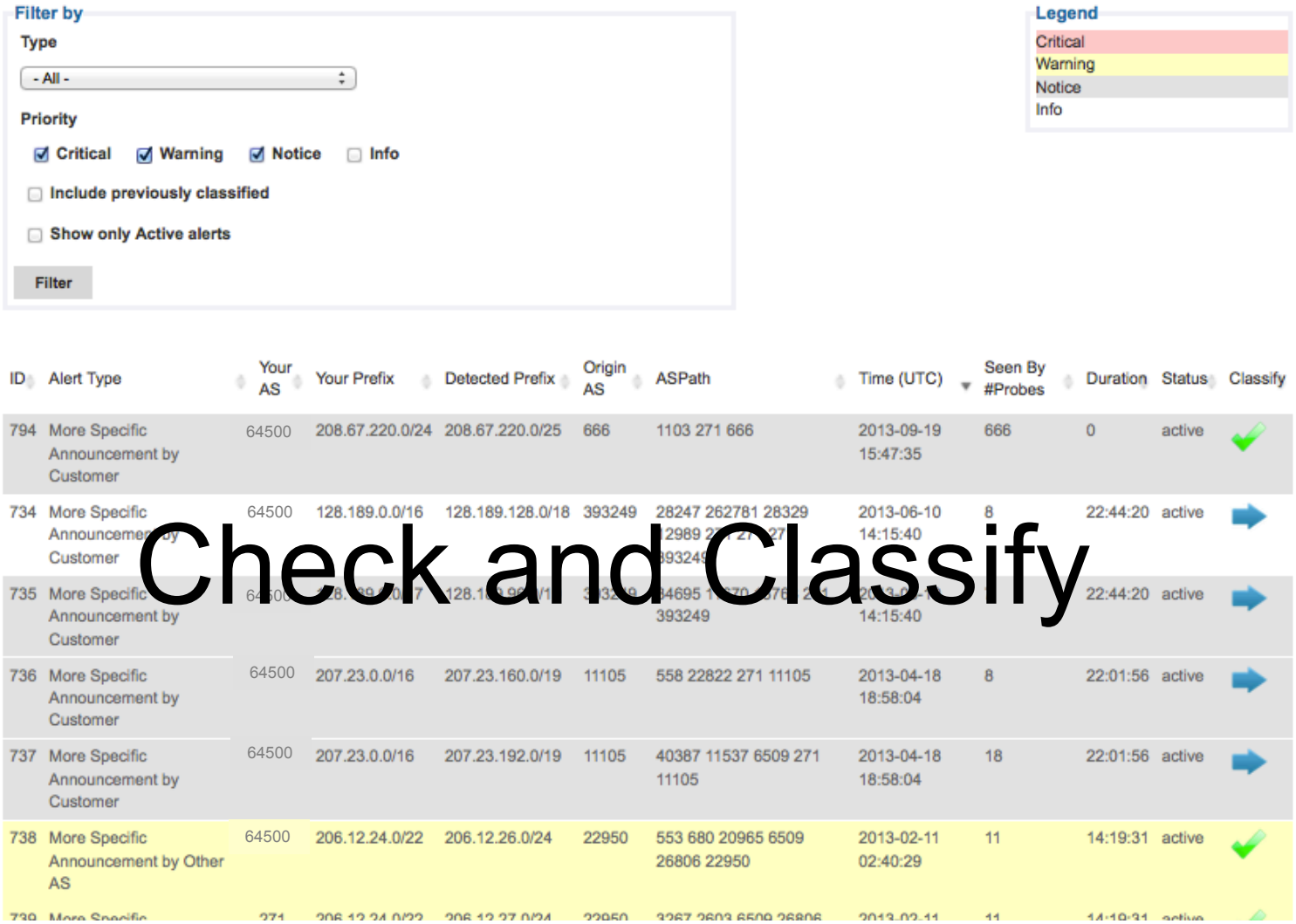
Анализ рисков на основе фактических данных





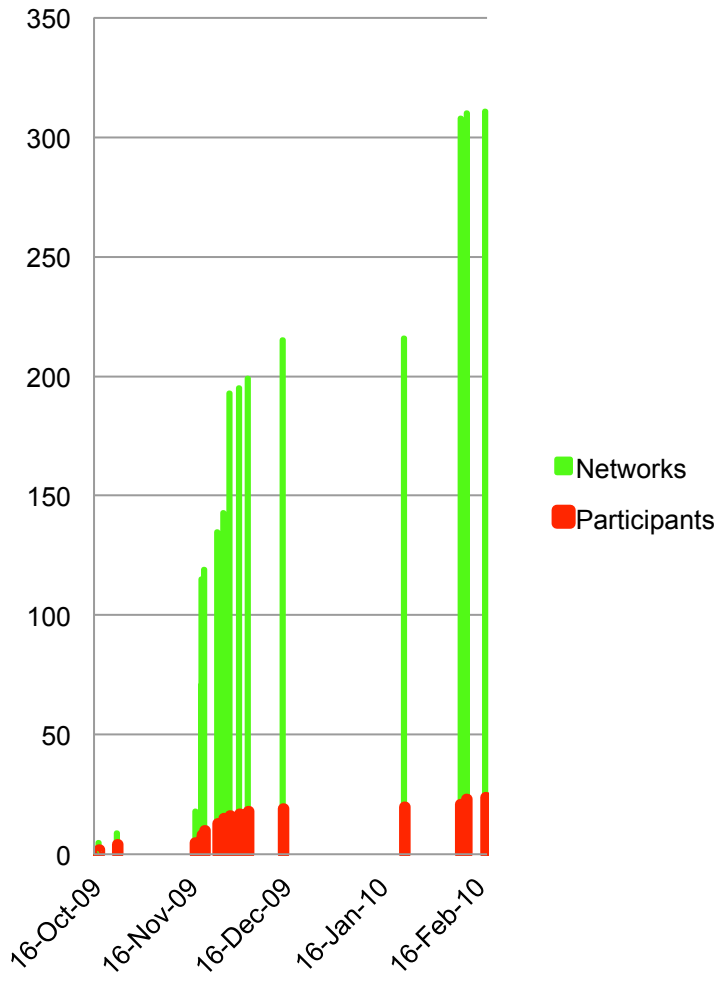
ID	Alert Type	Your AS	Your Prefix	Detected Prefix	Origin AS	ASPath	Time (UTC)	Seen By #Probes	Duration	Status	Classify
794	More Specific Announcement by Customer	64500	208.67.220.0/24	208.67.220.0/25	666	1103 271 666	2013-09-19 15:47:35	666	0	active	
734	More Specific Announcement by Customer	64500	128.189.0.0/16	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	3267 2603 6509 26806	2013-02-11	11	14:19:31	active	

Анализ рисков на основе фактических данных



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	2013-06-10 14:15:40	8	22:44:20	active	
735	More Specific Announcement by Customer	64500				393249	2013-06-10 14:15:40		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	3267 2603 6509 26806	2013-02-11	11	14:19:31	active	

Статистика: Участие



>4 months

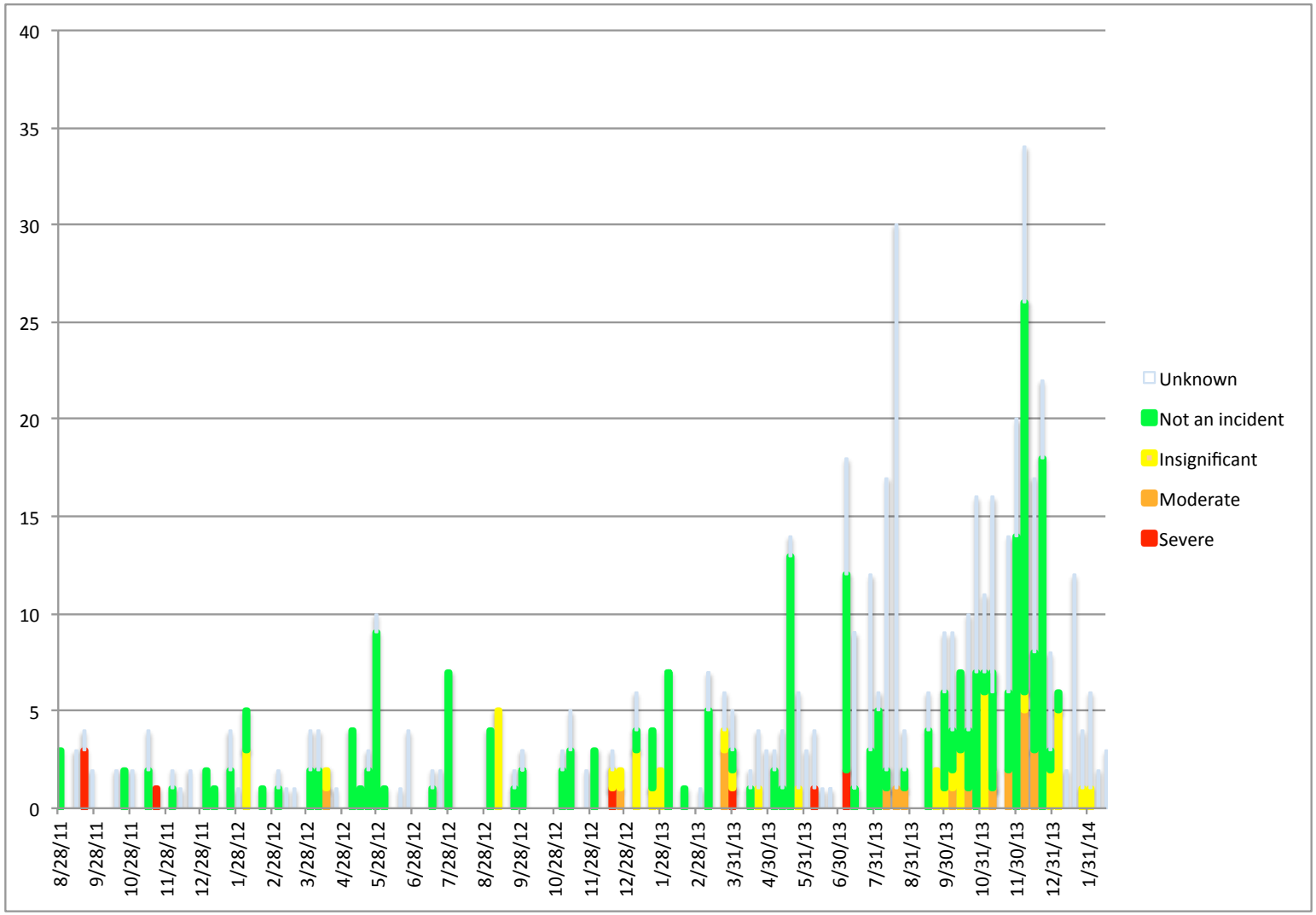
25 participants

311 networks

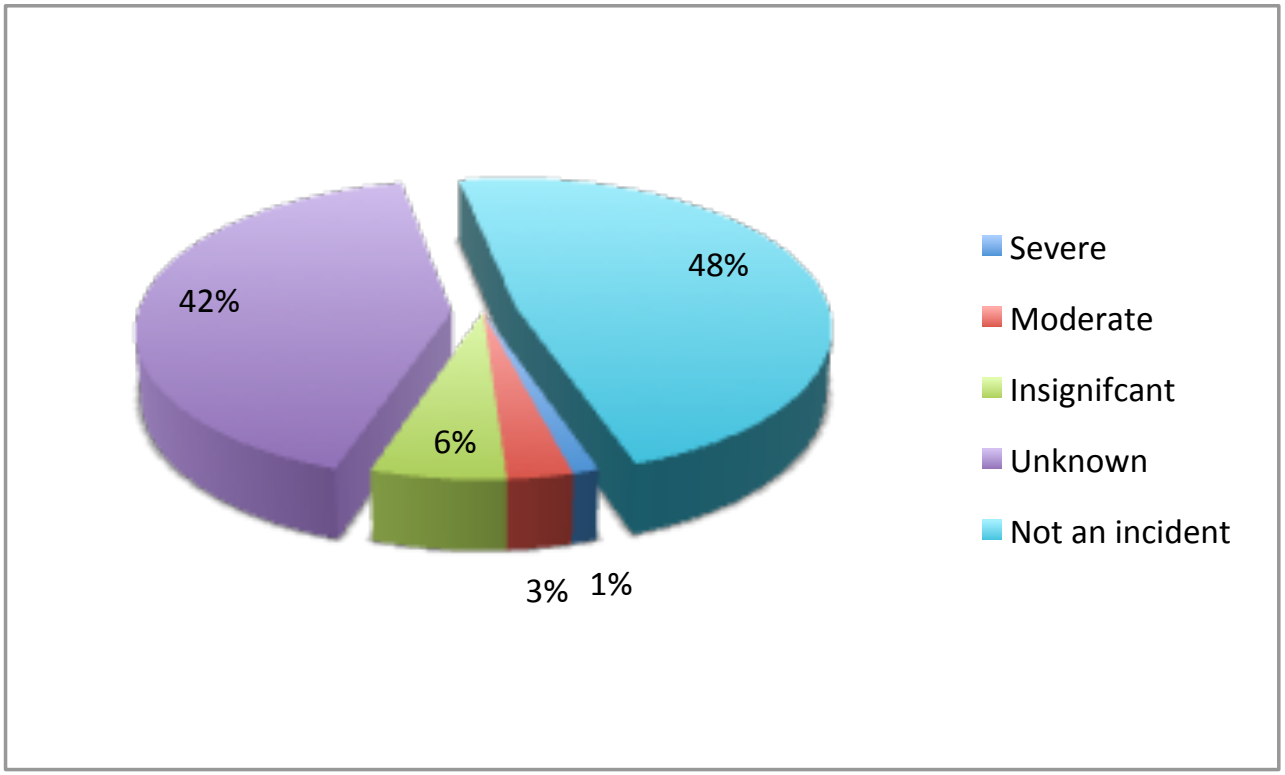
442 events registered

264 events classified

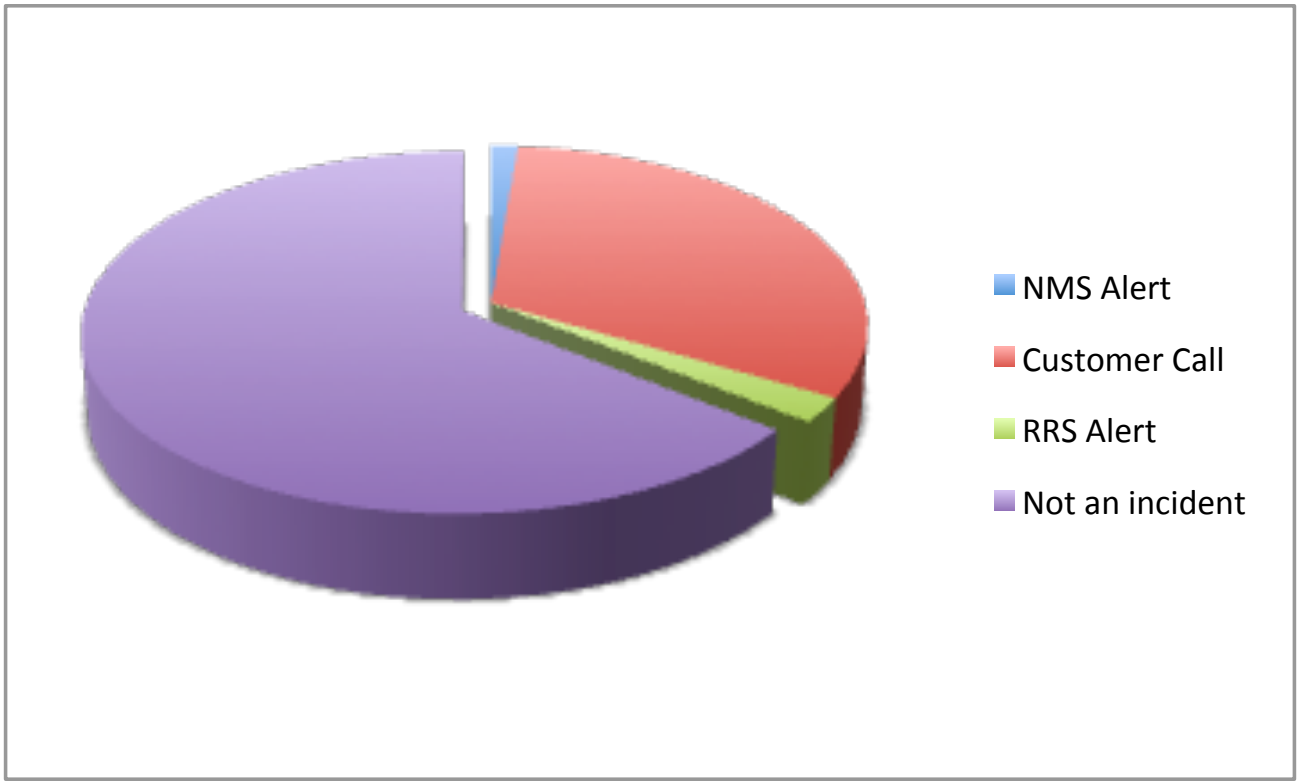
Эффект происшествий на услуги сети



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 пиров**
- **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 BCOP, BCP

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

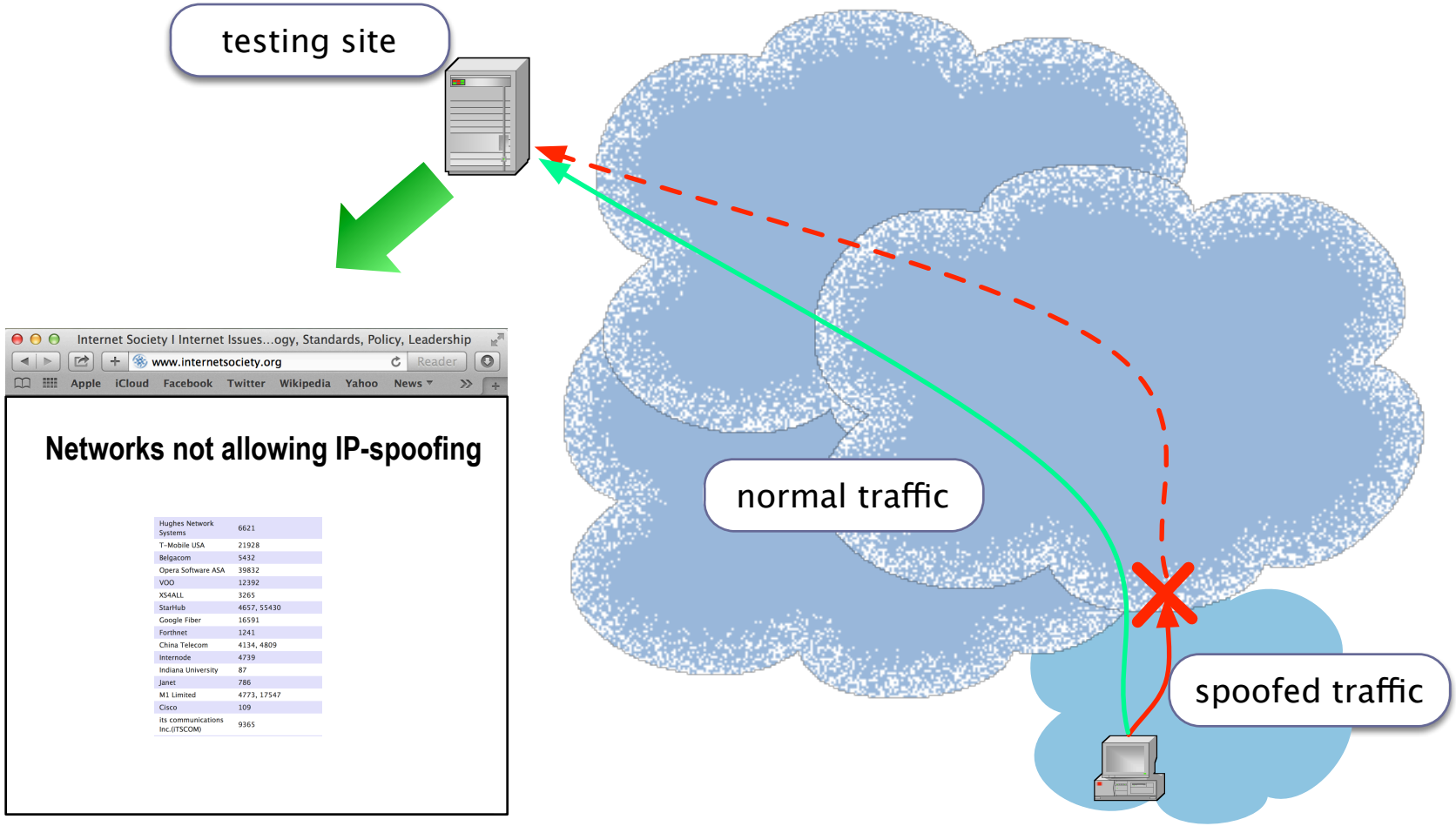
Закончить черновую работу

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



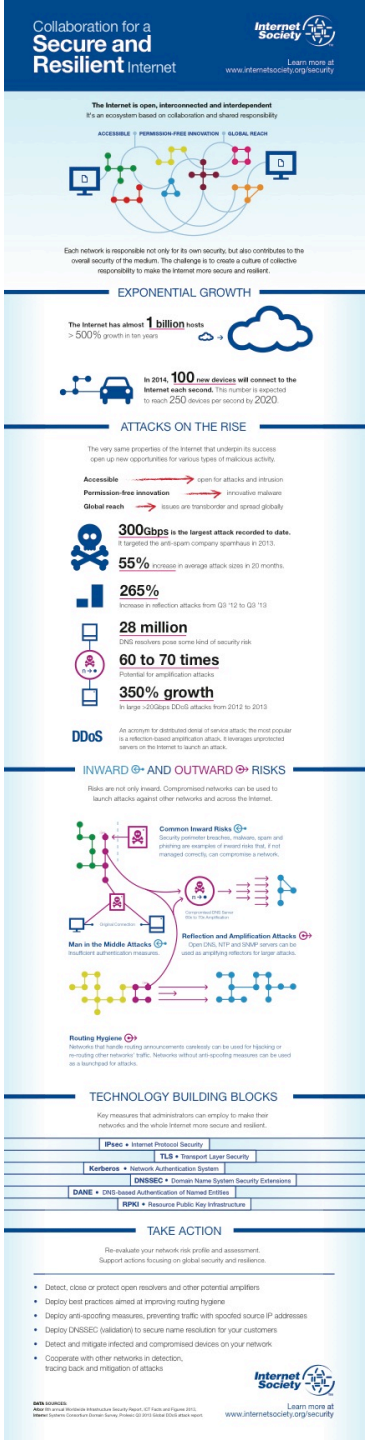
Цели

- **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”



Заинтересовались?

Напишите нам:

resilience@isoc.org