BGP Spoofing in the Episode: Stealing Your (cc)TLD

Berislav Todorovic, KPN

What is this about?

- Nothing new - you heard it already (Pakistan Telecom, Pilosov-Kapela etc.):
  - http://www.youtube.com/watch?v=IzLPKuAOe50
  - http://blog.wired.com/27bstroke6/2008/08/revealed-the-in.html
- Yes, others can steal your BGP traffic easily.
  - Hint => the most specific route rule ...
- Consequences well understood by Network Operators, however ...
- ... often not taken seriously in the DNS operator community.
- Especially not in the ccTLD and gTLD world (think of .tv / .tk / .aero ...).
- And those you need for your services to operate correctly, so ...

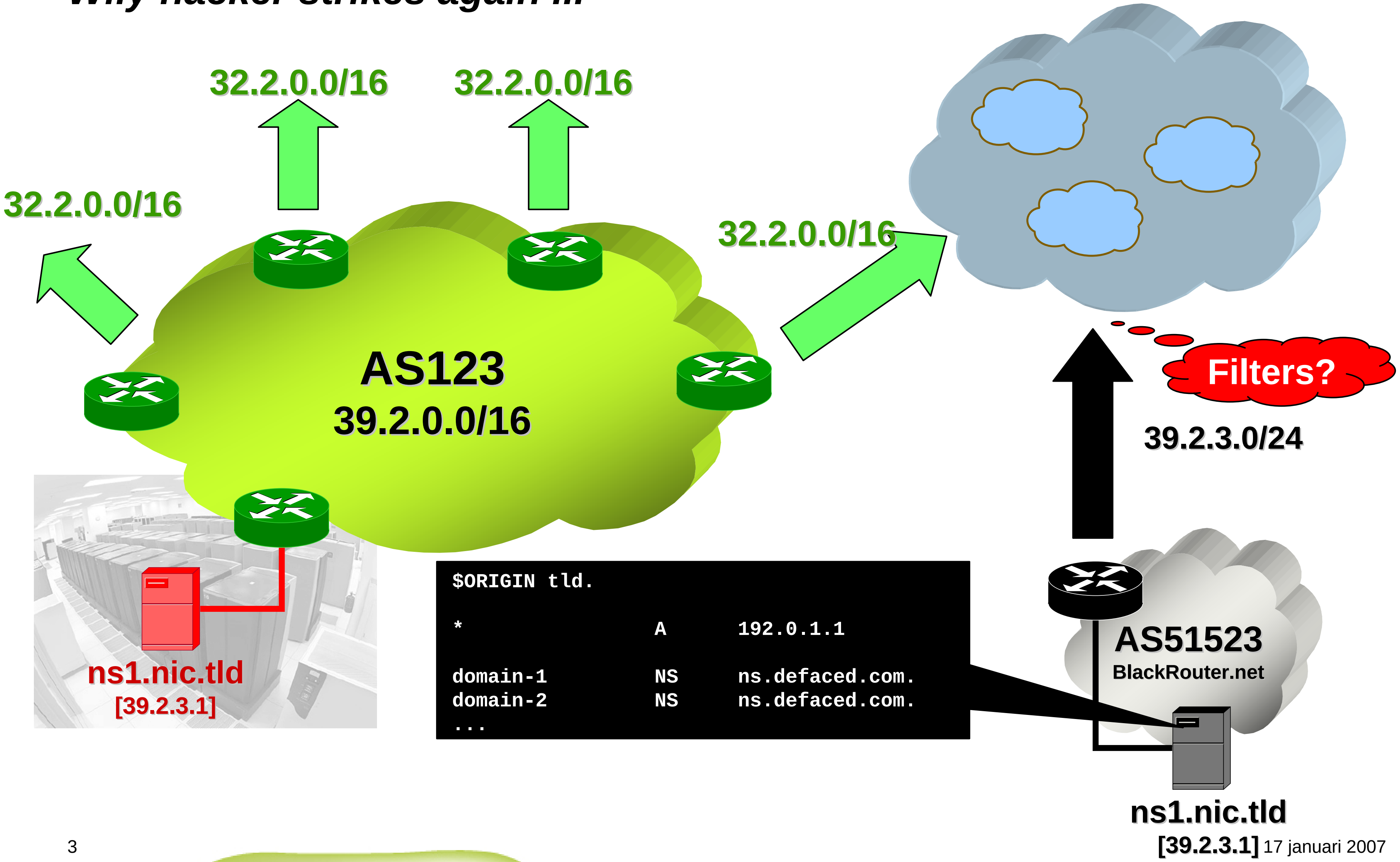
The world is not what it used to be …

- Ten years ago, BGP customers were considered trusted:
  - Not everyone had knowledge to run BGP.
  - Not everyone could afford a BGP speaking router.
  - Access line prices were higher.
- Today:
  - 10Mbps IP Transit incl. BGP costs $20 to $50.
  - Even kids know “**conf t**”.
  - Malicious parties are not only curious War Games kiddies anymore.

It’s a new world … do not trust anyone!

Possible Scenario - Stealing Your TLD

Wily hacker strikes again ...



```
$ORIGIN tld.

*                A      192.0.1.1

domain-1         NS     ns.defaced.com.
domain-2         NS     ns.defaced.com.
...
```

Route Filtering

- Manual requests ("Please, update your filters")
  - Good, but do you trust just <u>everything</u> from your customer?
  - *"We will soon start announcing 198.41.0.0/24 – please, update …"* ☺
- IRR:
  - Most providers rely on AS macros (**as-set** objects).
  - What would stop a malicious party to claim that AS-xxxx is their customer?
  - Anyone can add your ASN to their own AS macro and you won't be notified
  - Besides, adding garbage in RADB is easy.
- LOA:
  - Yes, on company letterhead.
  - Now, that's really great.
  - Security through obscurity.

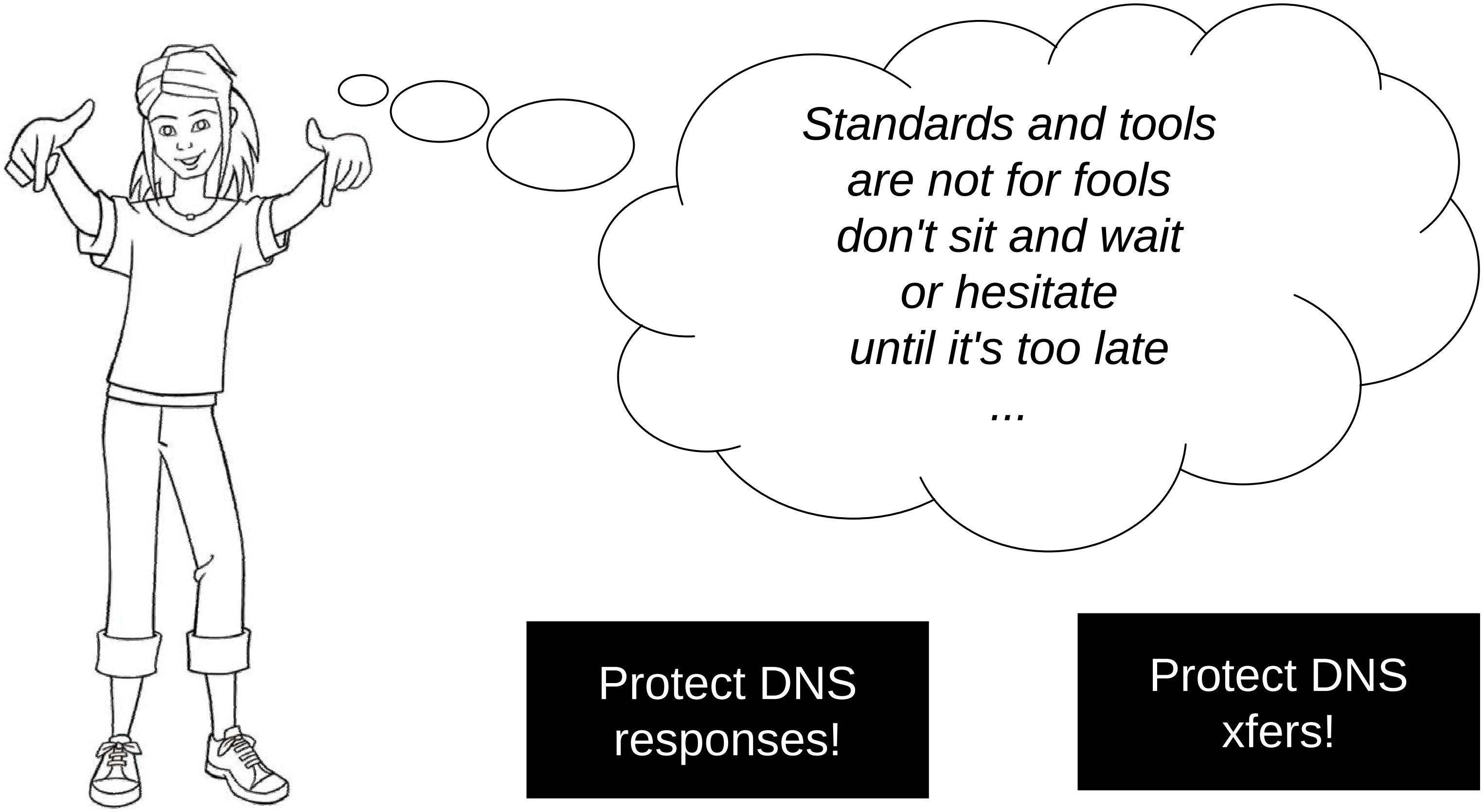
The Worst is Yet to Come ...

```
tld.      IN    NS    ns1.nic.tld.
          IN    NS    ns.secdns1.com.
          IN    NS    ns.secdns2.com.
          ...
```

- Secondaries pick up the zone from the fake.
- The attacker may also want to:
  - Increase the SOA serial to a high value.
  - Increase the $TTL of all RR's
  - Set SOA timers to 4,200,000,000 (133 years!)
  - Turn the fake primary DNS off after this happens.
  - Launch a DDOS against the real primary DNS.
  - etc.
- Consequences:
  - Secondaries will hold the wrong information.
  - It will take a couple of hours to fix the issue.
  - Cache pollution will last for days.

Act Now!

Your provider can’t protect you forever



Standards and tools
are not for fools
don't sit and wait
or hesitate
until it's too late
...

Protect DNS responses!

Protect DNS xfers!

Protect DNS Responses

- Advertise the primary DNS network as /24:
  - Yes, yes, I know ... routing table grows again ...
  - But will we ever have so that many TLD's? Come on ...
- Anycast:
  - If it's good for K and I root servers, why shouldn't be good for your TLD?
  - There are DNS hosting providers offering this as a service.
  - Narrows the impact of a fake advertisement.
- Promote DNSSEC and its operational simplicity among your customers.
  - Hahahahahahaha ... :-)

Protect DNS XFER's (1/2)

- Use a separate IP address for DNS XFER:
  - Better something than nothing.
  - Not the same address that will be used for queries
  - Do not delegate this one to the root!
  - Known by you and other secondaries.
  - Separate query and xfer traffic.

```
; --- root zone excerpt
$ORIGIN .
tld.           IN    NS    ns1.nic.tld.
ns1.nic.tld.   IN    A     192.0.2.1
tld.           IN    NS    ns-tld.secondary-provider.com.
...
```

Do not use the IP address of your primary DNS delegated in the root zone for zone xfer's!

Protect DNS XFER's (2/2)

- Use a protected link (e.g. IPsec tunnel) link between the networks of the primary and secondaries.
  - Usually possible only if you own both the primary and the secondary servers.
- **Protect xfers via TSIG:**
  - **Part of DNSSEC, but far from fully-blown DNSSEC.**
  - **Keys protect xfer only => zone signing is not needed**
  - **Easy and quick to set up, almost zero maintenance!**

As Network Operators You Can ...

- Tighten route filtering (well, at least keep trying …)
- Promote the use of DNSSEC wherever possible.
- Advise "special" customers to protect their DNS infra - think of:
  - Content providers (YouTube is not the only one ...)
  - Search engines
  - ccTLD and gTLD operators
  - ...
- Spread this message to the appropriate communities and forums:
  - IETF, RIPE, CENTR, ICANN/ccTLD etc.