

Rede de sensores distribuídos do CAIS

Edilson Lima

5º Fórum brasileiro de CSIRTs

cert.br

Agenda



Apresentação

O Projeto



Principais números



Integração com o sistema SGIS



Encerramento

Apresentação



CAIS

CSIRT de coordenação da rede acadêmica brasileira, a Rede Ipe, desde 1997.

Atua na detecção, resolução e prevenção de incidentes de segurança de rede, além de elaborar, promover e disseminar práticas de segurança na RNP e instituições a ela vinculadas.

Projeto - Contexto

**Rede Ipê, backbone da rede acadêmica.
Capacidade integrada de 345,45 Gb/s.**

**Interliga 1.237 *campi* de Organizações Usuárias
(IFs, IFEs, Unidades de Pesquisa).**

**Ambiente altamente diversificado em redes,
tecnologias e maturidade das equipes de segurança.**

Dificuldades para uma detecção eficiente.

CAMPI INSTITUTOS FEDERAIS

Total: 709



CAMPI INSTITUTOS FEDERAIS DE ENSINO SUPERIOR

Total: 440



UNIDADES DE PESQUISA

Total: 88



Projeto - Objetivo

Criar uma rede se sensores na rede acadêmica.

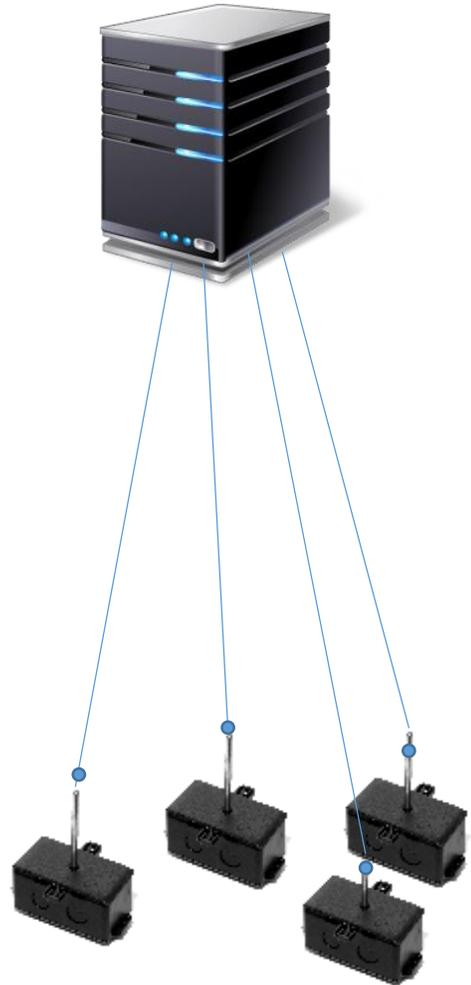


Projeto - O sistema



Projeto - O sistema

Master



Sensor

Sensores Distribuídos CAIS/RNP

HOME INSTITUIÇÕES SENSORES ATUALIZAÇÕES RELATÓRIOS ADMINISTRAÇÃO LOGOUT

Sensores distribuídos - MASTER

Bem vindo ao gerenciador de sensores distribuídos

Tarefas comuns:

- [Cadastrar novo sensor](#)
- [Inserir atualizações de regras](#)
- [Ver relatórios](#)
- [Mapa geral de incidentes](#)

TOP TALKERS

Instituição	Sensor	Qtde
[REDACTED]	200 [REDACTED]	2236075
[REDACTED]	200 [REDACTED]	1402551
[REDACTED]	200 [REDACTED]	1201383
[REDACTED]	200 [REDACTED]	1101994
[REDACTED]	200 [REDACTED]	775189

TOP INCIDENTES

Evento	Qtde	Porcentagem
2101867	8443279	29.0%
2017921	895943	7.55%
2001569	763299	6.43%
2017318	555843	4.68%

Sensor de atividade maliciosa - CAIS/RNP

Por favor, escolha uma opcao:

- 1 **Configurar rede**
- 2 Selecionar interface coletora
- 3 Configurar DNS
- 4 Inserir chave de registro
- 5 Gerenciar o servico IDS
- 6 Gerenciar o crond da ENGINE
- 7 Configurar o NTP da ENGINE
- 8 Checar update
- 9 Diagnostico
- 10 Sobre

< OK > <<Cancel>

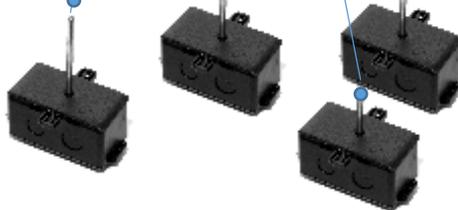
Projeto - O sistema

Master



- Gerenciamento dos sensores e instituições
- Gerenciamento das atualizações
- Estatísticas do sistema geral e dos sensores
- Classificação das atividades maliciosas
- Administração geral do sistema

Sensor

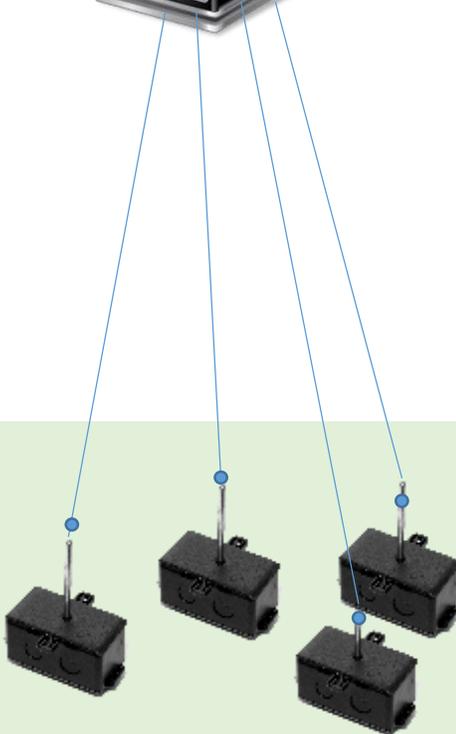


Projeto - O sistema

Master



Sensor



- Interface friendly user
- Plug and play
- Exige pouco conhecimento técnico
- Pouca manutenção e suporte
 - Envio das detecções por e-mail
 - Envio de dados estatísticos e de status
 - Solicitação de atualizações

Projeto - O sistema

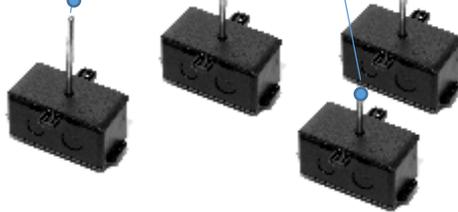
Master



Conexão

- HTTPS
- Autenticação

Sensor

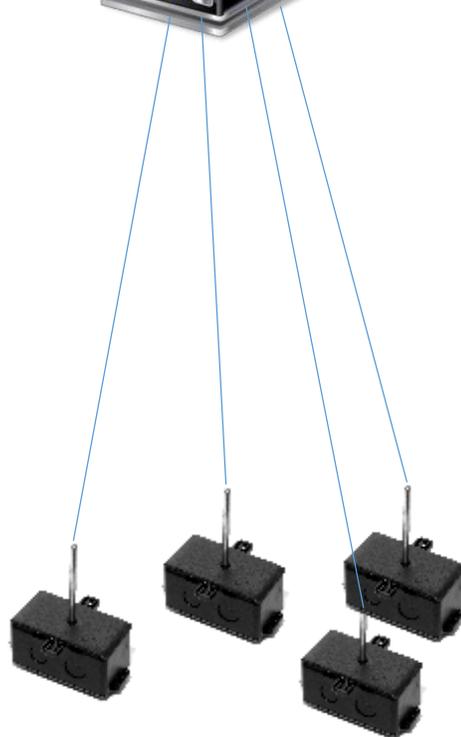


Projeto - O sistema

Master



Sensor



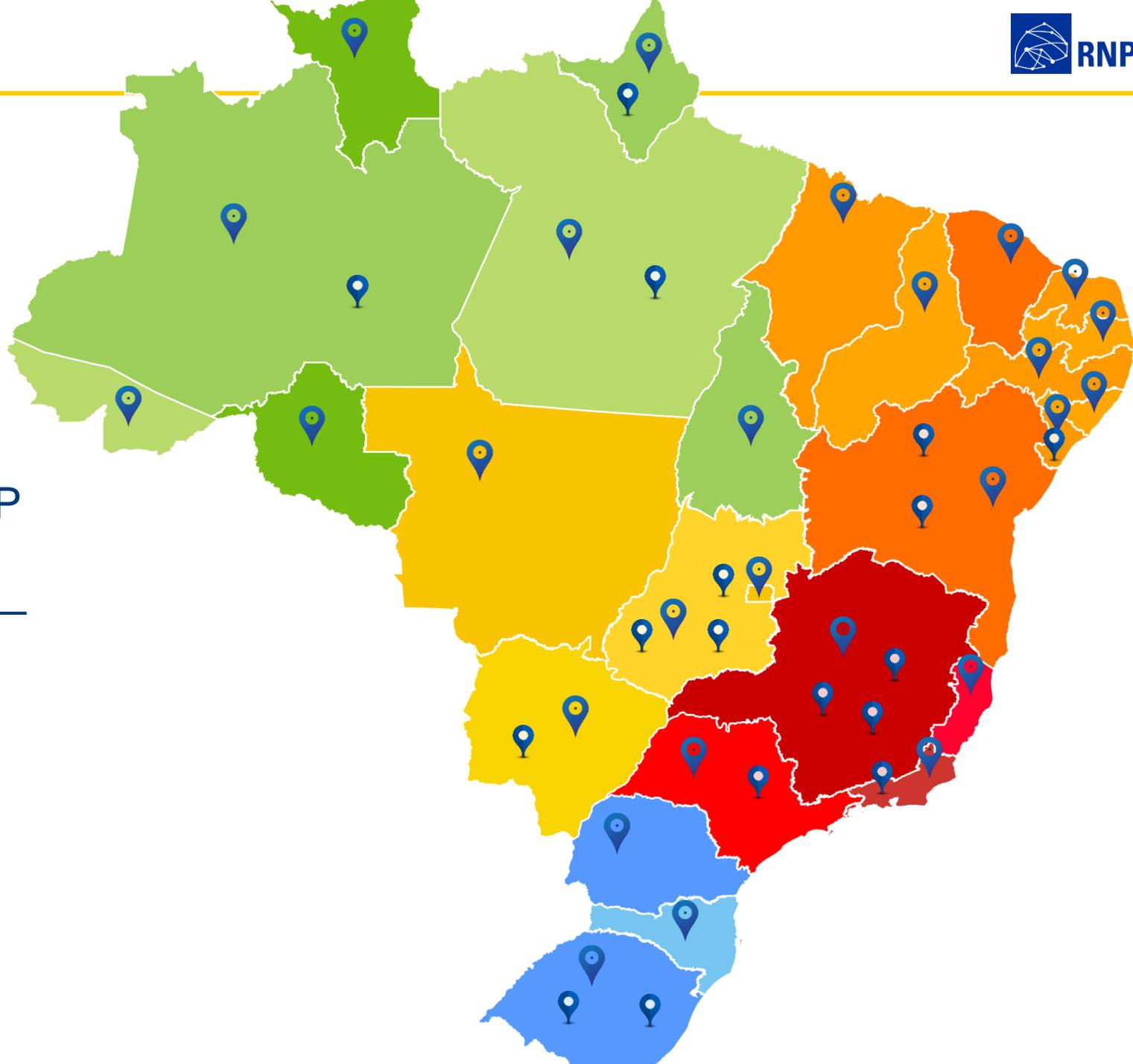
Tipos de atualizações

Tipo	Finalidade
Regras gerais	Prover as regras gerais.
Regras customizadas	Prover regras específicas, sob demanda.
Exceções de regras	Desativar regras, sem a necessidade de gerar nova release.
Blacklist URLs	Identificar acessos a URLs maliciosas
Blacklist de IPs	Identificar acessos a IPs maliciosos, como C&C.
Redes	Cada cliente possui sua própria rede, portanto a HOME_NET de cada um deve ser única, para maior assertividade.
Atualizações de Sistema	Novas versões do sensor, correções e features.

Projeto - Implantação

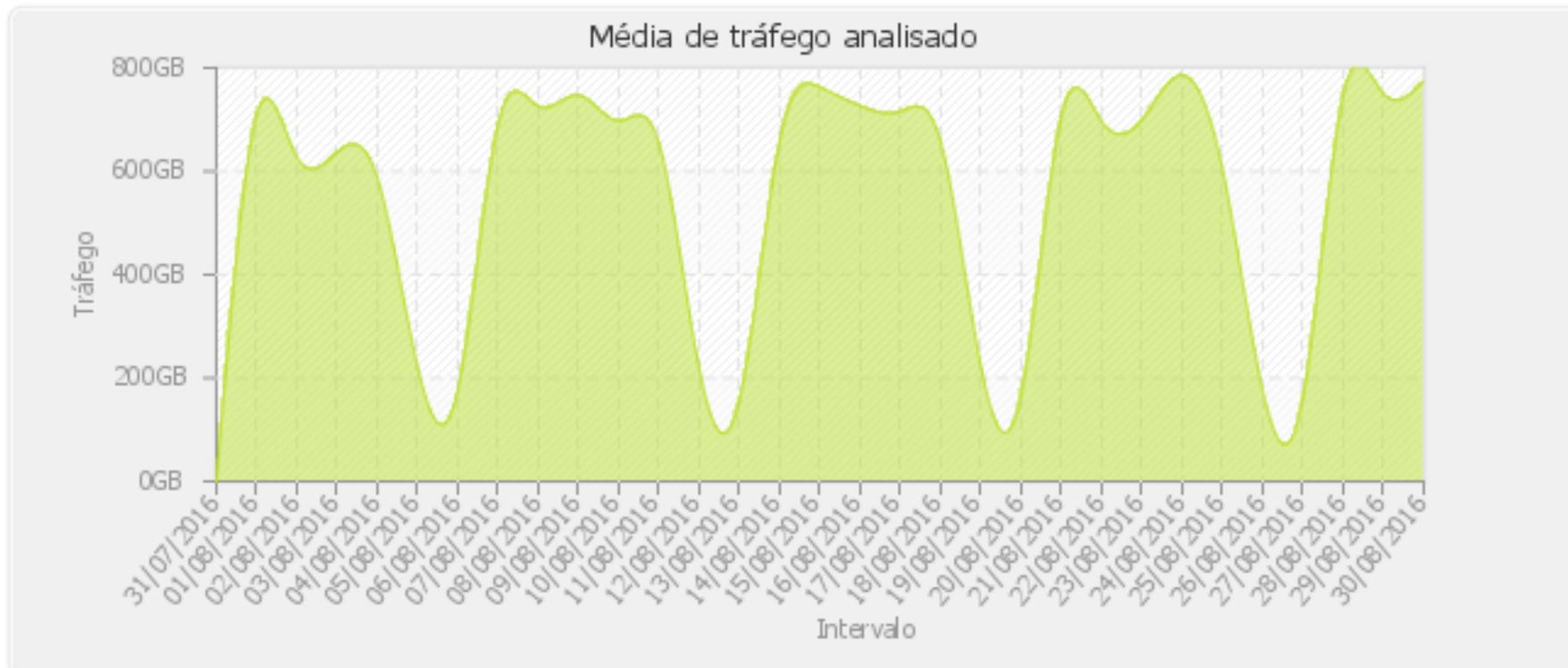
- ✓ 27 Pontos de Presença da RNP
- ✓ 17 Organizações Usuárias

44 Sensores Instalados



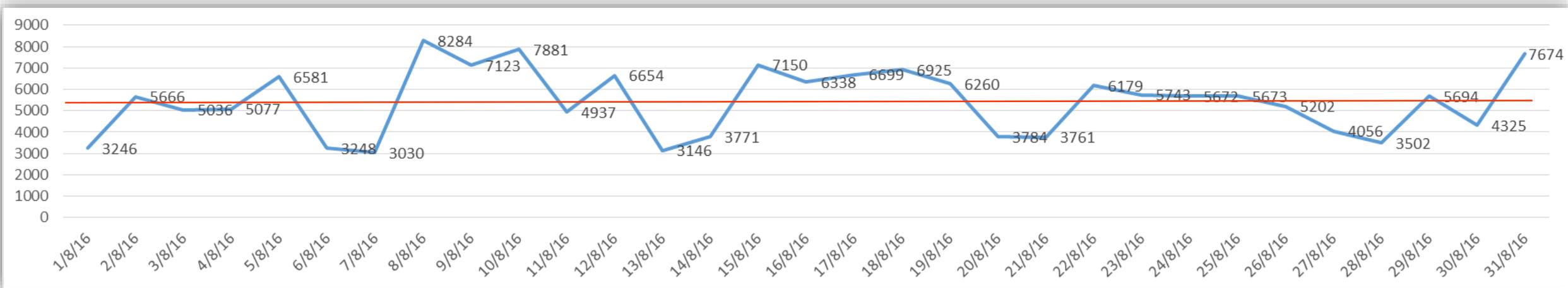
Principais números

Tráfego analisado



Principais números

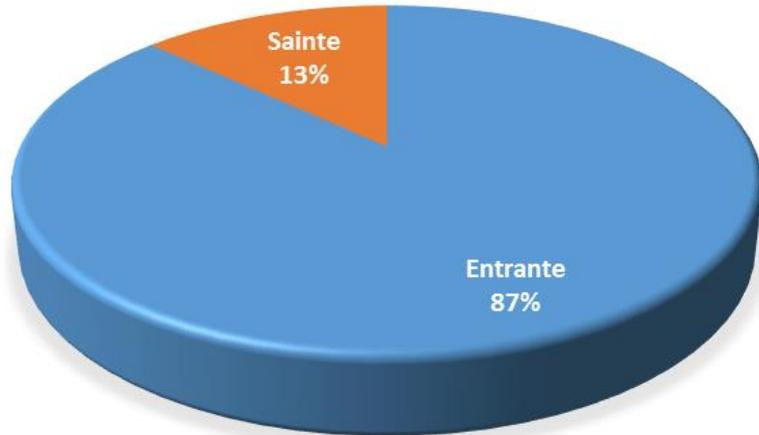
Quantidade de detecções x dia



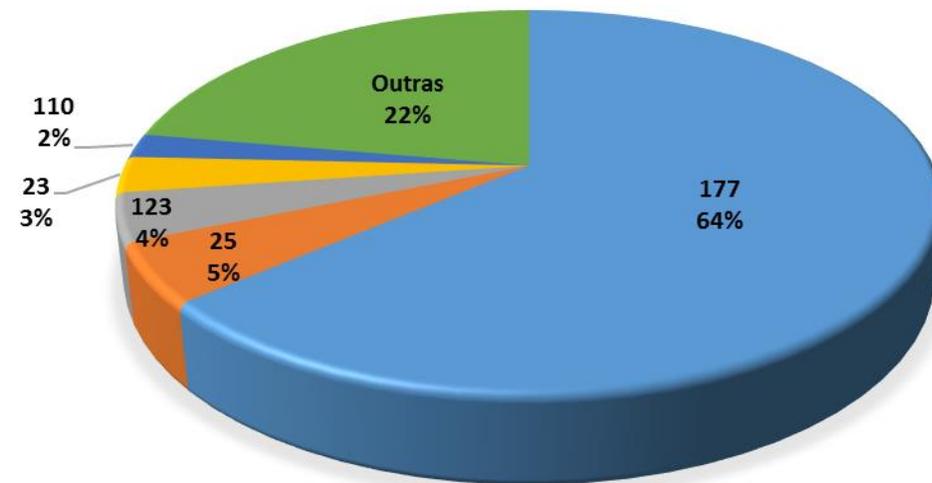
----- Média: 5.430

Principais números

Fluxo da atividade maliciosa



Portas utilizadas



Principais números

Principais atividades maliciosas detectadas

```
[*] Generating module info table, hang on...
- Processing modules
- Done. Let's rock 'n roll.

Module info :
-----
Base      Top      Size      Rebase   SafeSEH  ASLR     NXCompat  OS Dll  Version, Modulename & Path
-----
0x77b20000 0x77b32000 0x00012000 False    True     False    True    5.1.2600.5512 [MSASNI.dll] (C:\WINDOWS\system32\MSASNI.dll)
0x00570000 0x005F0000 0x00080000 True     True     False    False   -1.0- [SDL.dll] (C:\Program Files\AudioCoder\SDL.dll)
0x77c10000 0x77c20000 0x00040000 True     True     False    True    5.00.2900.5512 [CONDL32.dll] (C:\WINDOWS\system32\CONDL32.dll)
0x77c50000 0x77c60000 0x00040000 False   True     False    True    5.1.2600.5512 [NETAPI32.dll] (C:\WINDOWS\system32\NETAPI32.dll)
0x1a400000 0x1a400000 0x00000000 True     True     False    True    5.1.2600.5512 [urlmon.dll] (C:\WINDOWS\system32\urlmon.dll)
0x00000000 0x00000000 0x00000000 True     True     False    True    5.1.2600.5512 [image.dll] (C:\Program Files\AudioCoder\SDL\image.dll)
0x77a00000 0x77b15000 0x00095000 False   True     False    True    5.131.2600.5512 [CRVPT32.dll] (C:\WINDOWS\system32\CRVPT32.dll)
0x02d10000 0x02fd5000 0x002c5000 True     True     False    True    5.1.2600.5512 [xpsp2res.dll] (C:\WINDOWS\system32\xpsp2res.dll)
0x02140000 0x021b0000 0x00090000 True     True     False    True    1.0.0.402 [SysInfo.dll] (C:\Program Files\AudioCoder\SysInfo.dll)
0x77c10000 0x77c80000 0x006e0000 True     True     False    True    5.1.2600.5512 [msvert.dll] (C:\WINDOWS\system32\msvert.dll)
0x00400000 0x005e9000 0x001e9000 False   True     False    False   0.9.22.5506 [AudioCoder.exe] (C:\Program Files\AudioCoder\AudioCoder.exe)
0x77700000 0x77710000 0x00010000 False   True     False    True    5.1.2600.5512 [RPCRT4.dll] (C:\WINDOWS\system32\RPCRT4.dll)
0x00000000 0x00000000 0x00000000 True     True     False    True    -1.0- [libxml2.dll] (C:\Program Files\AudioCoder\libxml2.dll)
0x00000000 0x71100000 0x00000000 True     False   True     True    5.1.2600.5512 [wshcpip.dll] (C:\WINDOWS\system32\wshcpip.dll)
0x00140000 0x00140000 0x00000000 True     False   True     True    8.00.6001.18702 [ieframe.dll] (C:\WINDOWS\system32\ieframe.dll)
0x722b0000 0x722b5000 0x00005000 False   True     False    True    5.1.2600.5512 [sensapi.dll] (C:\WINDOWS\system32\sensapi.dll)
0x76ee0000 0x76fc0000 0x000c0000 False   True     False    True    5.1.2600.5512 [RASAPI32.dll] (C:\WINDOWS\system32\RASAPI32.dll)
0x05dc0000 0x05dc0000 0x00000000 False   True     False    True    8.00.6001.18702 [terutil.dll] (C:\WINDOWS\system32\terutil.dll)
0x76900000 0x76900000 0x00000000 False   True     False    True    5.1.2600.5512 [IMAGEHELP.dll] (C:\WINDOWS\system32\IMAGEHELP.dll)
0x76fc0000 0x76fc0000 0x00000000 False   True     False    True    5.1.2600.5512 [rasadhlp.dll] (C:\WINDOWS\system32\rasadhlp.dll)
0x77700000 0x77710000 0x00010000 False   True     False    True    5.1.2600.5512 [Secur32.dll] (C:\WINDOWS\system32\Secur32.dll)
0x76900000 0x76900000 0x00000000 False   True     False    True    5.1.2600.5512 [MSOCK32.dll] (C:\WINDOWS\system32\MSOCK32.dll)
0x76900000 0x76900000 0x00000000 False   True     False    True    8.00.2900.5512 [shdocvw.dll] (C:\WINDOWS\system32\shdocvw.dll)
0x71100000 0x71100000 0x00000000 True     False   True     True    5.1.2600.5512 [MS2HELP.dll] (C:\WINDOWS\system32\MS2HELP.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [ole32.dll] (C:\WINDOWS\system32\ole32.dll)
0x662b0000 0x663ad000 0x00090000 False   True     False    True    5.1.2600.5512 [IM32.DLL] (C:\WINDOWS\system32\IM32.DLL)
0x7e410000 0x7e410000 0x00001000 False   True     False    True    5.1.2600.5512 [hnetcfg.dll] (C:\WINDOWS\system32\hnetcfg.dll)
0x754d0000 0x75550000 0x00080000 False   True     False    True    5.1.2600.5512 [USER32.dll] (C:\WINDOWS\system32\USER32.dll)
0x76900000 0x76900000 0x00000000 False   True     False    True    1.13 [libiconv-2.dll] (C:\Program Files\AudioCoder\libiconv-2.dll)
0x76900000 0x76900000 0x00000000 False   True     False    True    5.131.2600.5512 [CRYPTUI.dll] (C:\WINDOWS\system32\CRYPTUI.dll)
0x76900000 0x76900000 0x00000000 False   True     False    True    5.1.2600.5512 [rtutils.dll] (C:\WINDOWS\system32\rtutils.dll)
0x76900000 0x76900000 0x00000000 False   True     False    True    5.1.2600.5512 [IPHLPAPI.DLL] (C:\WINDOWS\system32\IPHLPAPI.DLL)
0x77700000 0x77700000 0x00000000 False   True     False    True    2001.12.4414.700 [CLBTRUST.dll] (C:\WINDOWS\system32\CLBTRUST.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    2001.12.4414.700 [COMRes.dll] (C:\WINDOWS\system32\COMRes.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [OLEAUT32.dll] (C:\WINDOWS\system32\OLEAUT32.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [rasman.dll] (C:\WINDOWS\system32\rasman.dll)
0x7c9c0000 0x7c9c0000 0x00000000 False   True     False    True    8.00.2900.5512 [SHELL32.dll] (C:\WINDOWS\system32\SHELL32.dll)
0x019e0000 0x01a45000 0x00065000 True     True     False    False   -1.0- [nres.dll] (C:\Program Files\AudioCoder\nres.dll)
0x76900000 0x76900000 0x00000000 False   True     False    True    5.1.2600.5512 [DNSAPI.dll] (C:\WINDOWS\system32\DNSAPI.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    2001.12.4414.700 [CLBQATO.DLL] (C:\WINDOWS\system32\CLBQATO.DLL)
0x77700000 0x77700000 0x00000000 False   True     False    True    2001.12.4414.700 [COMCTL32.dll] (C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6095b641-8ccf-48c4-b8a2-000084519548\6095b641-8ccf-48c4-b8a2-000084519548\252\comctl32.dll)
0x01100000 0x01100000 0x00000000 True     True     False    True    5.1.2600.5512 [SHLWAPI.dll] (C:\WINDOWS\system32\SHLWAPI.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [ATL7IL32.dll] (C:\WINDOWS\system32\ATL7IL32.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [INETAPI.dll] (C:\WINDOWS\system32\INETAPI.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [MSCTF.dll] (C:\WINDOWS\system32\MSCTF.dll)
0x01ac0000 0x01ac0000 0x00000000 True     False   False   False   -1.0- [dsp_zsc.dll] (C:\Program Files\AudioCoder\plugins\dsp_zsc.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [CONCTL32.dll] (C:\WINDOWS\system32\CONCTL32.dll)
0x769c0000 0x76ca7000 0x00040000 False   True     False    True    5.1.2600.5512 [USERENV.dll] (C:\WINDOWS\system32\USERENV.dll)
0x769c0000 0x769c0000 0x00000000 False   True     False    True    5.1.2600.5512 [MINIHAL.dll] (C:\WINDOWS\system32\MINIHAL.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [Keynote132.dll] (C:\WINDOWS\system32\Keynote132.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [GDI32.dll] (C:\WINDOWS\system32\GDI32.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    -1.0- [ncommon.dll] (C:\Program Files\AudioCoder\ncommon.dll)
0x01100000 0x01100000 0x00000000 True     True     False    True    6.00.2900.5512 [xtheme.dll] (C:\WINDOWS\system32\xtheme.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    -1.0- [jres.dll] (C:\Program Files\AudioCoder\jres.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [MLDAP32.dll] (C:\WINDOWS\system32\MLDAP32.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [msvl_0.dll] (C:\WINDOWS\system32\msvl_0.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [VERSION.dll] (C:\WINDOWS\system32\VERSION.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [ADUAP132.dll] (C:\WINDOWS\system32\ADUAP132.dll)
0x769c0000 0x769c0000 0x00000000 False   True     False    True    5.1.2600.5512 [PSAPI.DLL] (C:\WINDOWS\system32\PSAPI.DLL)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [MS2_32.dll] (C:\WINDOWS\system32\MS2_32.dll)
0x77700000 0x77700000 0x00000000 False   True     False    True    5.1.2600.5512 [Normaliz.dll] (C:\WINDOWS\system32\Normaliz.dll)
0x00000000 0x00000000 0x00000000 True     True     False    True    6.0.5441.0 [Normaliz.dll] (C:\WINDOWS\system32\Normaliz.dll)
0x76eb0000 0x76edf000 0x0002f000 False   True     False    True    5.1.2600.5512 [TAPI32.dll] (C:\WINDOWS\system32\TAPI32.dll)

[*] This nona.py action took 0:00:00.500000
```

Intentativa de DDoS (xdmcp)

Shellshock

Brute force

Malware

Transferência de zona (DNS)

Ataque a serviço IMAP

Poodle

Integração com o SGIS



Encerramento



Encerramento

Muito obrigado,

Edilson Lima
edilson.lima@rnp.br