



Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing

Porquê DNSSEC?

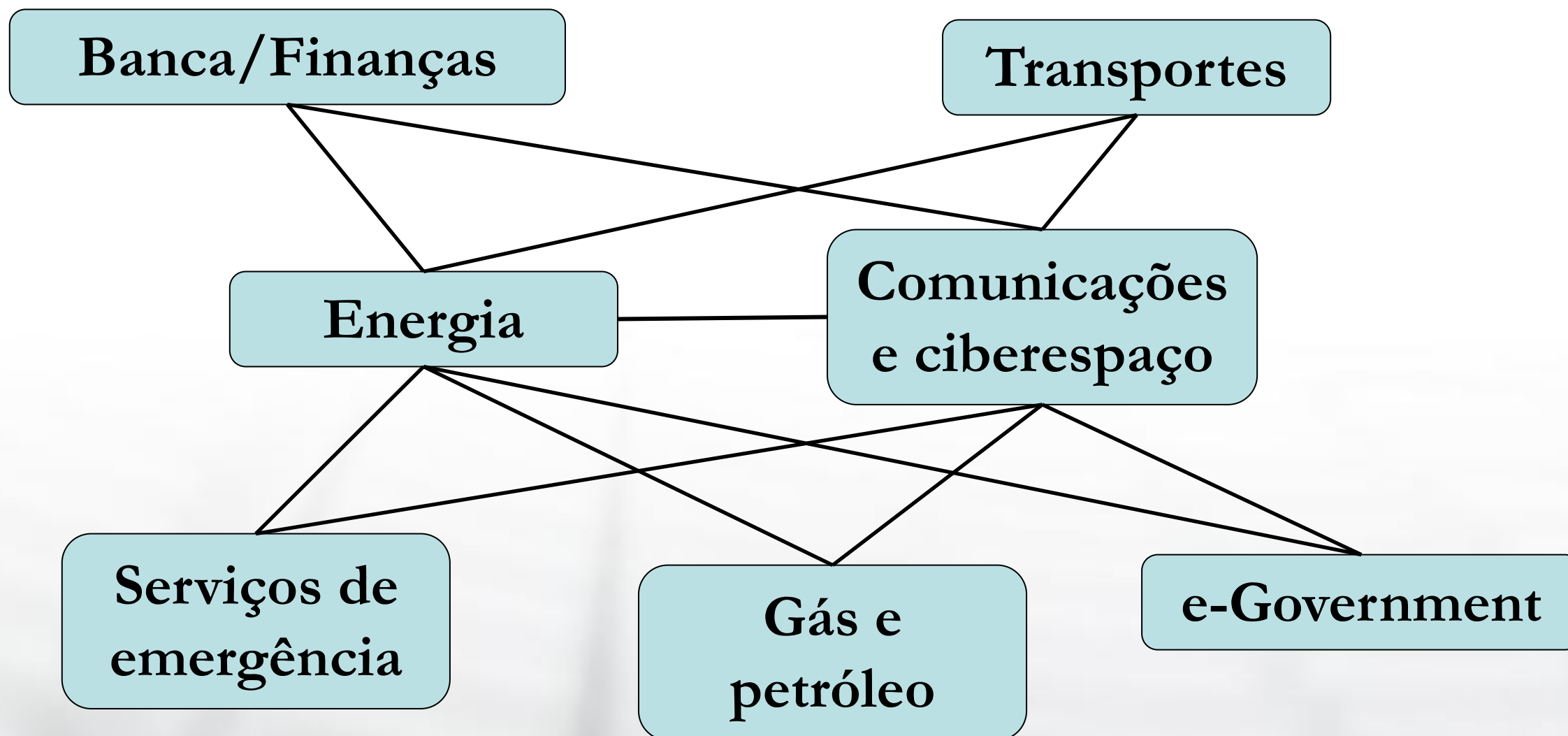
25 de Novembro 2009

Lino Santos

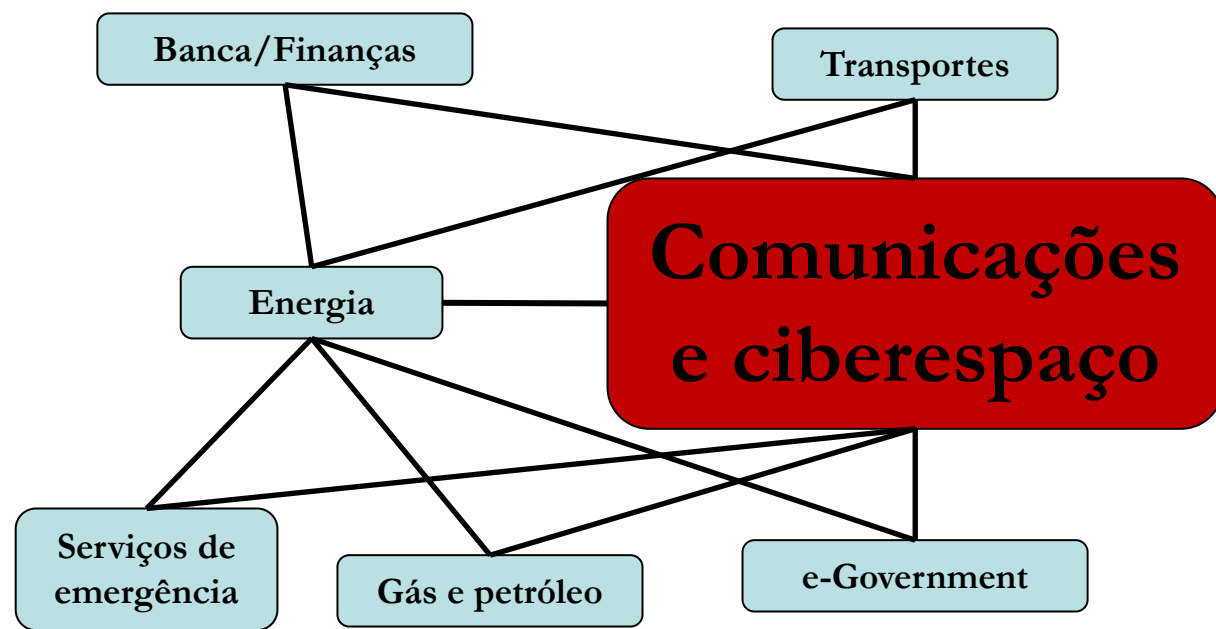
Segurança e Serviços à Comunidade



O DNS é uma infra-estrutura crítica da Internet



O DNS é uma infra-estrutura crítica da Internet



- US: Securing the Federal Government's Domain Name System Infrastructure
- Protecting Europe from large scale cyber-attacks and disruption (COM/2009/0149)
- Technologies to improve resilience (ENISA)

Ameaças ao bom funcionamento do DNS

- Disrrupção de serviço
- Personificação de sites web
- Fraude bancária
- Roubo de identidade
- Distribuição de malware
- ...
- Uma vez redireccionada a vítima, todo o tipo de ataques direccionados



**DNS AND CACHE
POISONING**



July 8th, 2008

Dan Kaminsky breaks DNS, massive multi-vendor patch coming, details at Black Hat Vegas '08


Posted by Nathan McFeters @ 2:59 pm




Categories: [Black Hat](#), [Black Hat Las Vegas](#), [Complex Attacks](#), [Hackers](#), [Patch Watch...](#)

Tags: [Black Hat](#), [DNS](#), [CERT](#), [Flaw](#), [Moquill...](#)

 **29** TalkBacks ADD YOUR OPINION

 SHARE
  PRINT
  E-MAIL
  WORTHWHILE?
  **+28** 30 VOTES



00:00 0%

It would seem there's a bigger story to that MS08-037 flaw that came out for Patch Tuesday today.

From Dave Lewis over at the Liquid Matrix security blog:

Today Dan Kaminsky released a first, as far as I can recall. A coordinated patch was released today by Dan Kaminsky of IO Active that fixes a vulnerability that apparently exists in all DNS servers.

Unlike other researchers who give up the gory details, Kaminsky took a wiser path by smiling and nodding. He'll give up the goods at Black Hat in August. That should give folks enough time to patch their systems.



The latest security.
The green bar.
Extended Validation SSL
from VeriSign. [Learn more >>](#)

Identified by VeriSign

Sponsored Links

- **MSc in digital innovation**
Future service design engineering systems security architecture
sde.tkk.fi
- **User provisioning**
Central user provisioning and identity management. White paper.
www.evidian.com

Recent Entries

- [Opera patches 'extremely severe' security hole](#)

July 23rd, 2008

Attack code published for DNS flaw

Posted by Ryan Naraine @ 2:55 pm

Categories: [Arbitrary Code Execution](#), [Botnets](#), [Browsers](#), [Data theft](#), [Exploit code...](#)

Tags: [DNS](#), [Exploit](#), [Attack](#), [Flaw](#), [Domain Names...](#)

 **31** TalkBacks ADD YOUR OPINION
 SHARE
 PRINT
 E-MAIL
 WORTHWHILE?
 **+14** 18 VOTES



The urgency to patch Dan Kaminsky's [DNS cache poisoning vulnerability](#) just went up a few notches.

Exploit code for the flaw, which allows the insertion of malicious DNS records into the cache of the target nameserver, has been added to Metasploit, a freely distributed attack/pen-testing tool.

According to Metasploit creator HD Moore (left), who teamed up with researcher [J\)ruid](#) to create the exploit, a DNS service has also been created to assist with the exploit.

[SEE: [Vulnerability disclosure gone awry: Understanding the DNS debacle](#)]

The code, [available here](#), takes aim at known deficiencies in the DNS protocol and common DNS implementations that aid in serious cache poisoning attacks.

This exploit caches a single malicious host entry into the target nameserver. By causing the target nameserver to query for random hostnames at the target domain, the attacker can spoof a response to the target server including an answer for the query, an authority server record, and an additional record for that server, causing target

Is the Printed Page Dead (or Just a Little Sick)?

Doc is a big believer in the power of print, but I do have to admit some print products are moving in new directions. That's why a

[read more >>](#)

Read Doc's blog on ZDNet

IN PARTNERSHIP WITH
RICOH™



Sponsored Links

- [It Security](#)
Physical Penetration Testing for IT Security Teams
www.amazon.co.uk
- [Europe IT Salary Report](#)
Want to benchmark if you are paid your tech worth. Register here!
www.activetechpros.com

Recent Entries

- [Opera patches 'extremely severe' security hole](#)
- [Exploit published for critical IE 7 zero-day flaw](#)

The **F**
S

Sm

Though
progre
on dive
that int
techno
busine
and ma
world a
[SmartP](#)

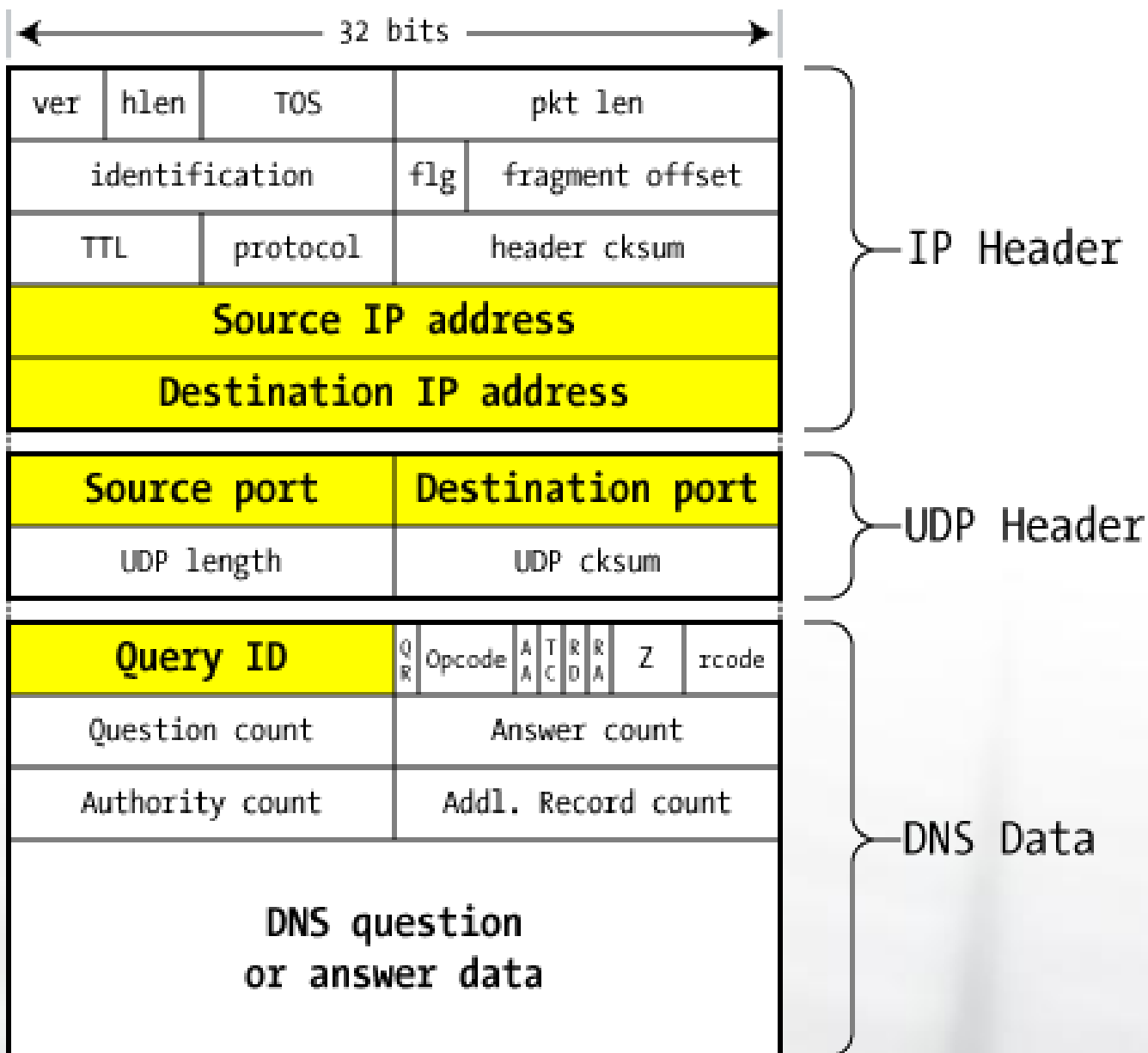
More f



Can yo
work s
[Learn m](#)
[Lotus S](#)

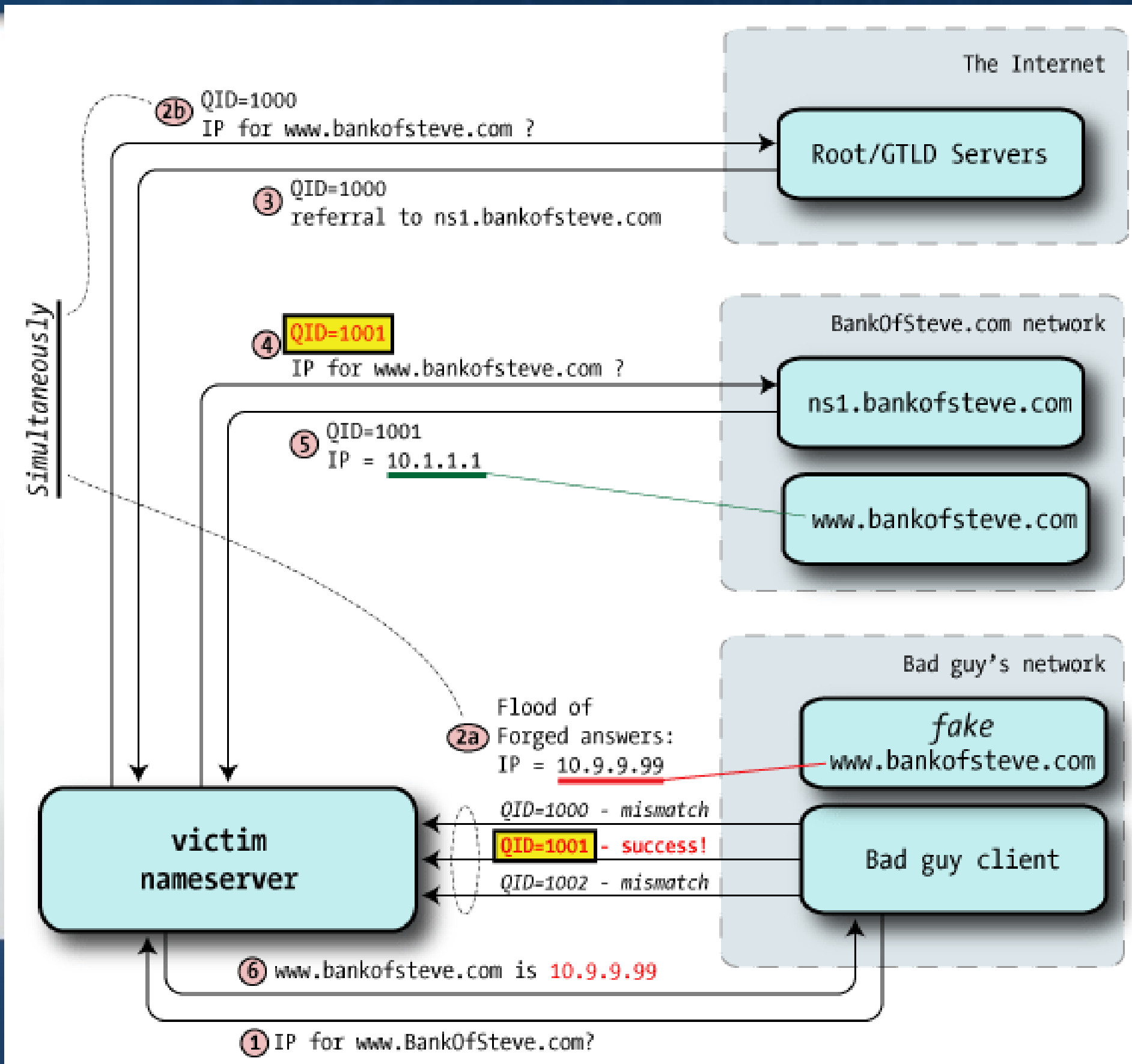
Learn h
smarte
optimiz
the IBM
approa
[Downlo](#)
[eBook](#)

Smarte
make s
produc
[Read th](#)
[IBM](#)



DNS packet on the wire

- Baixa entropia de informação no pacote DNS
- Query ID com 2^{16} valores possíveis
- Valor fácil de “adivinhar”
- Ataque facilitado com o aumento da largura de banda disponível





17/04/09 - 08h00 - Atualizado em 17/04/09 - 10h46

Ataque leva clientes do Virtua a site clonado de banco

Golpe permitiu redirecionamento de site do Bradesco e AdSense. Colunista resume essa e outras notícias de segurança da semana.

Altieres Rohr*
Especial para o G1

Tamanho da letra

A-

A+

Segurança para o PC Com Altieres Rohr

O fato mais marcante da semana na segurança da internet brasileira foi a confirmação de ataques sofisticados ao provedor de internet Virtua, que permitiram o redirecionamento do site do Bradesco e do AdSense, do Google, a endereços maliciosos, com o objetivo de roubar dados e instalar um cavalo de troia, respectivamente.

Também no resumo desta semana: rede do Conficker é ativada para distribuir anti-spyware fraudulento; Microsoft elimina 20 brechas de segurança, entre elas a vulnerabilidade no Excel desde fevereiro.

Se você tem alguma dúvida sobre segurança da informação (antivírus, invasões, cibercrime, roubo de dados, etc), vá até o fim da reportagem e utilize a seção de comentários. A coluna responde perguntas deixadas por leitores todas as quartas-feiras.

editorias

Primeira Página

Blogs e Colunas

Brasil

Carros

Ciência e Saúde

Cinema

Concursos e Emprego

Economia e Negócios

Esporte

Mundo

Música

Planeta Bizarro

Política

Pop & Arte

Rio de Janeiro

public

A
C
s

/
2
C
p
P
2
A
re
p
2
M
a

- Limitar o acesso ao resolver – não funciona para infra-estruturas de ISP
- Mecanismos de segurança perimétrica - idem
- DNSCurve (cifra na comunicação – mais lento)
- DNSSEC
 - “No better, no easier, no cheaper alternative” ENISA



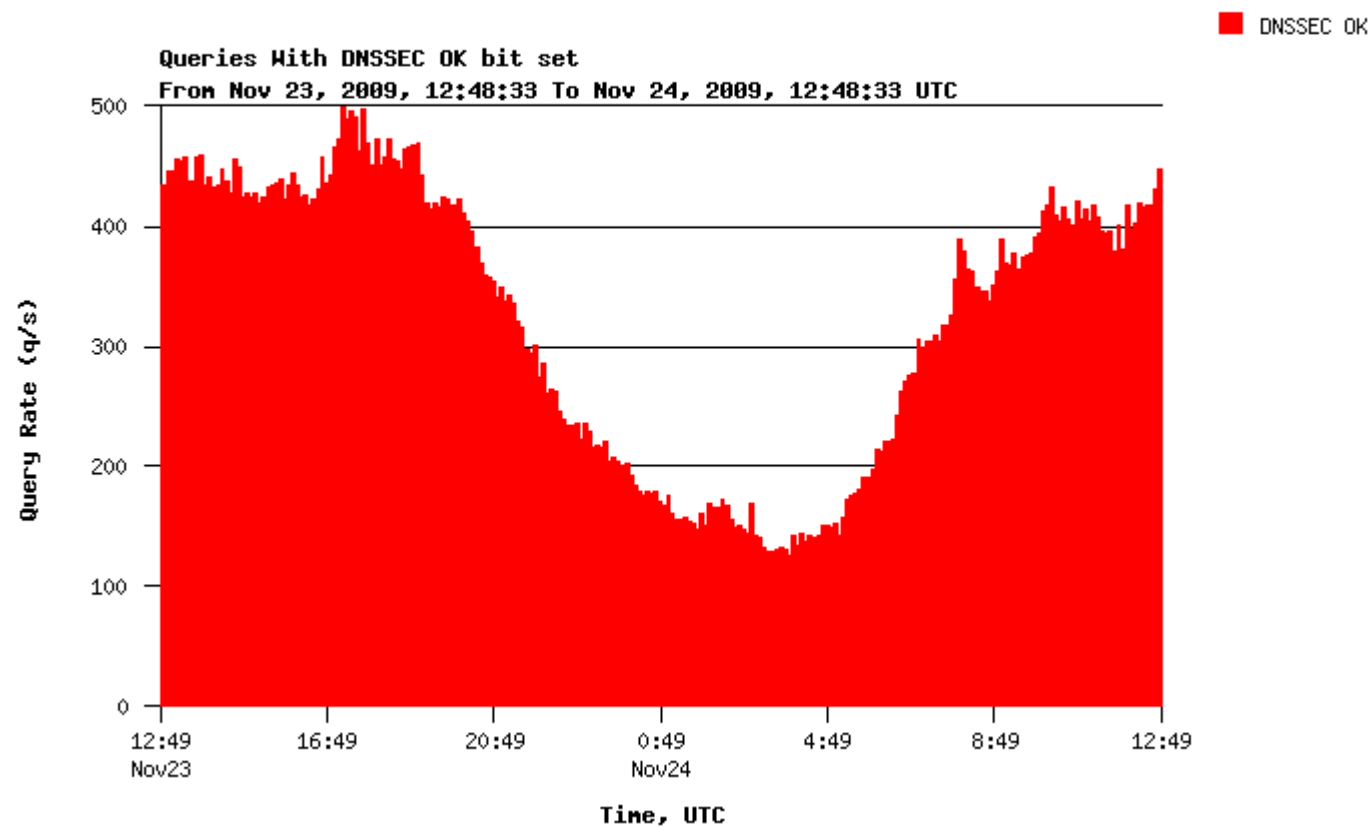


registro.br



CZ.nic
cz domain registry

DNSSEC Support



Mirror K de Genebra; Fonte: RIPE

Deployment status as of: *Tue Nov 24 12:09:02 2009 UTC*

Monitoring Summary:

18850 Zones

16897 Zones have NS sets that match their parents' delegation set

9224 DNSSEC enabled zones

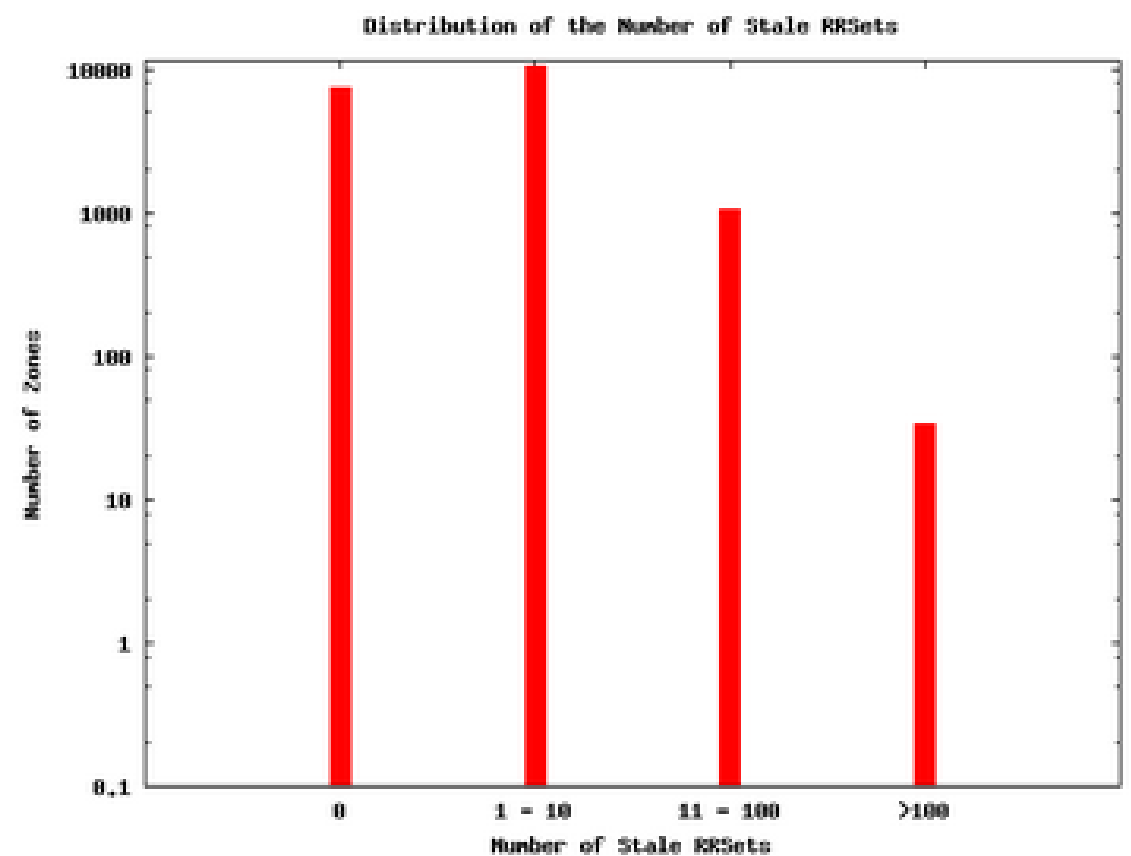
4805 Zones use both KSKs and ZSKs

3709 Production DNSSEC-enabled zones

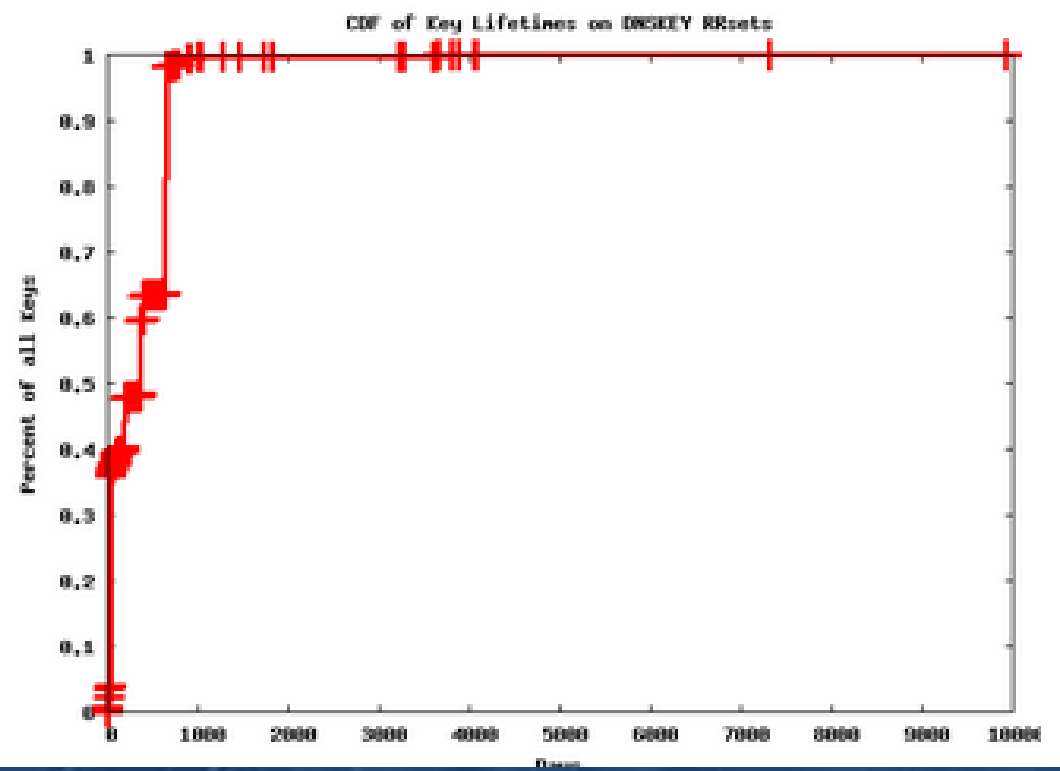
Distribution of key algorithms in use:

Algorithm	# Keys
RSA/MD5 [RSAMD5]	15
Diffie-Hellman [DH]	0
DSA/SHA-1 [DSA]	23
Elliptic Curve [ECC]	0
RSA/SHA-1 [RSASHA1]	16498
Indirect [INDIRECT]	0
RSA-NSEC3-SHA1 [RSASHA1-NSEC3-SHA1]	407
Private [PRIVATEDNS]	0
Private [PRIVATEOID]	0
Reserved 0	0
Reserved 255	0
Unknown Key 6	2
Unresolved Names	0

Production DNSSEC-enabled Zones: (in DNS canonical order):



Distribution of the number of vulnerable RRsets in zones



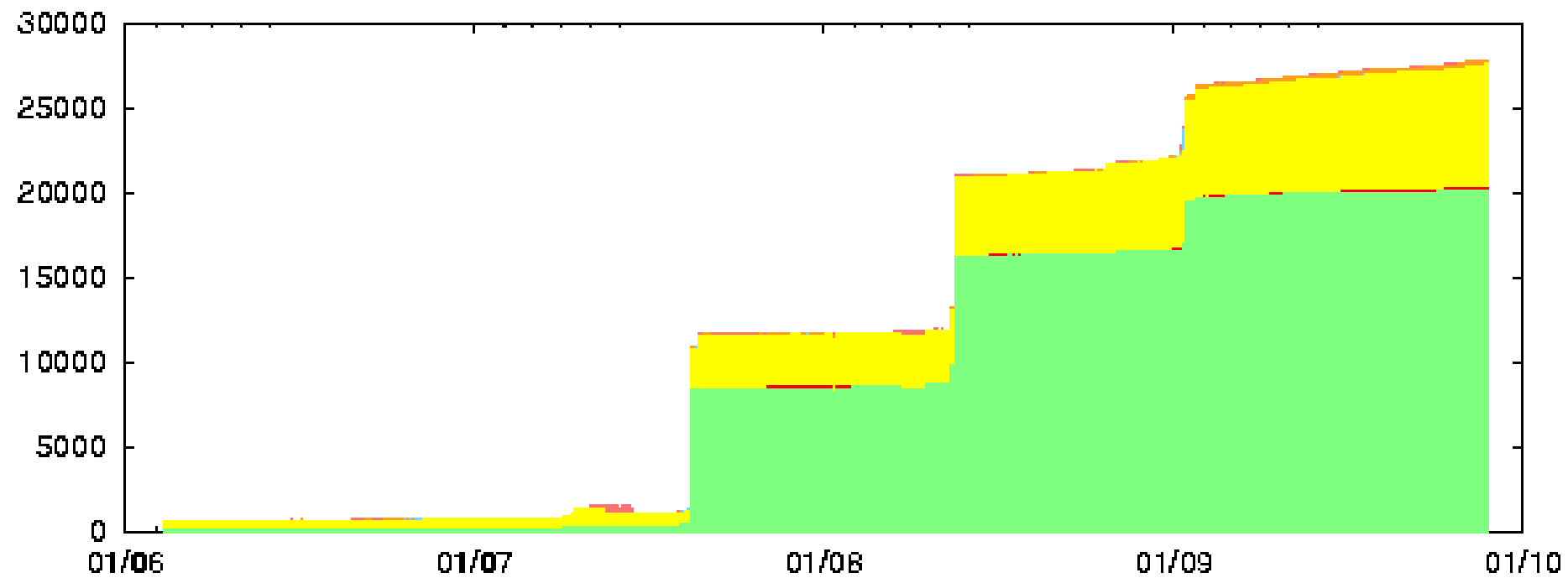
Content of dnssec.iks-jena.de

Serial# 2009112501

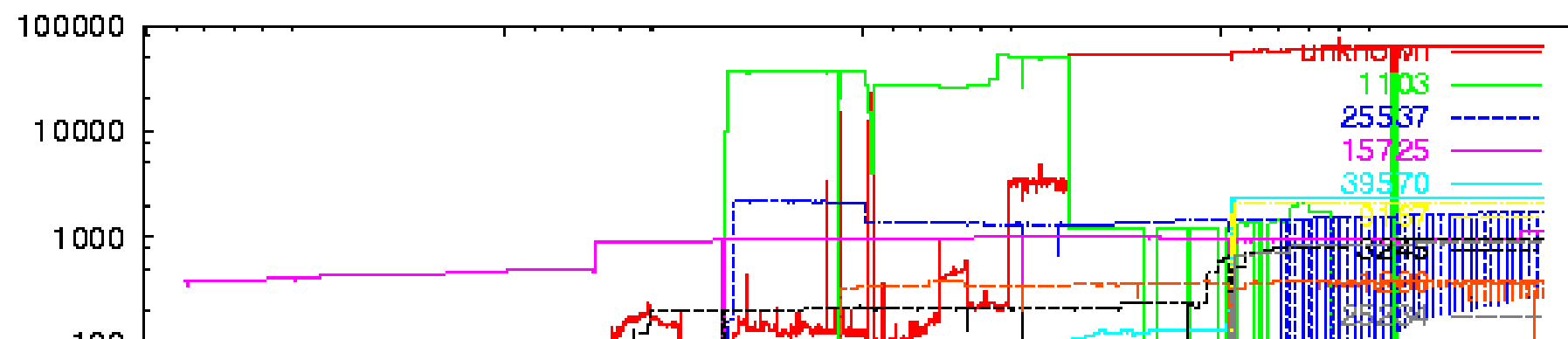
Overview about 26184 secured domains

Count	Source Description
38	DNSKEY unreachable and no parent: dead?
248	DNSKEY unreachable, parent signature found
0	unclassified new entry, DNSKEY retrieved
6967	DNSKEY found but no parent => Security Entry Point
156	DNSKEY found but chain is broken
18775	DNSKEY found and signed by parent

History of deployment



Top 10 autonomous systems injecting DNSSEC





Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing

E porque não DNSSEC?

É fácil

Melhora a segurança dos serviços em linha

Melhora a confiança dos utilizadores nesses serviços

- DNSSEC em Portugal
<http://www.dnssec.pt>
- Secure Domain Name System (DNS) Deployment Guide
<http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf>
- Incident Response to Guide to the Kaminsky DNS Cache Poison Exploit
<http://www.team-cymru.org/ReadingRoom/Whitepapers/2008/kaminsky-cache-poison-ir.pdf>
- DNS Spoofing by The Man In The Middle
http://www.sans.org/reading_room/whitepapers/dns/dns_spoofing_by_the_man_in_the_middle_1567?show=1567.php&cat=dns
- DNSSEC Frequently Asked Questions (and a few Frequently Heard Myths)
<http://www-x.antd.nist.gov/dnssec/faq.html>