Practical DNSSEC

Мастерская – 2013

Sergey Myasoedov
5.12.2013

Расписание

- Введение
- Принципы работы с ключами
- Практика: генерация ключей
- Практика: подписывание зоны
- Практика: публикация зоны
- Периодические задачи
- Другой софт
- Заключение

netart group

DNSSEC

- Придуман инженерами для инженеров
- Единственная надёжная технология защиты DNS
- Неплохо масштабируется
- Поддерживается большими игроками
- Поддерживается основными DNS-серверами

Реализация в крупных TLD

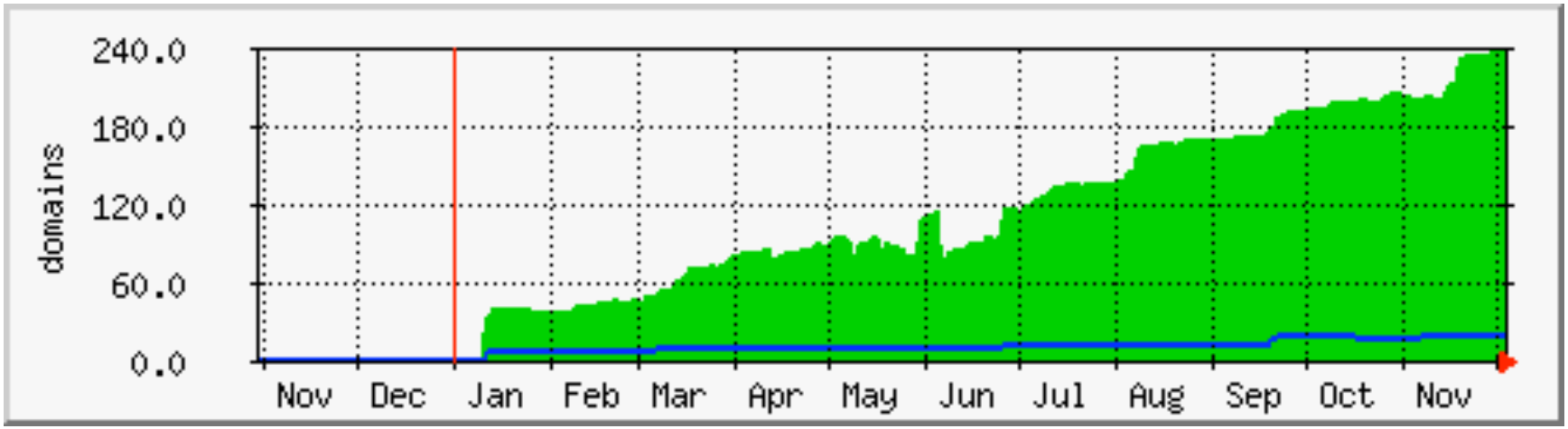
Все крупные gTLD (.com, .net, .org etc) – поддерживают!

Многие крупные ccTLD (.de, .uk, .se, .ru) – поддерживают!

Подписаны, но и только: .by, .ua

Регистраторы в .ru/.рф/.ua – увы ☹. Крайне мало. Возможно, я ошибаюсь?

Статистика .RU / .РФ 4.12.2013



.ru – 237 доменов

.рф – 17 доменов

Статистика .UA

Всего 7 делегированных доменов с DS.

Динамику мы отслеживаем.
За 12 месяцев - динамика отсутствует.

Домены:

chernovtsy.ua, cv.ua, netassist.ua, nic.ua, rovno.ua, rv.ua, ua.ua

Для сравнения – .COM / .NET

Подписано:

- 319 тыс. доменов из ~113 млн доменов в .COM
- 66 тыс. доменов из ~15 млн доменов в .NET

Скорость подписания – 3-4 тысячи доменов в неделю

Техника

- Документируем свои намерения, выбираем параметры криптографии и DNSSEC
- Генерируем ключи
- Помещаем ключи в свою зону
- Подписываем зону
- Публикуем DS через регистратора

Ключи

- RFC 6781 рекомендует использовать два ключа: KSK и ZSK (sec. 3.1)
- Размер ключа в зависимости от криптоалгоритма – от 1 до 4096 бит
- Крайне рекомендуется содержать закрытые части ключей отдельно или даже в HSM. Но это затрудняет последующие манипуляции с ними.

netart group

Поехали!

Bind 9.9 и тестовая зона enog.ru

Заходим по ssh/IPv4/IPv6:

username **enog**

password **uadom**

server **dns.enog.ru**

.. и создаём свой рабочий каталог

mkdir mynickname; cd mynickname

.. копируем тестовую зону

cp /enog.ru .

Процесс

- Только ключи, никаких сертификатов
- Bind 9.8/9.9 требует явного указания NSEC3 при генерации ключей
- Один ключ генерируем с параметром -f KSK
- Второй ключ – без этого параметра, и получится ZSK
- В итоге – 4 файла ключей, 2 из них готовы к включению в зону и уже имеют правильный origin

netart group

На очереди – зона

- После запуска dnssec-signzone получим подписанную зону и файл с DS для публикации
- Если хотим NSEC3 – указываем -3 и задаём SALT для хэш-функции
- На выходе имеем подписанную зону, которая как минимум в 4 раза больше неподписанной зоны с ключами, и в 25 раз больше оригинальной зоны.

netart group

Сравним?

- Оригинальная зона
- Оригинальная зона с ключами
- Подписанная зона с NSEC
- Подписанная зона с NSEC3
- Наконец – DS-SET для передачи в родительскую зону

Вариации

- Дополнительные флаги для Key Rollover: Revoked key
- NSEC3 не используется напрямую для криптографии DNSSEC – лишь для сокрытия указателя на следующую запись (Next SECure) для исключения перебора (walkthrough) зоны
- Для зон, похожих на нашу ENOG.RU, употребление NSEC3, пожалуй, избыточно

Минималистский вариант

- Один ключ для подписи, KSK==ZSK
- Максимальный период валидности подписи – год, два, десять
- Одна DS-запись в TLD
- NSEC вместо NSEC3
- И ведь всё работает!
- Важно, чтобы хотя бы по одной цепочке DS-KSK-ZSK прошла успешная валидация, а сколько этих цепочек – не так уж и важно

Оптимум?

- Настройки by default у bind (валидность подписей +30 дней с момента подписи)
- Другие разумные defaults у разных SW package
- Всё указанное хорошо работает у одного домена и неплохо масштабируется до десятков доменов
- Если нужно больше доменов – готового легко доступного решения нет
- Работа с зоной у ccTLD – вне нашего интереса

netart group

Немного в сторону

Chicken & egg problem:

- Валидация подписей основывается на моменте времени
- Может случиться, что после запуска системы время в CMOS не будет соответствовать реальности (например, 01:00 01 Jan 2010)
- Резолвинг даже NS, обслуживающих корневую зону, будет неуспешным
- До NTP-сервера таким образом достучаться не получится
- Выхода нет. Можно прописать IP-адрес NTP-сервера явным образом

Публикация DS

Только два примера.

NIC.RU

GODADDY.COM

Буду рад показать и других регистраторов здесь.

Автоматизация

- Переподписание зоны перед моментом истечения валидности подписи RRSIG – критично и необходимо.
- Для хостеров – [пере] подписание большого количества зон одним KSK/ZSK.

Хостерам

- Один KSK на много зон – удобно и эффективно
- Зоны придётся подписывать по одной сразу по окончании редактирования
- Все зоны придётся подписывать не позднее момента валидности RRSIG
- Придётся внедрять дополнительный мониторинг
- Не принесёт сразу никакого дохода
- Требуется наличие API у регистраторов для передачи DS в TLD
- Угрозы безопасности при использовании такой модели классические – компрометация ключа гораздо вероятнее успешной атаки на криптоалгоритмы

Софт для автоматизации

- Я видел all-in-one решения. Слишком громоздко для мини-хостинга
- Моё решение не претендует на красоту, но работает
- В нём даже нет named-checkzone (to do)
- Один KSK и один ZSK для всех зон

http://pastebin.com/KjBcvjiE

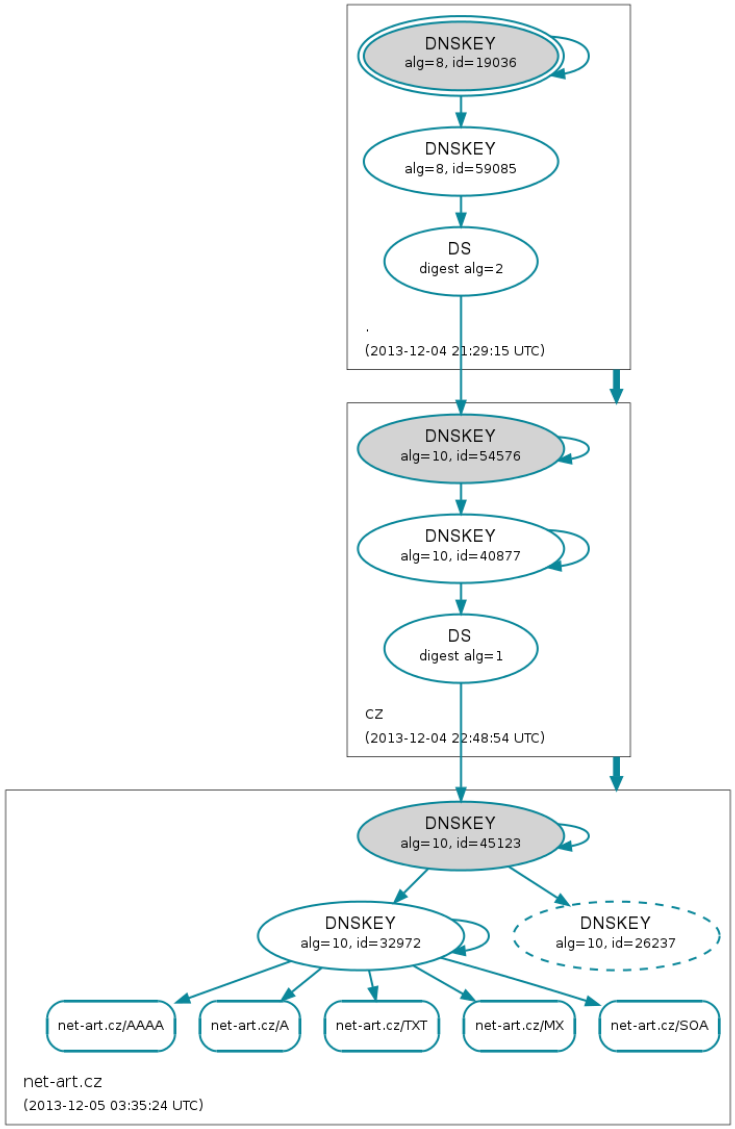
Валидация наших зон

Утилит довольно много, здесь только несколько производителей:

- NLnetLabs
- ISC
- CZ.NIC
- VERISIGN
- SurfNet

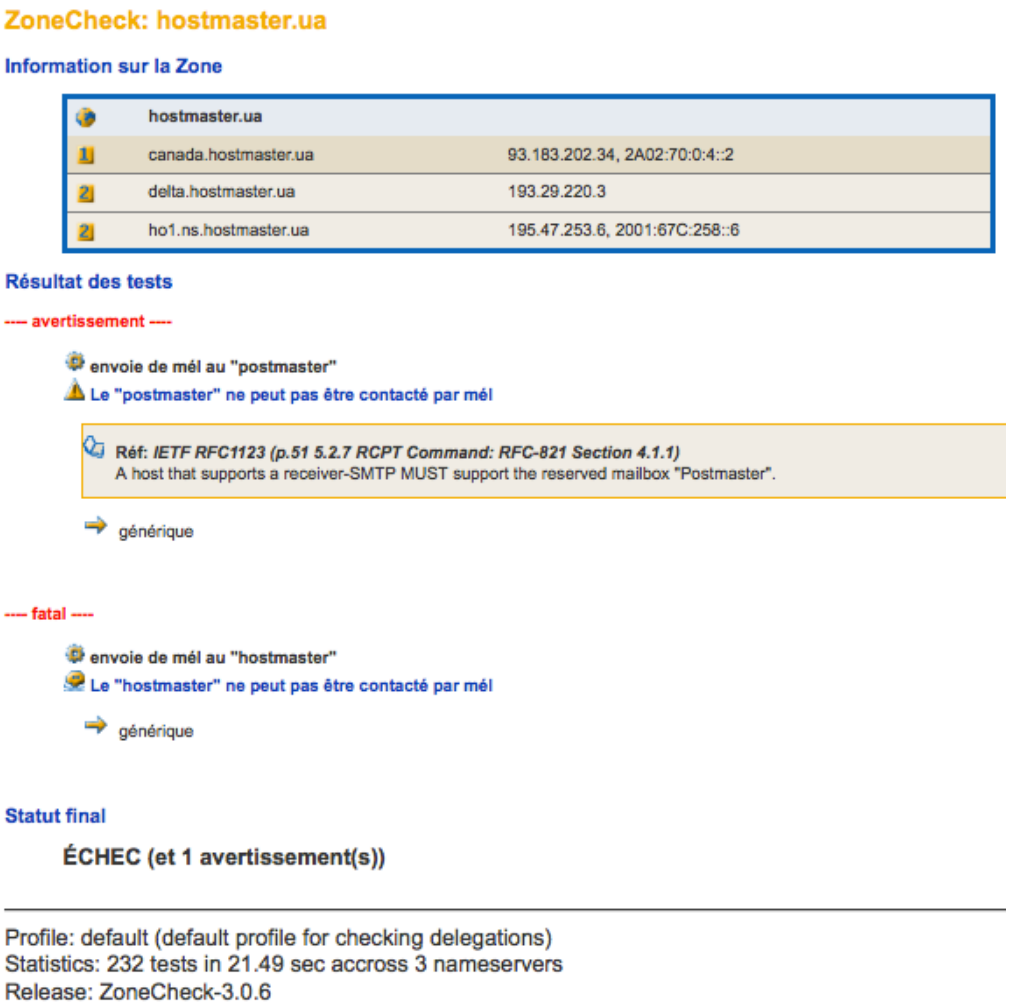
Визуальная диагностика

- DNSViz.net



Визуальная диагностика

- ZoneCheck (AFNIC)



ZoneCheck: hostmaster.ua

Information sur la Zone

	hostmaster.ua	
1	canada.hostmaster.ua	93.183.202.34, 2A02:70:0:4::2
2	delta.hostmaster.ua	193.29.220.3
2	ho1.ns.hostmaster.ua	195.47.253.6, 2001:67C:258::6

Résultat des tests

---- avertissement ----

envoie de mél au "postmaster"

Le "postmaster" ne peut pas être contacté par mél

Réf: *IETF RFC1123 (p.51 5.2.7 RCPT Command: RFC-821 Section 4.1.1)*
A host that supports a receiver-SMTP MUST support the reserved mailbox "Postmaster".

générique

---- fatal ----

envoie de mél au "hostmaster"

Le "hostmaster" ne peut pas être contacté par mél

générique

Statut final

ÉCHEC (et 1 avertissement(s))

Profile: default (default profile for checking delegations)
Statistics: 232 tests in 21.49 sec accross 3 nameservers
Release: ZoneCheck-3.0.6

Вопросы?

Предложения?

Оценки?

LinkedIn.com/in/myasoedov

netart group