Resposta à incidentes

Diagnósticos equivocados e finais felizes

Nelson Murilo
http://twitter.com/nelsonmurilo

Casos

Ataques de IP Spoofing

Pacotes não mentem

Mais que log de erros

CASO 1

Ataques de IP Spoofing

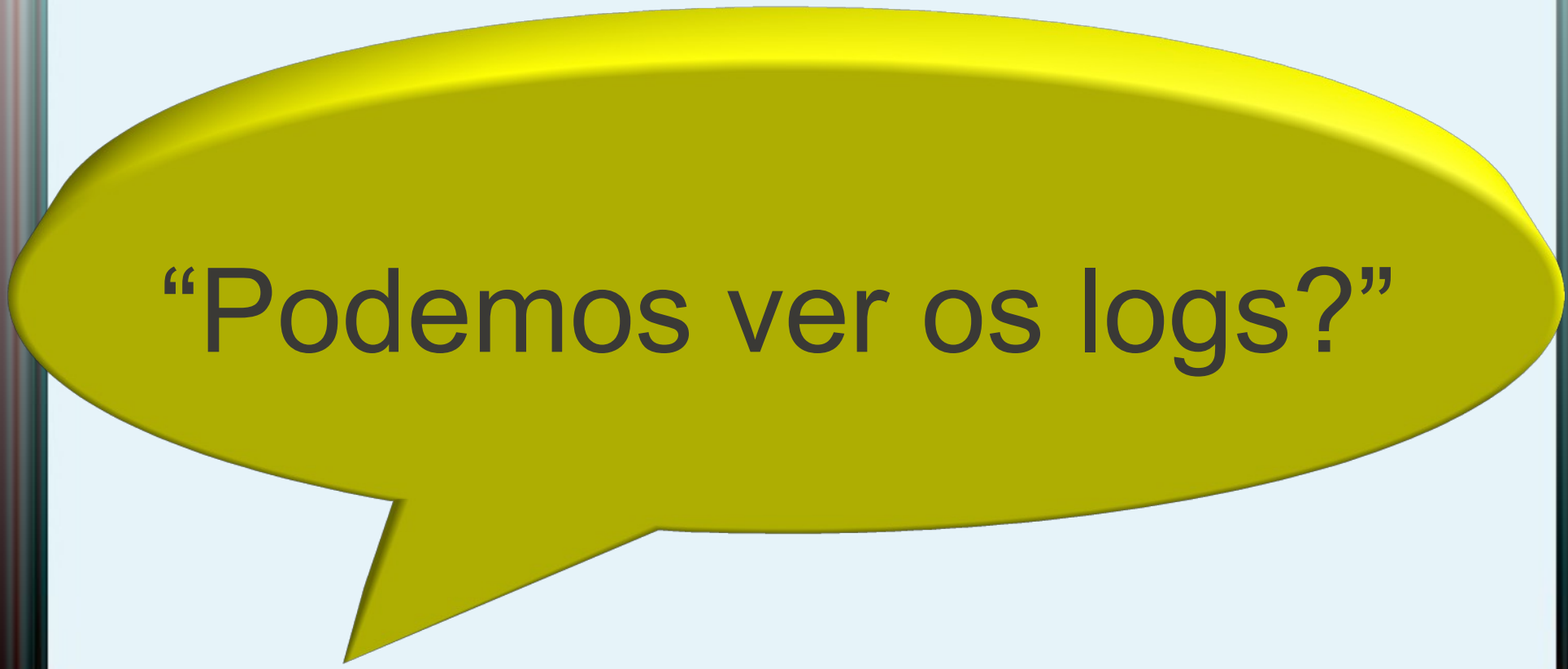
CASO 1

Instituição governamental diz estar sendo vítima de ataques constantes

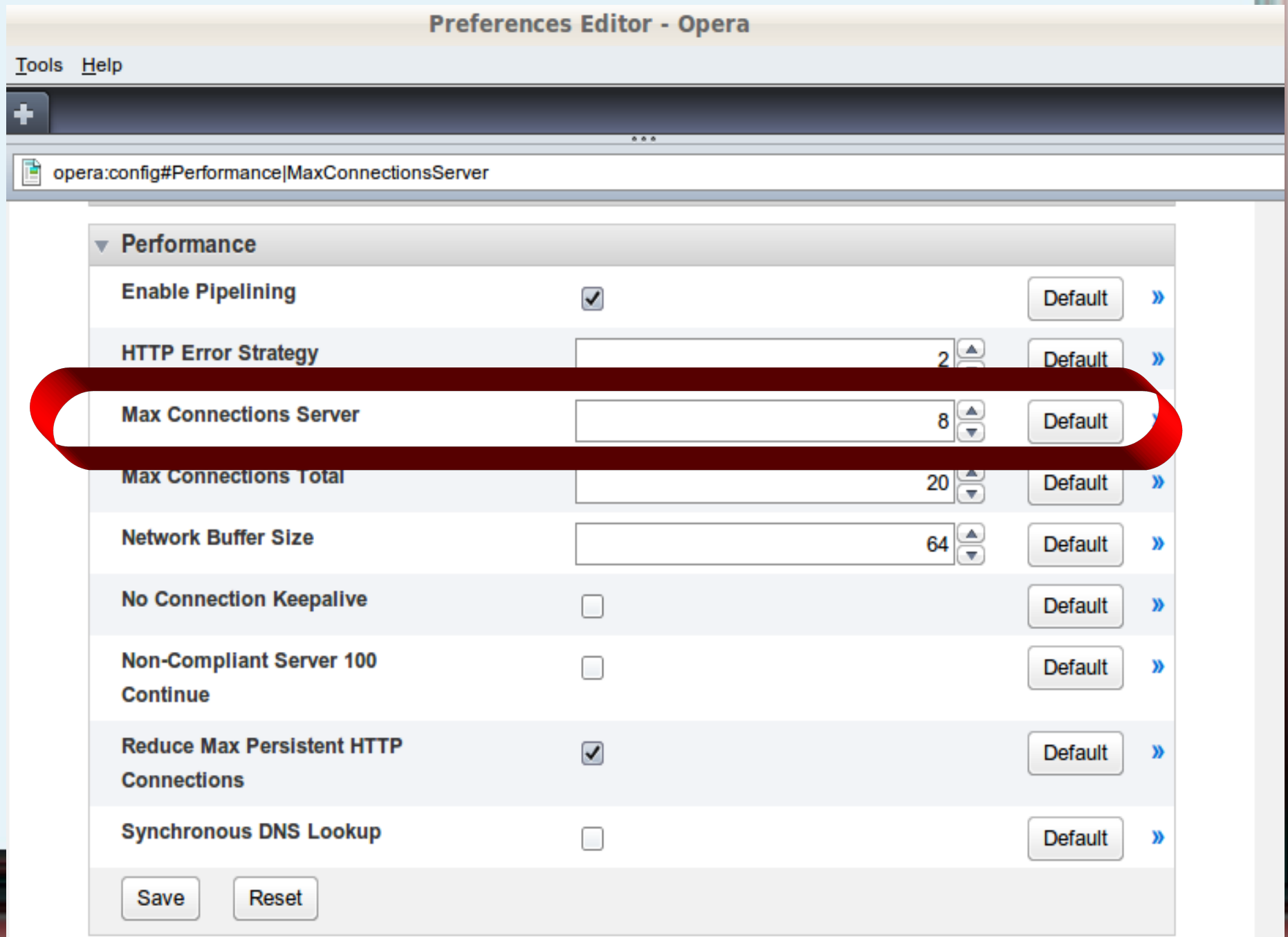
Reunião com provedores de backbone, agencias de governo, entidades representativas da Internet/BR, orgãos policiais e outros

Discussões acaloradas sobre como bloquear ataques de IP spoofing em roteadores ao redor do mundo

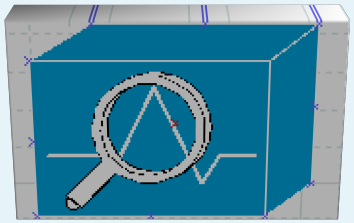
CASO 1



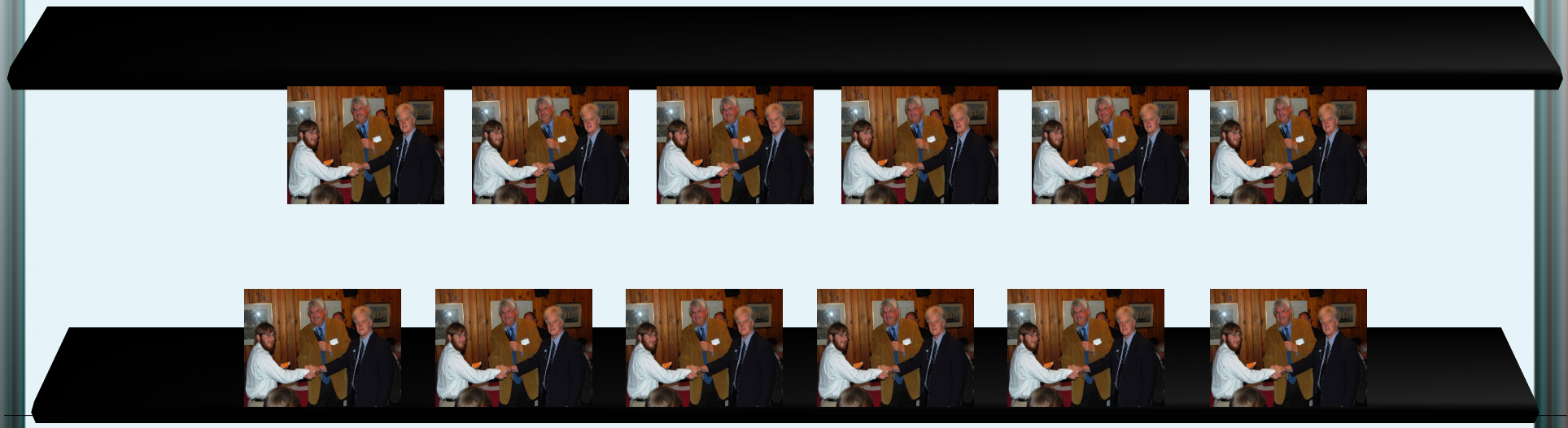
CASO 1

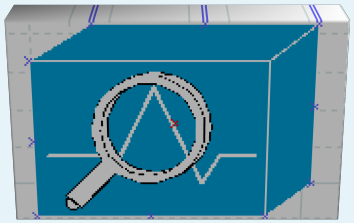

Preferences Editor - Opera
Tools Help
opera:config#Performance|MaxConnectionsServer
Performance
Enable Pipelining
Default
HTTP Error Strategy
2
Default
Max Connections Server
8
Default
Max Connections Total
20
Default
Network Buffer Size
64
Default
No Connection Keepalive
Default
Non-Compliant Server 100 Continue
Default
Reduce Max Persistent HTTP Connections
Default
Synchronous DNS Lookup
Default
Save
Reset

CASO 1



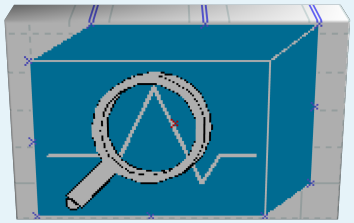
CASO 1



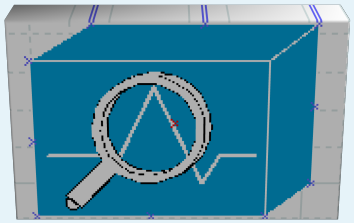


CASO 1

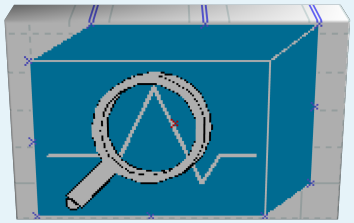
syn



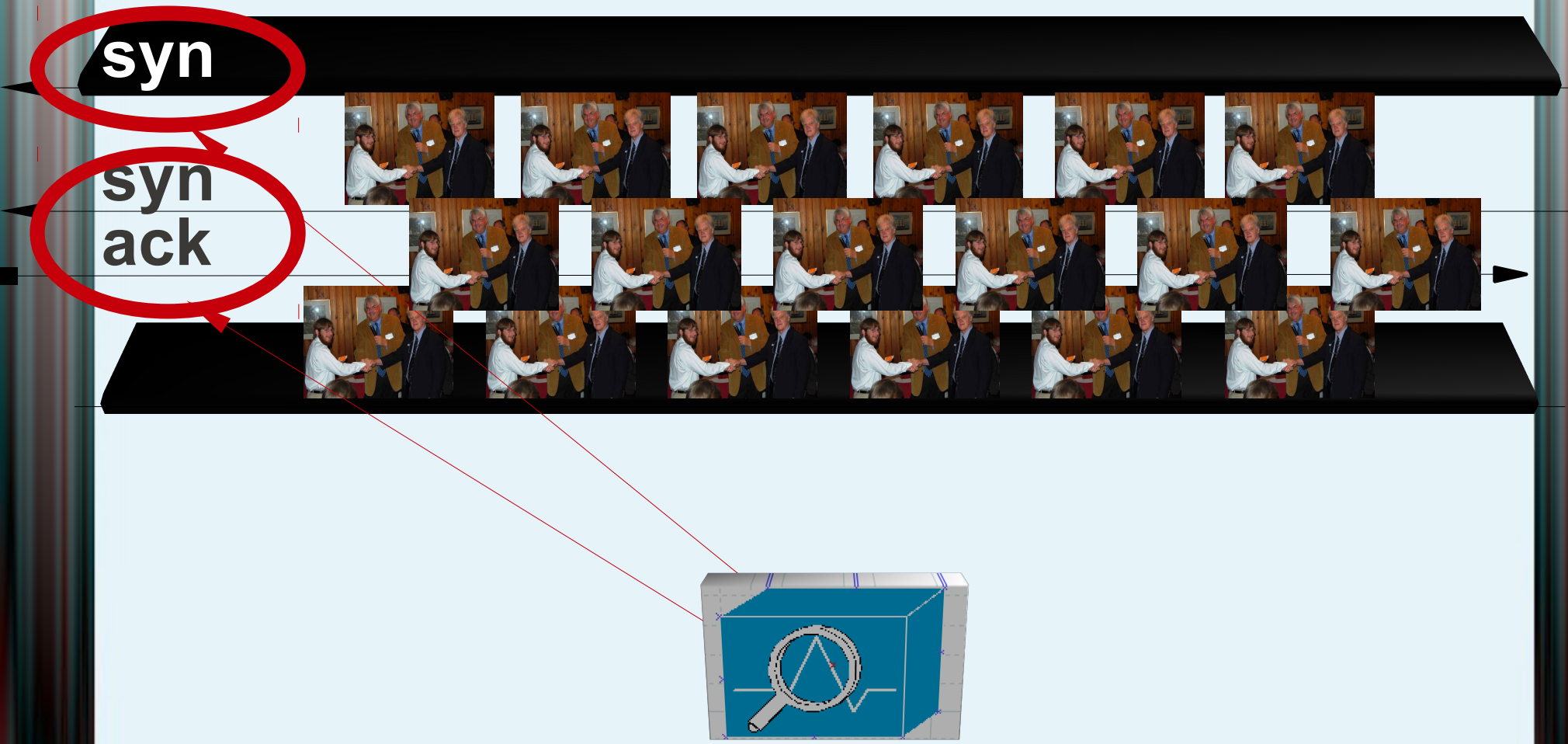
CASO 1



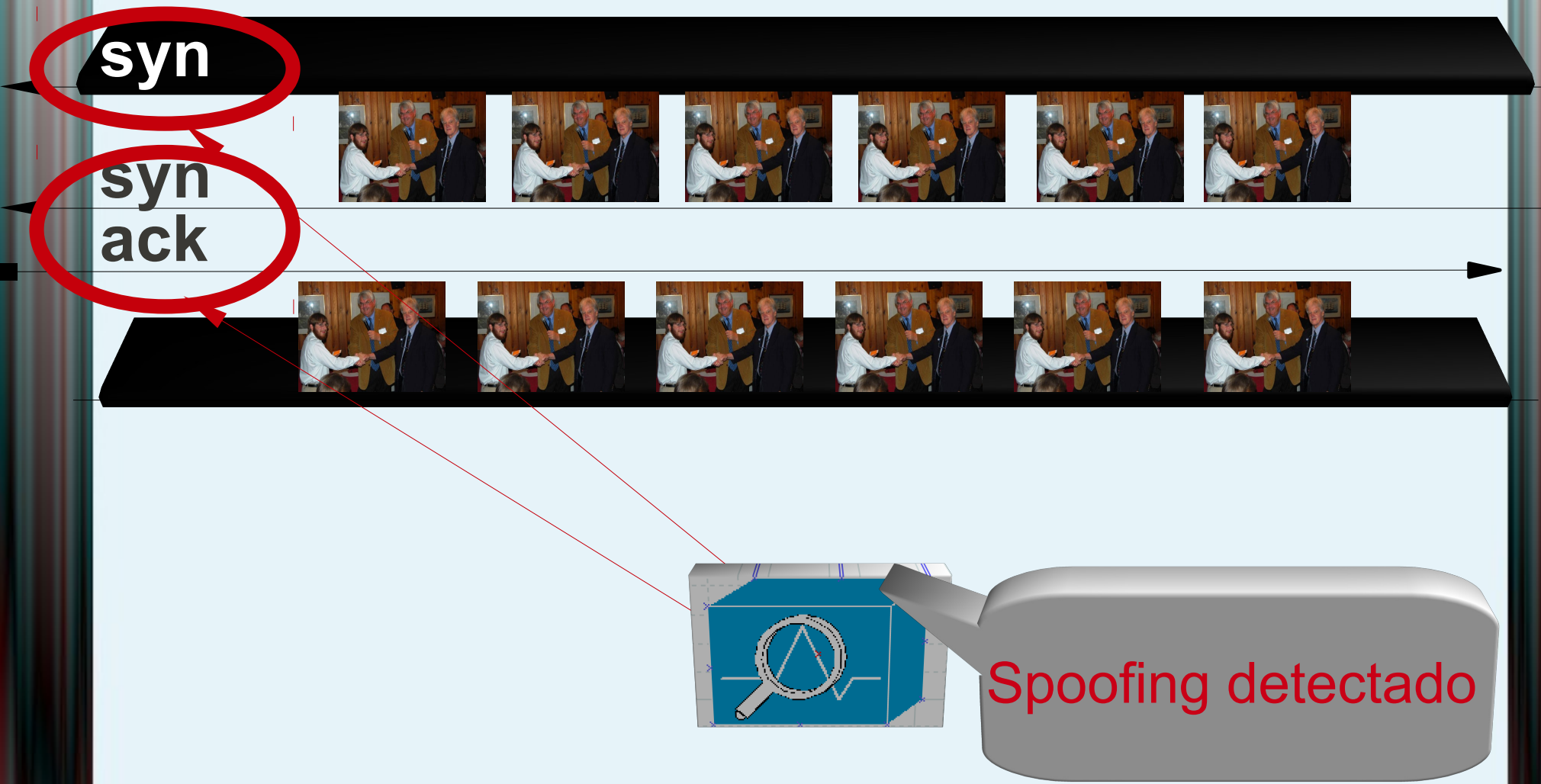
CASO 1



CASO 1



CASO 1



CASO 1

Conclusão:

Um link maior deve ser adquirido

CASO 2

Pacotes nao mentem

CASO 2

Um grande banco nacional estava sendo acusado de atacar uma instituição estrangeira

A vítima apresentou vários logs para comprovar isso

Algumas consultorias tentaram identificar, sem sucesso, o problema

O banco inicia uma auditoria interna para achar o culpado

CASO 2

```
10:20:46.402935 3957us Clear-To-Send RA:00:25:86:f8:c2:56
10:20:46.466936 4667us Clear-To-Send RA:00:25:86:f8:c2:56
10:20:46.471032 Strictly Ordered 0us CF-End RA:ff:ff:ff:ff:ff:ff
10:20:46.569337 4667us Clear-To-Send RA:00:25:86:f8:c2:56
10:20:46.573431 Strictly Ordered 0us CF-End RA:ff:ff:ff:ff:ff:ff
10:20:46.671737 0us STP 802.1w, Rapid STP, Flags [Proposal, Learn, Forward, Agreement], bridge-id 8000.00:1c:c5:16:42:c0.8009, length 36
       message-age 0.00s, max-age 20.00s, hello-time 2.00s, forwarding-delay 15.00s
       root-id 8000.00:1c:c5:16:42:c0, root-pathcost 0, port-role Designated
10:20:46.671736 4667us Clear-To-Send RA:00:25:86:f8:c2:56
10:20:46.675320 Strictly Ordered 0us CF-End RA:ff:ff:ff:ff:ff:ff
10:20:46.703501 0us STP 802.1w, Rapid STP, Flags [Proposal, Learn, Forward, Agreement], bridge-id 8000.00:1c:c5:16:42:c0.800b, length 43
       message-age 0.00s, max-age 20.00s, hello-time 2.00s, forwarding-delay 15.00s
       root-id 8000.00:1c:c5:16:42:c0, root-pathcost 0, port-role Designated
10:20:46.709622 3957us Clear-To-Send RA:00:25:86:f8:c2:56
10:20:46.774137 4667us Clear-To-Send RA:00:25:86:f8:c2:56
10:20:46.778233 Strictly Ordered 0us CF-End RA:ff:ff:ff:ff:ff:ff
10:20:46.876537 4667us Clear-To-Send RA:00:25:86:f8:c2:56
10:20:46.880631 Strictly Ordered 0us CF-End RA:ff:ff:ff:ff:ff:ff
10:20:46.920546 0us STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.00:1e:c1:1c:d0:6a.800c, length 43
       message-age 2.00s, max-age 20.00s, hello-time 2.00s, forwarding-delay 15.00s
       root-id 8000.00:1c:c5:16:42:c0, root-pathcost 200000, port-role Designated
10:20:46.978936 4667us Clear-To-Send RA:00:25:86:f8:c2:56
10:20:46.983032 Strictly Ordered 0us CF-End RA:ff:ff:ff:ff:ff:ff
10:20:47.016886 3957us Clear-To-Send RA:00:25:86:f8:c2:56
10:20:47.081400 4667us Clear-To-Send RA:00:25:86:f8:c2:56
10:20:47.084984 Strictly Ordered 0us CF-End RA:ff:ff:ff:ff:ff:ff
10:20:47.183800 4667us Clear-To-Send RA:00:25:86:f8:c2:56
10:20:47.186873 Strictly Ordered 0us CF-End RA:ff:ff:ff:ff:ff:ff
```

tcpdump em ação!

CASO 2

Vários ACKs saindo do servidor HTTP

A vítima apresentou vários logs para comprovar isso

Algumas consultorias tentaram identificar, sem sucesso, o problema

O banco inicia uma auditoria interna para achar o culpado

CASO 2

Junto com o *tcpdump* foi verificado que:

Haviam Clientes do banco no escritório da “vítima”

Era normal haver acessos legítimos partindo do site da “vitima” em direção ao servidor web do banco

CASO 2

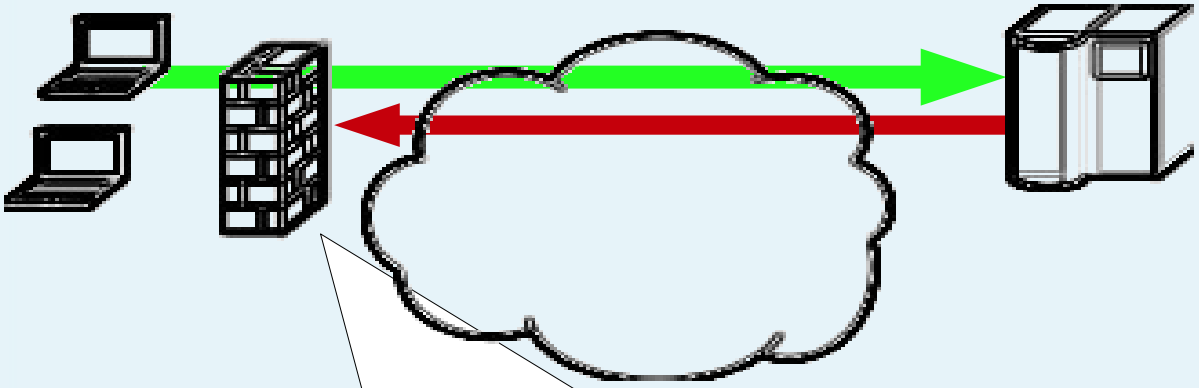
10.1.1.1:1025 to 192.168.1.1:80 – Ok
192.168.1.1:80 to 10.1.1.1:1025 – Ok

CASO 2

A “vitima” possuia um firewall stateful

O produto usado como servidor web pelo banco tinha um bug que fazia cache de algumas conexões

CASO 2



10.1.1.1:1025 to 192.168.1.1:80 – Ok
192.168.1.1:80 to 10.1.1.1:1025 – Ok

~~192.168.1.1:80 to 10.1.1.1:1025 – Ok~~

CASO 2

Fabricante do servidor WEB foi contactado, a correção foi desenvolvida e aplicada

Auditoria interna foi encerrada

CASO 2

Nota: Nenhum funcionário do Banco foi sacrificado ao final deste caso

CASO 2

Caso 3

Mais que log de erros

“Mais que log de erros”

Caso 3

1) Um vírus se propaga rapidamente em uma instituição governamental

2) Empresa de antivírus é contactada para Identificar o malware e desenvolver a vacina

3) Após análise a empresa AV divulga um boletim sobre as características do malware

Caso 3

4) A desinfecção não ocorre como esperado. Várias máquinas são reinfectadas

5) Um grupo é chamado a auxiliar nos trabalhos

6) Uma análise forense e de tráfego revela que se trata de uma botnet

Caso 3

4) A desinfecção não ocorre como esperado. Várias máquinas são reinfectadas

5) Um grupo é chamado a auxiliar nos trabalhos

6) Uma análise forense e de tráfego revela que se trata de uma botnet

Caso 3

Análise da botnet mostra que a vacina é efetiva, mas a política da instituição permitia parar o AV nas estaçoes e o malware estava fazendo isso.

O Malware foi subestimado na análise da empresa de AV e sua característica de Botnet não foi identificada

Caso 3

O firewall logava as conexões permitidas, desta forma foi possível contabilizar a quantidade de estações contaminadas


© Bronek Kaminski / Barcroft Media

Resposta à incidentes

Diagnósticos equivocados e finais felizes

Nelson Murilo
http://twitter.com/nelsonmurilo