Covert channels: o que são, o que fazem e como se prevenir contra eles

Rede Nacional de Ensino e Pesquisa - RNP
Centro de Atendimento a Incidentes de Segurança - CAIS
Dezembro de 2006

Ivo de Carvalho Peixinho
ivocarv@cais.rnp.br

RNP/PAL/0198

CAIS

Sumário

CAIS

Introdução

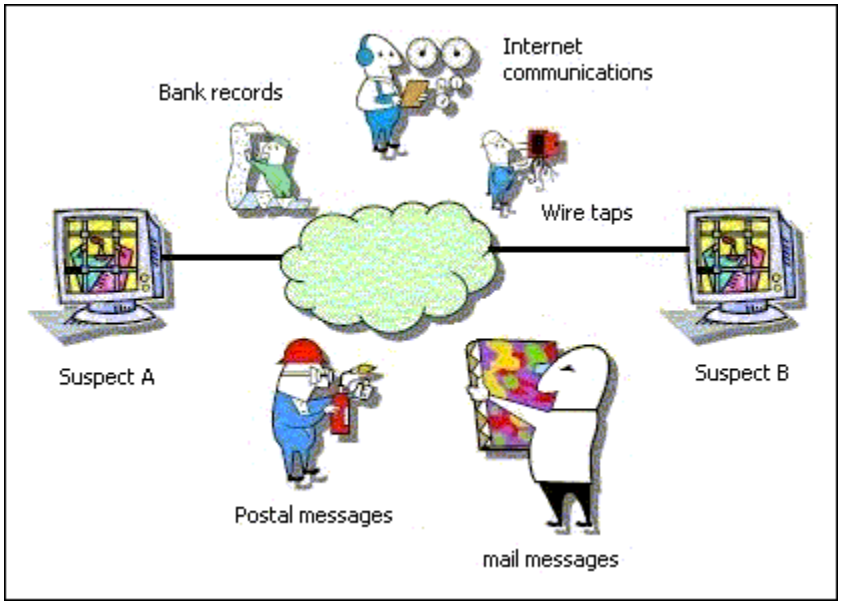
- Covert channels
  - Canais "camuflados"
  - Transferência de informação através de um canal escondido
    - Ocultar informação na rede
  - Exemplos
    - Túneis IPv6
    - Túneis ICMP
    - Túneis DNS
    - Steganografia
    - TCP/IP Headers

Um covert channel é um canal de comunicação que permite a um processo transmitir informação de uma forma que viola a política de segurança do sistema

CAIS

Introdução

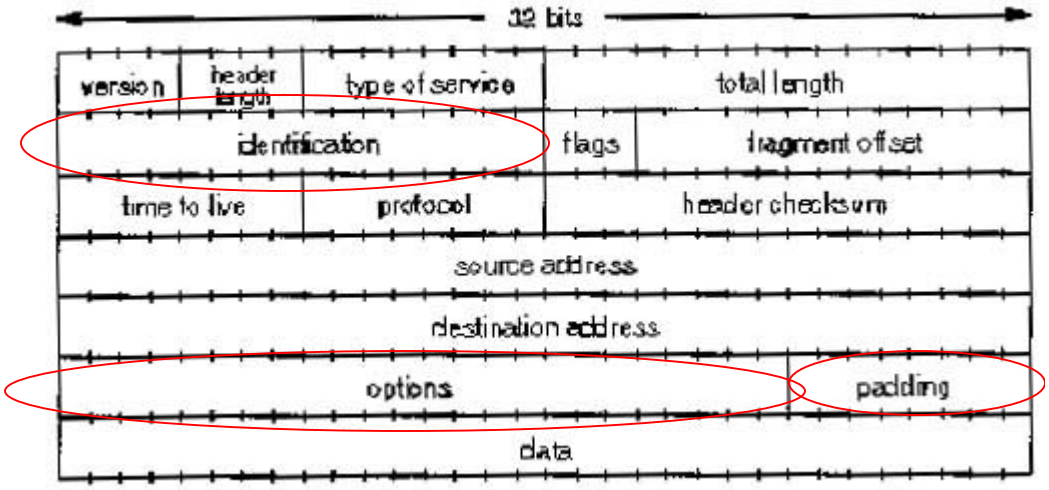
- Covert channels – "Finalidades"
  - Esconder informação que trafega na rede
    - Botnets
    - Worms
    - Honeypots / honeynets
  - Burlar *firewalls* e sistemas de autenticação
    - Botnets
    - *Captive Portals* de provedores Wireless
    - Autenticação ADSL



CAIS

Introdução

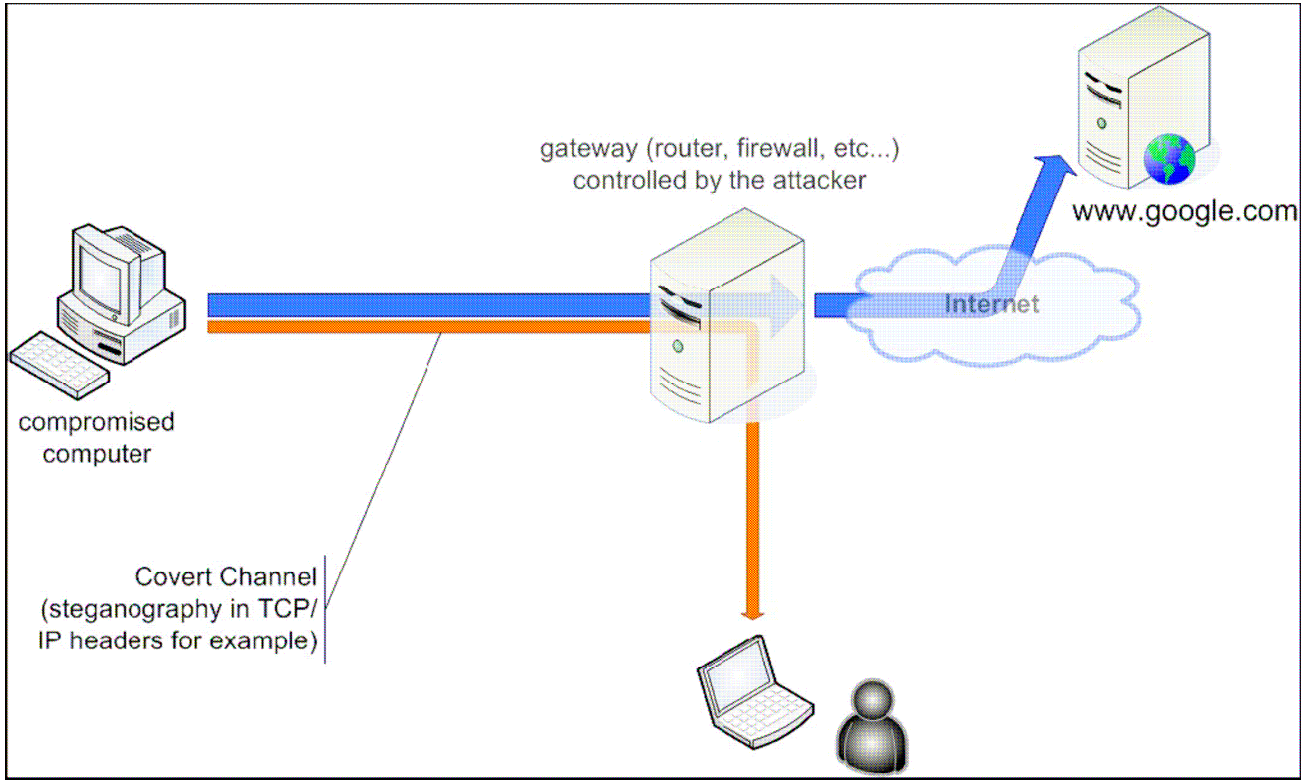
- Covert channels em TCP/IP headers
- Pacote IP
  - 16 bit identification field
    - Identificação de fragmentos
  - 24 bit IP Options
  - 8 bit padding
- Pacote TCP
  - 32 bit sequence number
  - 32 bit acknowledge number



CAIS

Introdução

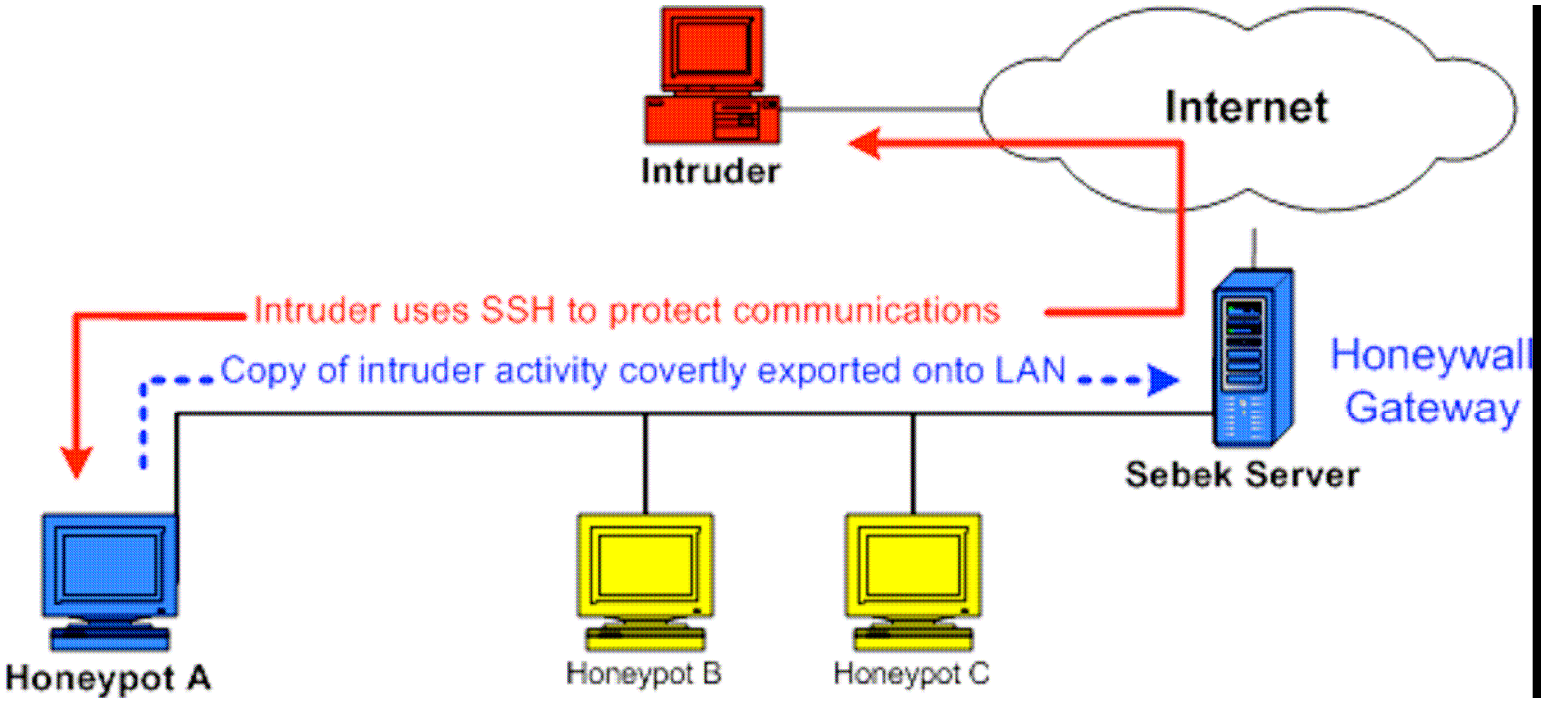
- Covert channels - Implementações
  - The Implementation of Passive Covert Channels in the Linux Kernel – Joanna Rutkowska Dec 2004 (NUSHU)



CAIS

Introdução

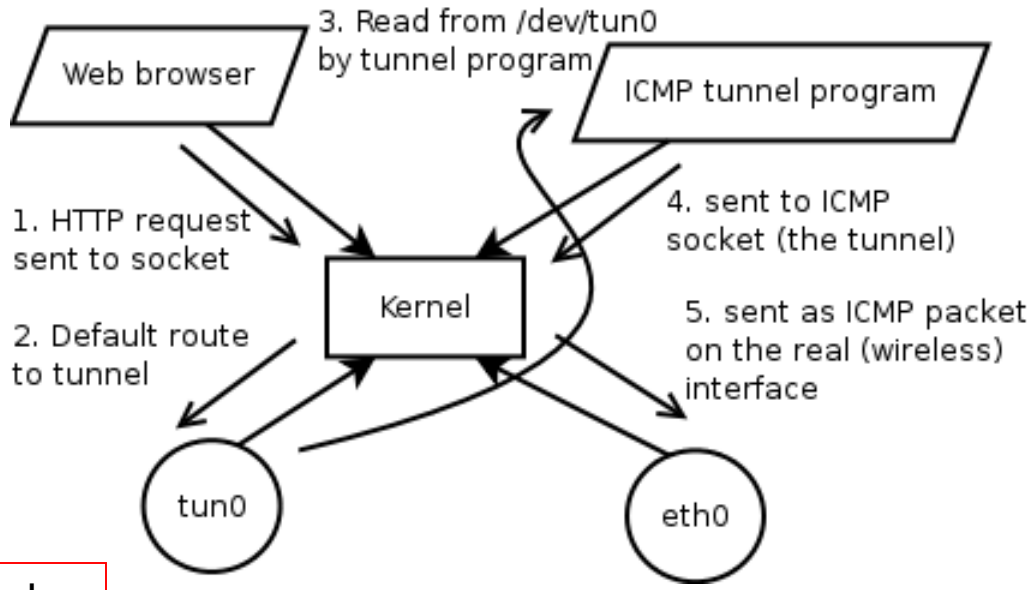
- Covert channels - Implementações
  - Know your enemy – Sebek – Nov 2003



CAIS

Introdução

- Covert channels - Implementações
  - IP sobre ICMP
    - Encapsulamento de pacotes IP dentro de pacotes ICMP
      - Túnel ICMP
    - Ferramentas
      - ICMPTX
      - itun
      - PingTunnel
      - Ptunnel



ICMPTX Utiliza icmp types 0 (echo reply) e 8 (echo request)

CAIS

Introdução

- Covert channels - Implementações
  - IP sobre DNS
    - Encapsulamento de pacotes IP dentro de pacotes DNS
    - Ferramentas
      - NSTX
      - OzymanDNS (Dan Kaminsky)
      - DNScat
  - Porque DNS?
    - Normalmente liberado em *firewalls*
    - Wireless *captive portals* aceitam tráfego DNS
    - Autenticação ADSL

Covert Channels usando DNS

- IP Sobre DNS – Funcionamento (OzymanDNS)
  - Envio de pacotes
    - Nome DNS comporta até 253 caracteres
    - 63 caracteres entre os pontos (.)
    - Codificação de informação usando base32
      - Um caracter para cada 5 bits (a-z, 0-6)
      - 180 caracteres (3 grupos de 60) separados por pontos = 180 * 5 = 900 bits = 112 bytes por consulta

Exemplo:
zjabdbcctvaojbz55mqwe224ceyeltkbhyaasncpljgc53pirtsmuzihcjrw.uujca7ytd3tifmmglrcsl65r3w3ba4mixix6nemd6eulfy2ss62xmff3zecv.ttivj2trx642zlrgpbwo2f2glnxk7yxyu3pfeiuvgawc7mijpqn5sh4j.63034-0.id-1187.up.foo.com

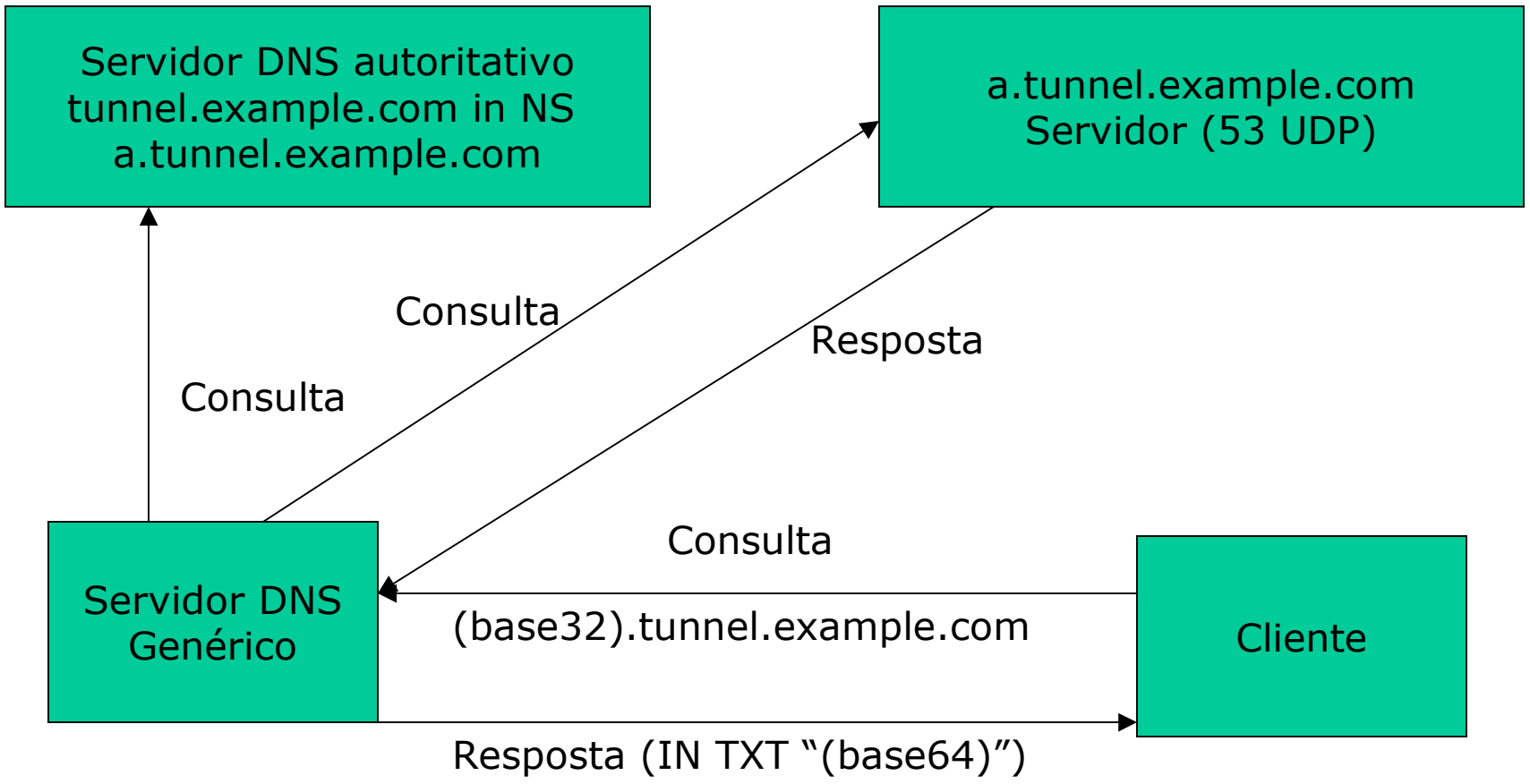
Covert Channels usando DNS

- IP Sobre DNS - Funcionamento
  - Recebimento de pacotes
    - Pacotes DNS até 512 bytes
      - Fragmentação
    - Registros TXT (SPF)
      - Codificação de informação usando base64
      - Um caracter para cada 6 bits (a-z, A-Z, 0-9,=,/)

Exemplo:
"MCaydY5mzxGm2QCqAGLObIAKAAAAAAAACAAAAAECMyaydY5mzxGm2QCqAGLObCwAAAAAAAAAAgAC\010AAIAAgACAAAAAAAAAAAACh3KuMR6nPEY7kAMAMIFNlaAAAAAAAAAAlpqVwQ5lVTr9mPCY=\010"

Covert Channels usando DNS

- Arquitetura



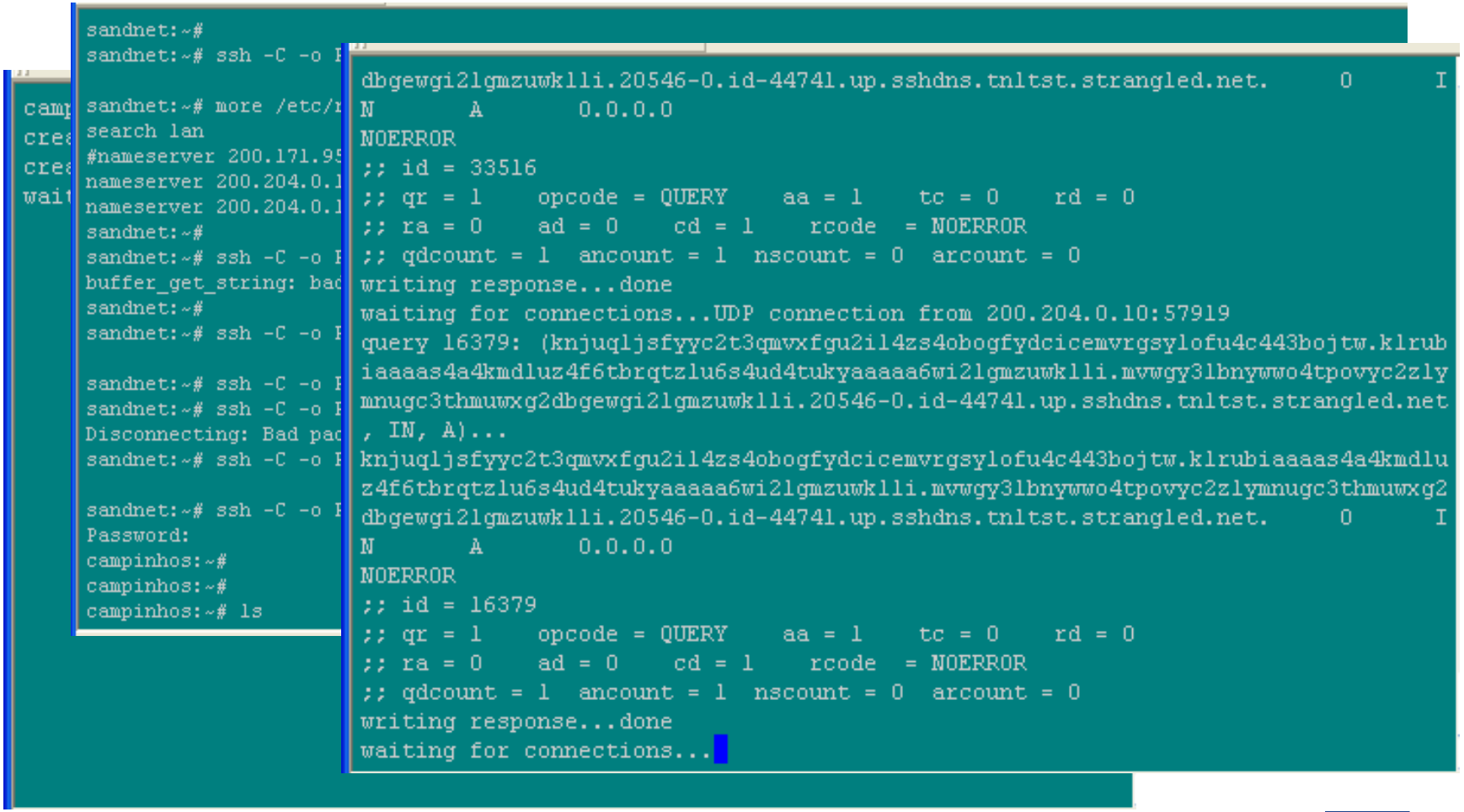
Covert Channels usando DNS

- Arquitetura
  - Máquina com autoridade DNS
    - Criação de um subdomínio para o servidor IP-sobre-DNS (IN NS)
    - Serviços de redirecionamento gratuitos (freedns.afraid.org)
  - Máquina com endereço IP válido / servidor IP-sobre-DNS (ex: speedy)
    - Porta 53 UDP disponível
    - OzymanDNS + SSH Forwarding
    - NSTX + interfaces tun
    - DNScat + PPPD
  - Cliente IP-sobre-DNS / laptop Wireless

Covert Channels: o que são, o que fazem e como se prevenir contra eles

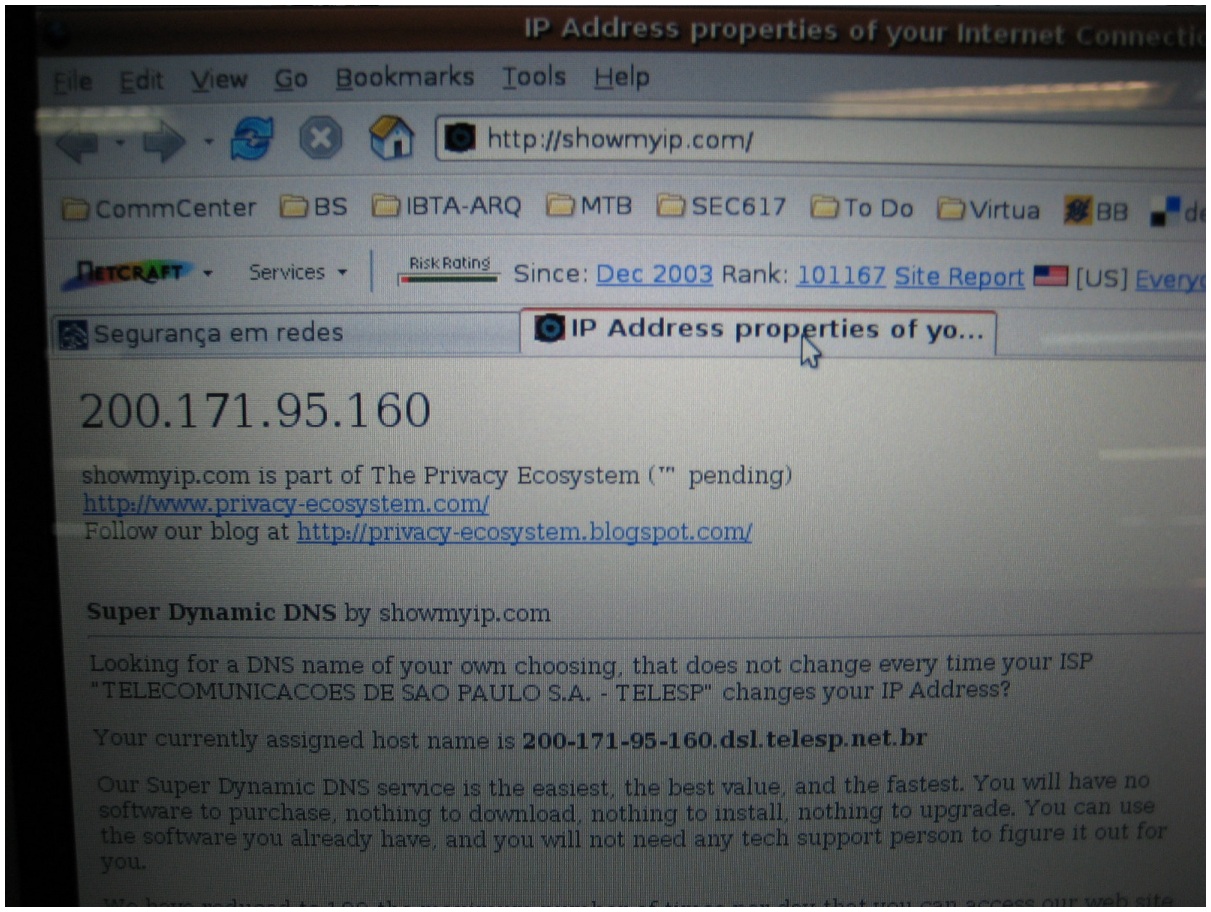
CAIS

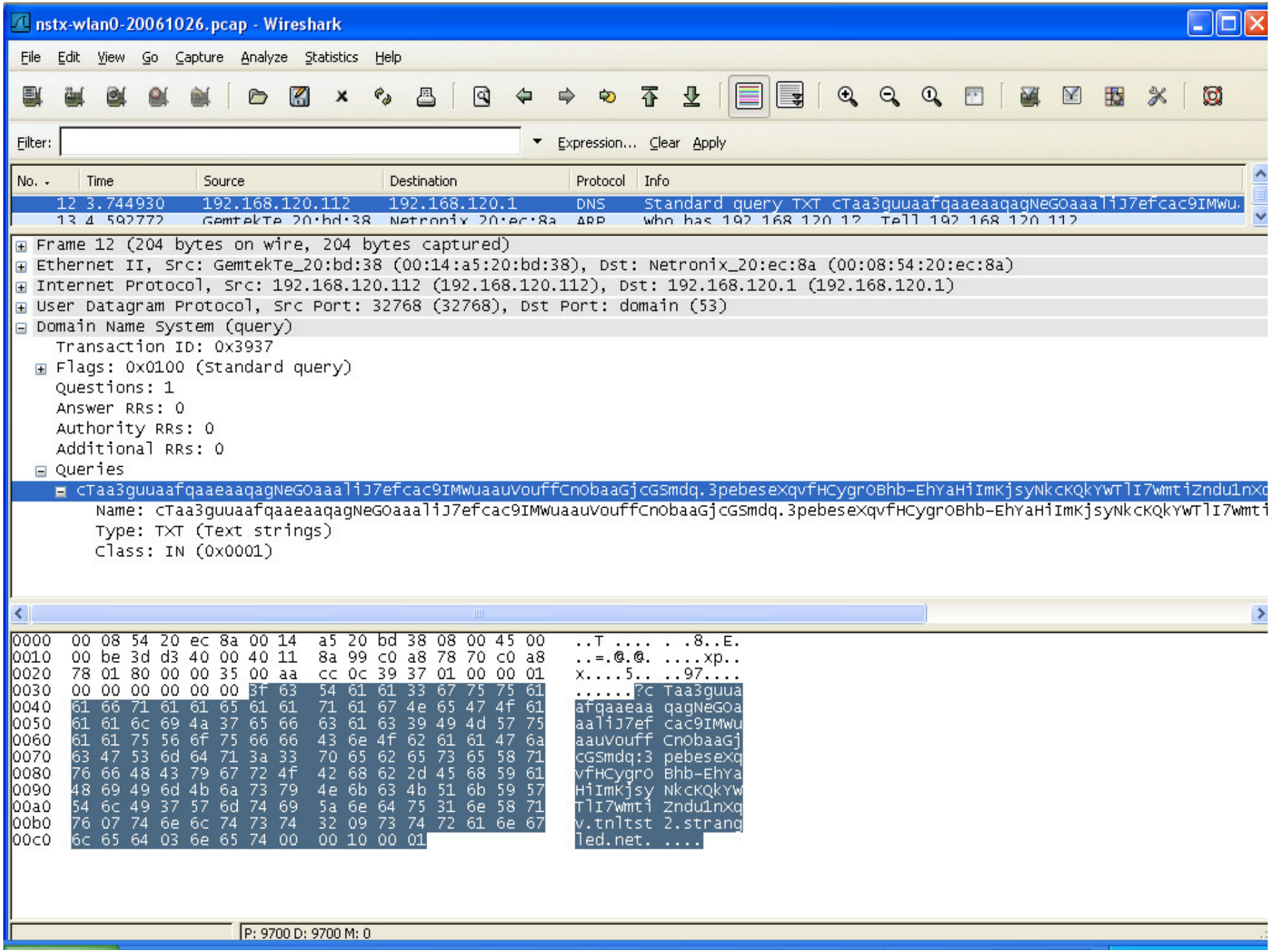
Covert Channels usando DNS

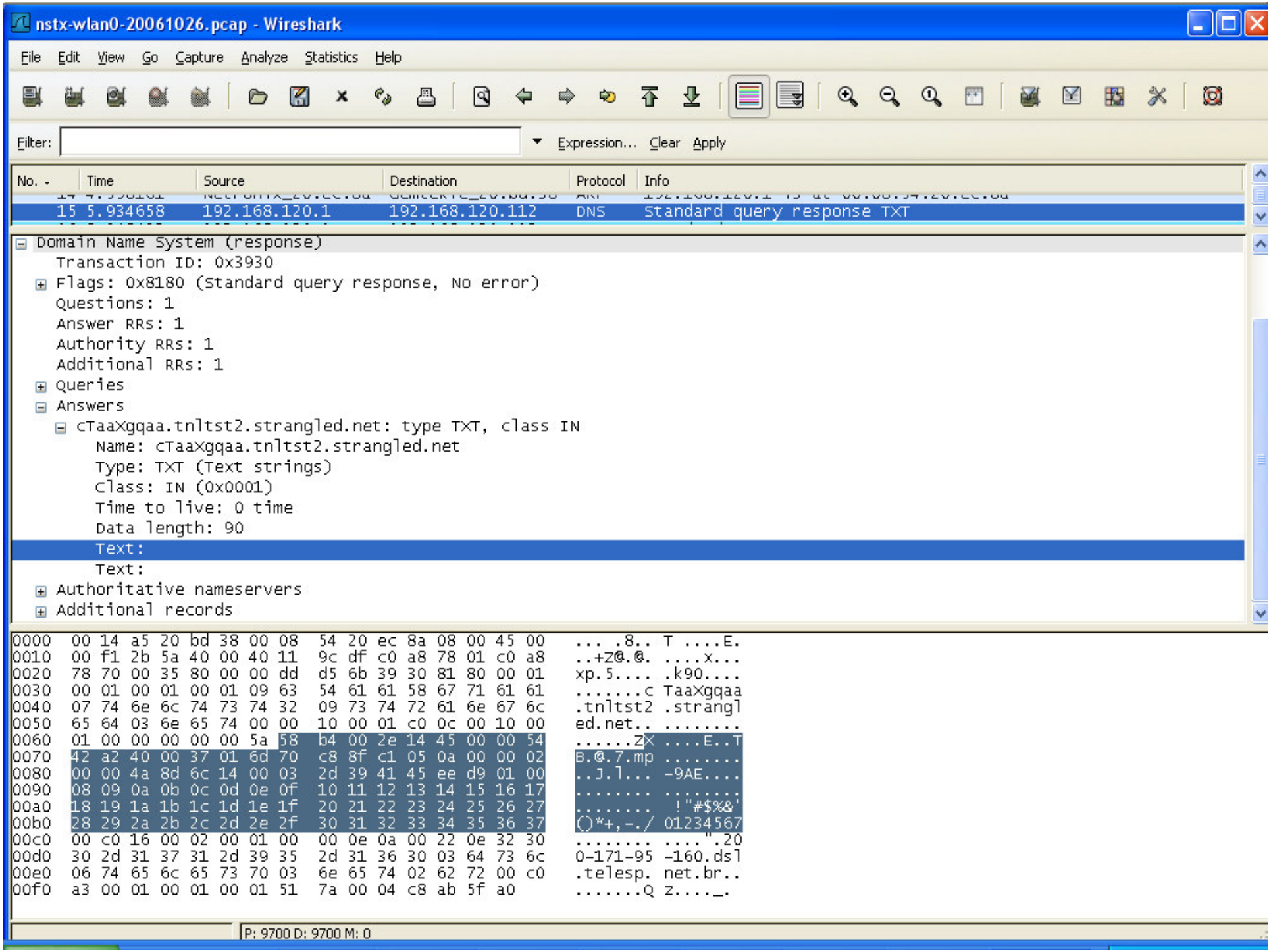


CAIS

Covert Channels usando DNS




nstx-wlan0-20061026.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
12 3.744930 192.168.120.112 192.168.120.1 DNS Standard query TXT cTaa3guuaafqaaeaaqagNeGOaaaliJ7efcac9IMWu.
13 4.592772 GemtekTe_20:bd:38 Netronix_20:ec:8a ARP Who has 192.168.120.1? Tell 192.168.120.112
Frame 12 (204 bytes on wire, 204 bytes captured)
Ethernet II, Src: GemtekTe_20:bd:38 (00:14:a5:20:bd:38), Dst: Netronix_20:ec:8a (00:08:54:20:ec:8a)
Internet Protocol, Src: 192.168.120.112 (192.168.120.112), Dst: 192.168.120.1 (192.168.120.1)
User Datagram Protocol, Src Port: 32768 (32768), Dst Port: domain (53)
Domain Name System (query)
Transaction ID: 0x3937
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
cTaa3guuaafqaaeaaqagNeGOaaaliJ7efcac9IMWuaauVouffCnObaaGjcGSmdq.3pebeseXqvfHCygrOBhb-EhYaHiImKjsyNkcKQkYWTlI7wmtiZndu1nXq
Name: cTaa3guuaafqaaeaaqagNeGOaaaliJ7efcac9IMWuaauVouffCnObaaGjcGSmdq.3pebeseXqvfHCygrOBhb-EhYaHiImKjsyNkcKQkYWTlI7wmti
Type: TXT (Text strings)
Class: IN (0x0001)
0000 00 08 54 20 ec 8a 00 14 a5 20 bd 38 08 00 45 00 ..T .... . .8..E.
0010 00 be 3d d3 40 00 40 11 8a 99 c0 a8 78 70 c0 a8 ..=.@.@. ....xp..
0020 78 01 80 00 00 35 00 aa cc 0c 39 37 01 00 00 01 x....5.. ..97....
0030 00 00 00 00 00 00 3f 63 54 61 61 33 67 75 75 61 ......?c Taa3guua
0040 61 66 71 61 61 65 61 61 71 61 67 4e 65 47 4f 61 afqaaeaa qagNeGOa
0050 61 61 6c 69 4a 37 65 66 63 61 63 39 49 4d 57 75 aaliJ7ef cac9IMWu
0060 61 61 75 56 6f 75 66 66 43 6e 4f 62 61 61 47 6a aauVouff CnObaaGj
0070 63 47 53 6d 64 71 3a 33 70 65 62 65 73 65 58 71 cGSmdq:3 pebeseXq
0080 76 66 48 43 79 67 72 4f 42 68 62 2d 45 68 59 61 vfHCygrO Bhb-EhYa
0090 48 69 49 6d 4b 6a 73 79 4e 6b 63 4b 51 6b 59 57 HiImKjsy NkcKQkYW
00a0 54 6c 49 37 57 6d 74 69 5a 6e 64 75 31 6e 58 71 TlI7Wmti Zndu1nXq
00b0 76 07 74 6e 6c 74 73 74 32 09 73 74 72 61 6e 67 v.tnltst 2.strang
00c0 6c 65 64 03 6e 65 74 00 00 10 00 01 led.net. ....
P: 9700 D: 9700 M: 0


nstx-wlan0-20061026.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
15 5.934658 192.168.120.1 192.168.120.112 DNS Standard query response TXT
Domain Name System (response)
Transaction ID: 0x3930
Flags: 0x8180 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 1
Additional RRs: 1
Queries
Answers
cTaaXgqaa.tnltst2.strangled.net: type TXT, class IN
Name: cTaaXgqaa.tnltst2.strangled.net
Type: TXT (Text strings)
Class: IN (0x0001)
Time to live: 0 time
Data length: 90
Text:
Text:
Authoritative nameservers
Additional records
0000 00 14 a5 20 bd 38 00 08 54 20 ec 8a 08 00 45 00 ... .8.. T ....E.
0010 00 f1 2b 5a 40 00 40 11 9c df c0 a8 78 01 c0 a8 ..+Z@.@. ....x...
0020 78 70 00 35 80 00 00 dd d5 6b 39 30 81 80 00 01 xp.5.... .k90....
0030 00 01 00 01 00 01 09 63 54 61 61 58 67 71 61 61 ....c TaaXgqaa
0040 07 74 6e 6c 74 73 74 32 09 73 74 72 61 6e 67 6c .tnltst2 .strangl
0050 65 64 03 6e 65 74 00 00 10 00 01 c0 0c 00 10 00 ed.net.. ....
0060 01 00 00 00 00 00 5a 58 b4 00 2e 14 45 00 00 54 ......ZX ....E..T
0070 42 a2 40 00 37 01 6d 70 c8 8f c1 05 0a 00 00 02 B.@.7.mp ....
0080 00 00 4a 8d 6c 14 00 03 2d 39 41 45 ee d9 01 00 ..J.l... -9AE....
0090 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 ....
00a0 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 .... !"#$%&'
00b0 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,-./ 01234567
00c0 00 c0 16 00 02 00 01 00 00 0e 0a 00 22 0e 32 30 ....".20
00d0 30 2d 31 37 31 2d 39 35 2d 31 36 30 03 64 73 6c 0-171-95 -160.dsl
00e0 06 74 65 6c 65 73 70 03 6e 65 74 02 62 72 00 c0 .telesp. net.br..
00f0 a3 00 01 00 01 00 01 51 7a 00 04 c8 ab 5f a0 ....Q z...._.
P: 9700 D: 9700 M: 0

Detectando Covert Channels

- Verificar anomalias em cabeçalhos IP, TCP, ICMP
- Verificar desvios de tráfego normal (IDS estatístico)
- Verificar conteúdo de tráfego ICMP (Ex: ping)
  - Magic numbers (ex: 0xD5200880 – ptunnel)
- Verificar conteúdo de cabeçalhos HTTP e POST requests
- Verificar consultas TXT no DNS
- Verificar excesso de consultas DNS
- Monitorar tráfego IPv6

CAIS

Bloqueando Covert Channels

- Sanitizar ou bloquear tráfego anômalo
- Bloquear IP spoofing
- Bloquear echo request/respose, ou limitar a taxa de transmissão
- Utilizar um servidor proxy HTTP para processar requisições
  - Restringir o uso de cabeçalhos HTTP
- Bloquear consultas TXT
  - Problemas com SPF
- Limitar requisições DNS sucessivas de um mesmo endereço

Detectar e bloquear covert channels é uma tarefa complexa. Normalmente é necessário saber o que se está procurando

Conclusões

- Covert channels são uma realidade
  - Existem ferramentas desenvolvidas com esta finalidade
- Existe *malware* utilizando covert channels
  - Túneis IPv6
  - Tráfego escondido em consultas BGP
- Detecção e bloqueio de covert channels é uma tarefa complexa
  - Necessita saber o que se está procurando
- **Monitorar o tráfego entrando e saíndo na sua rede**
  - Anomalias em pacotes
  - Variações do tráfego normal

CAIS

Referências

- http://www.securityfocus.com/news/11406
- http://www.digitalsec.net/stuff/texts/dns-tunnelingv0.2-en.txt
- http://en.wikipedia.org/wiki/Covert_channel
- http://tadek.pietraszek.org/projects/DNScat/
- http://www.plenz.com/tunnel-everything
- http://dnstunnel.de/
- http://thomer.com/icmptx/
- http://thomer.com/howtos/nstx.html

Referências

- http://www.rsasecurity.com/rsalabs/node.asp?id=2351
- http://www.firstmonday.org/issues/issue2_5/rowland/
- http://kruptos.inchcolm.org/
- http://www.linuxexposed.com/content/view/153/1/
- http://www.waterken.com/dev/Enc/base32/
- http://staff.science.uva.nl/~delaat/snb-2005-2006/p27/report.pdf
- http://www.invisiblethings.org/
- http://directory.fsf.org/network/misc/PTunnel.html
- http://freedns.afraid.org/

CAIS

Informações de Contato

Centro de Atendimento a Incidentes de Segurança – CAIS

cais@cais.rnp.br - http://www.rnp.br/cais

Ivo de Carvalho Peixinho – ivocarv@cais.rnp.br
Ronaldo Vasconcellos – ronaldo@cais.rnp.br

CAIS

Contato com o CAIS: Notificação de Incidentes

Incidentes de segurança envolvendo redes conectadas ao backbone da RNP podem ser encaminhadas ao CAIS por:

1. ***E-mail*: cais@cais.rnp.br**

Para envio de informações criptografadas, recomenda-se o uso da chave PGP pública do CAIS, disponível em: **http://www.rnp.br/cais/cais-pgp.key**

2. ***Web*:** Através do Formulário para Notificação de Incidentes de Segurança, disponível em **http://www.rnp.br/cais/atendimento_form.html**

INOC-DBA

Para entrar em contato com o CAIS através da hotline INOC-DBA (Inter-NOC Dial-By-ASN): INOC-DBA: 1916*800

Atendimento Emergencial

Contatos emergenciais fora do horário comercial (09:00 - 18:00) devem ser feitos através do telefone **(61) 3217-6355**

Alertas do CAIS

O CAIS mantém a lista **rnp-alerta@cais.rnp.br**, com assinatura aberta à comunidade atuante na área. Inscrições através do formulário disponível em:

http://www.rnp.br/cais/alertas