Ferramenta para Gerência de Segurança Usando Análise de Tráfego em Backbones IP

Cláudia de Abreu Silva [1,2]
claudia@dtm.mar.mil.br

Luís Felipe Magalhães de Moraes [1]
moraes@ravel.ufrj.br

[1] Universidade Federal do Rio de Janeiro (UFRJ)

[2] Marinha do Brasil

8a. Reunião do Grupo de Trabalho em Segurança de Redes (GTS-8)
09 de dezembro de 2006 – São Paulo

Roteiro

- **Introdução;**
- Trabalhos Relacionados;
- Metodologia utilizada;
- A Ferramenta para Gerência de Segurança Usando Análise de Tráfego em Backbones IP ;
- Aplicação da Ferramenta em um Cenário Real;
- Resultados Obtidos;
- Conclusões e Trabalhos Futuros.

Introdução

- Aumento da velocidade e dos recursos computacionais das redes ⇨ aumento da exposição das vulnerabilidades de seus aplicativos.
- Pragas digitais (worms) propagam-se através das redes de dados, explorando sistemas vulneráveis. São auto-replicáveis.
- Registros de ações negadas.
- Necessidade de acesso irrestrito para ambientes abertos (Rede acadêmica e de pesquisa ou Backbone IP).

Introdução

- Aplicativos de monitoramento de tráfego geram grande volume de dados, geralmente, sob a forma de relatórios.
- Ferramentas tradicionais de captura de tráfego não conseguem manipular satisfatoriamente grandes quantidades de informações.
- Ferramentas de monitoramento baseadas em fluxos - comumente utilizadas como analizadores de tráfego (gerência de desempenho das redes).
- Para a identificação da origem da anormalidade na rede, é necessária a execução de diversos procedimentos, geralmente, manuais.

Introdução - Problemas

- Ausência de ferramenta específica para capturar, classificar e filtrar padrões de atividades maliciosas em redes livres de restrições e de alto tráfego;
- Número elevado de informações textuais para análise;
- Realização de procedimentos manuais para a identificação do(s) elemento(s) gerador(es) do tráfego anômalo;
- Desconhecimento do estado atual da segurança da rede;
- Ausência de histórico dos eventos anômalos encontrados.

Introdução - Objetivos

- Fornecer, em tempo real, subsídios necessários para a reação em casos de atividades maliciosas provenientes de propagação de *worms*, em ambientes livres de restrições de acesso e em grandes volumes de dados trafegados;
- Automatizar os procedimentos utilizados para a identificação do(s) elemento(s) gerador(es) do tráfego anômalo;
- Apresentar visualmente o resultado das análises do tráfego classificado;
- Prover um histórico das anormalidades identificadas;
- Não interferir no tráfego benigno.

Roteiro

- Introdução;
- **Trabalhos Relacionados;**
- Metodologia utilizada;
- A Ferramenta para Gerência de Segurança Usando Análise de Tráfego em Backbones IP ;
- Aplicação da Ferramenta em um Cenário Real;
- Resultados Obtidos;
- Conclusões e Trabalhos Futuros.

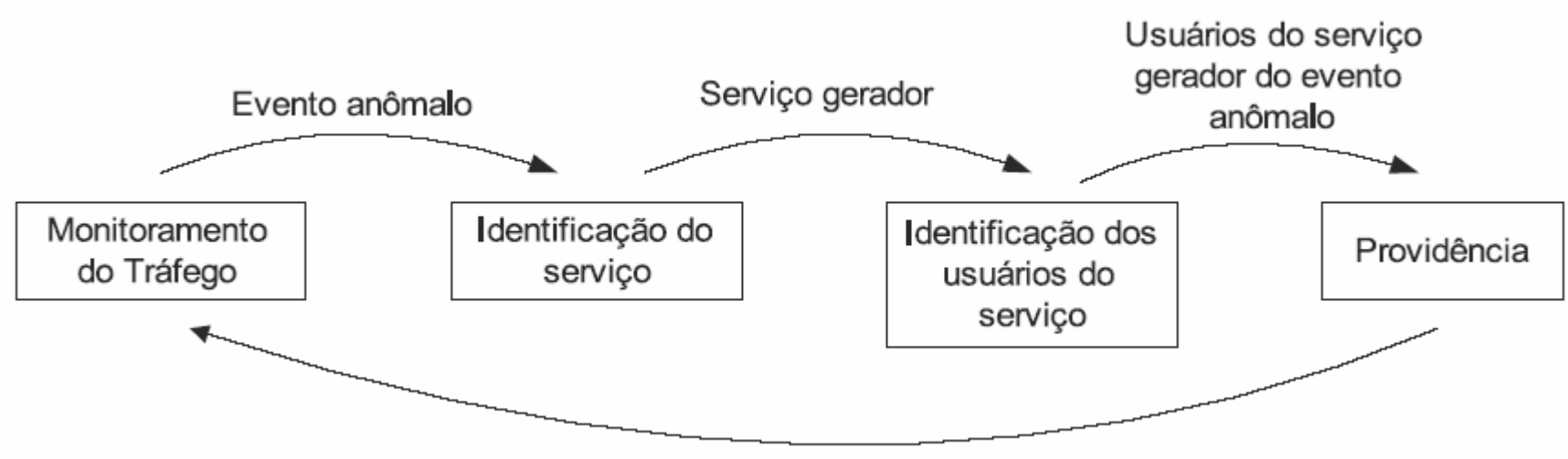
Trabalhos Relacionados

Fatores comumente adotados na identificação de eventos anômalos:

- Ø Alteração de volume de tráfego;
- Ø Elevação do número de sessões estabelecidas;
- Ø Conteúdo da área de dados dos pacotes;
- Ø Periodicidade de ocorrências de fluxos.

Trabalhos Relacionados

- **Metodologias tradicionais:**



Trabalhos Relacionados

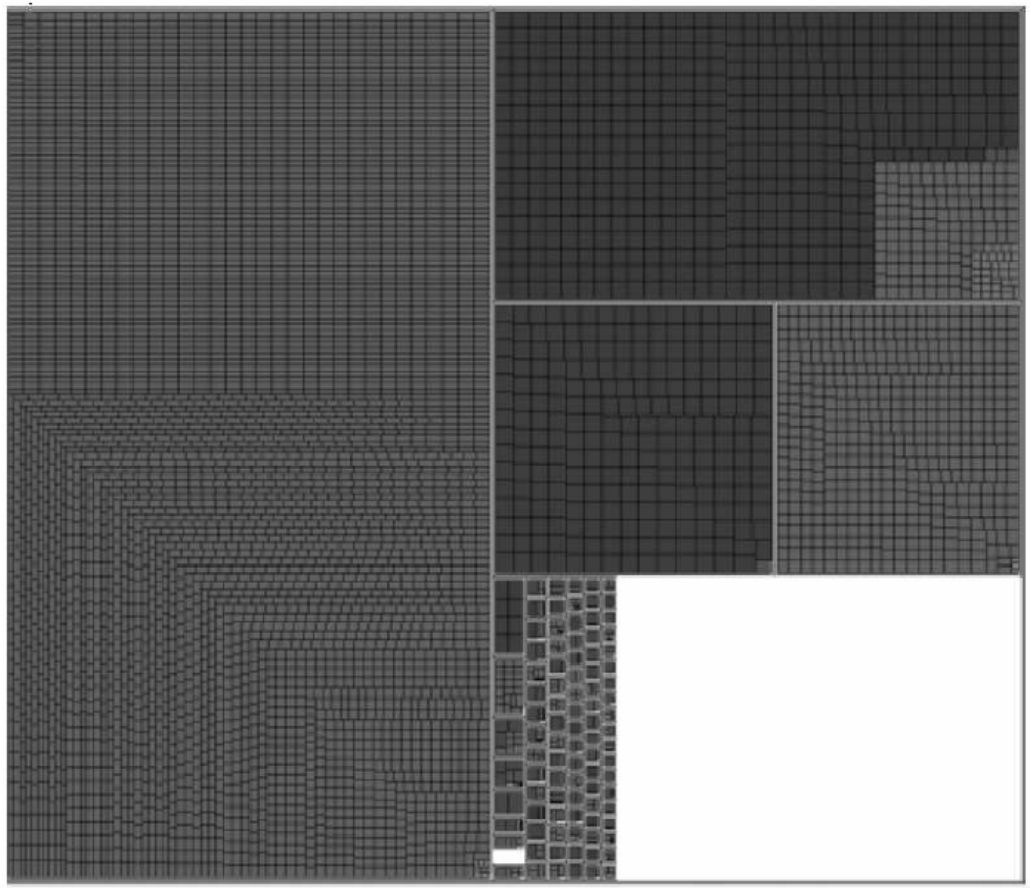
- **Visualização de eventos anômalos em rede.**

Vantagens:

- Identificação instantânea do estado da rede monitorada;
- Dispensa o conhecimento de um especialista para seu reconhecimento;
- Resume um número elevado de informações textuais em uma informação visual.

Trabalhos Relacionados

- Visualização de eventos anômalos em rede:

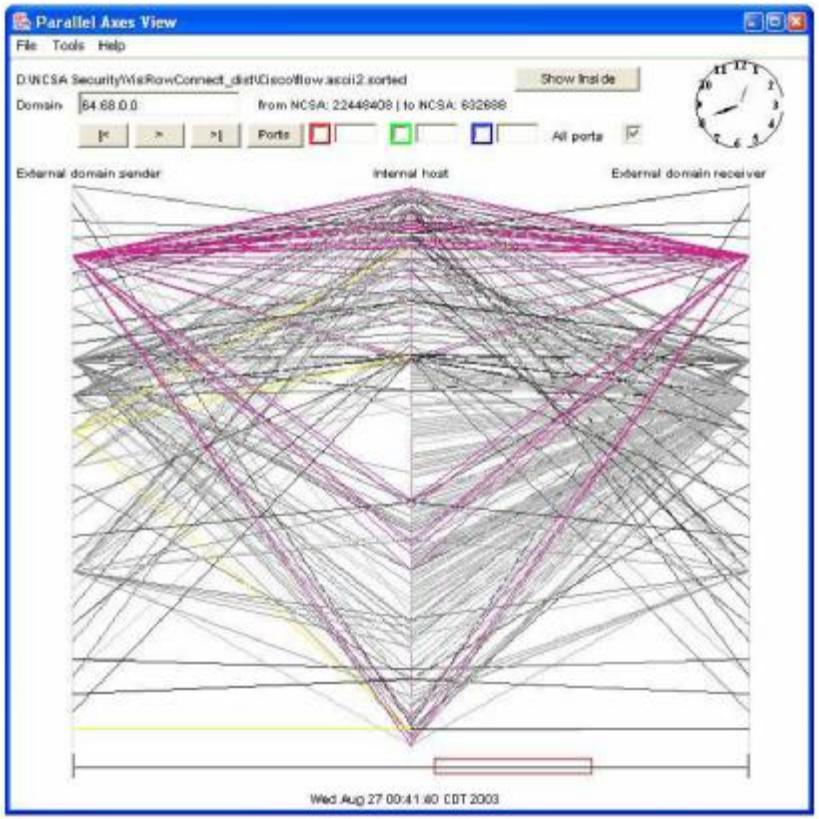


Visualização dos fluxos com porta de destino 25 [4].

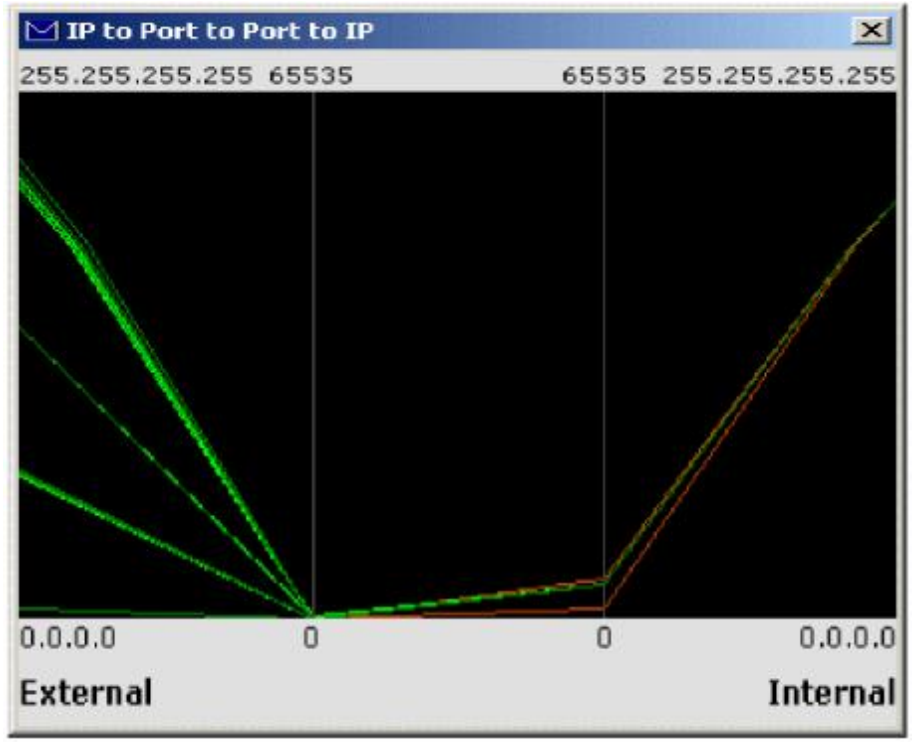
[4] SAMPAIO, L. e outros. Um ambiente de gerenciamento de medições por fluxo de tráfego baseado na utilização de mapas em Árvore. II WPerformance, Campinas, Brasil, p. 115-128, 2003.

Trabalhos Relacionados

- **Visualização de eventos anômalos em rede:**



VisFlowConnect e sua visão de tráfego suspeito [5].



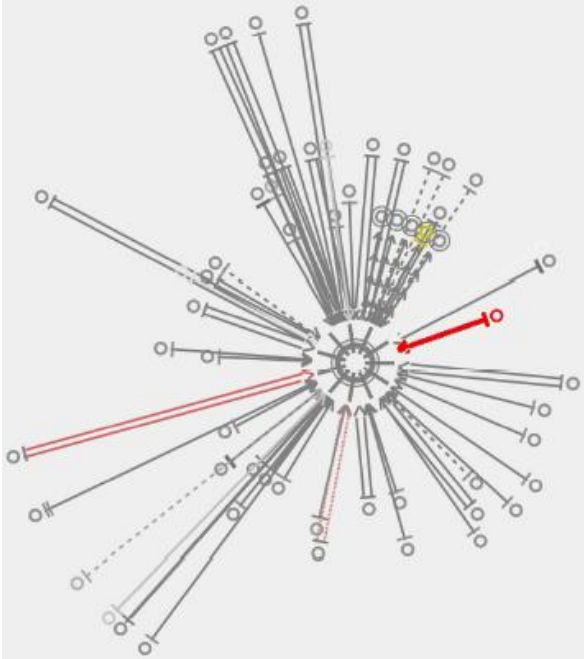
Impressão digital visual passiva [6].

[5] YIN, X. et al. Visflowconnect: netflow visualizations of link relationships for security situational awareness. In: VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security .Washington DC, USA: ACM Press, 2004. p. 2634. ISBN 1-58113-974-8.

[6] CONTI, G.; ABDULLAH, K. Passive visual fingerprinting of network attack tools. In: VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. New York, NY, USA: ACM Press, 2004. p. 4554. ISBN 1-58113-974-8.

Trabalhos Relacionados

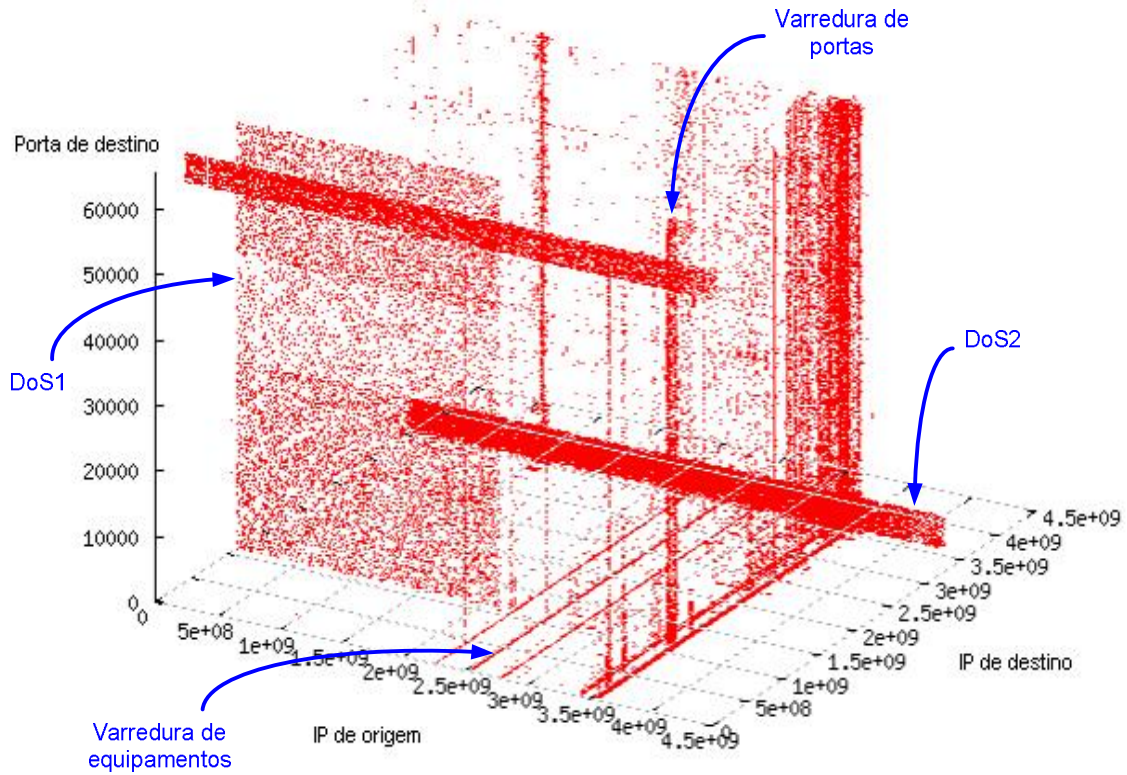
- **Visualização de eventos anômalos em rede:**



[7] ERBACHER, R. F. Glyph-based generic network visualization. In: Proceedings of the SPIE '2002 Conference on Visualization and Data Analysis. [s.n.], 2002.

Trabalhos Relacionados

- **Visualização de eventos anômalos em rede:**



[2] KIM, I. K. H.; BAHK, S. Real-time visualization of network attacks on highspeed links. IEEE Network, v. 18, p. 3019, 2004.

Sumário

- Introdução;
- Trabalhos Relacionados;
- **Metodologia utilizada;**
- A Ferramenta para Gerência de Segurança Usando Análise de Tráfego em Backbones IP ;
- Aplicação da Ferramenta em um Cenário Real;
- Resultados Obtidos;
- Conclusões e Trabalhos Futuros.

Metodologia Utilizada

Diferenciais:

Análise das informações sumarizadas contidas no cabeçalho do fluxo analisado.

- Tipo de protocolo
- Endereço IP de origem
- Endereço IP de destino
- Porta de origem
- Porta de destino
- Sinalizadores (TCP)

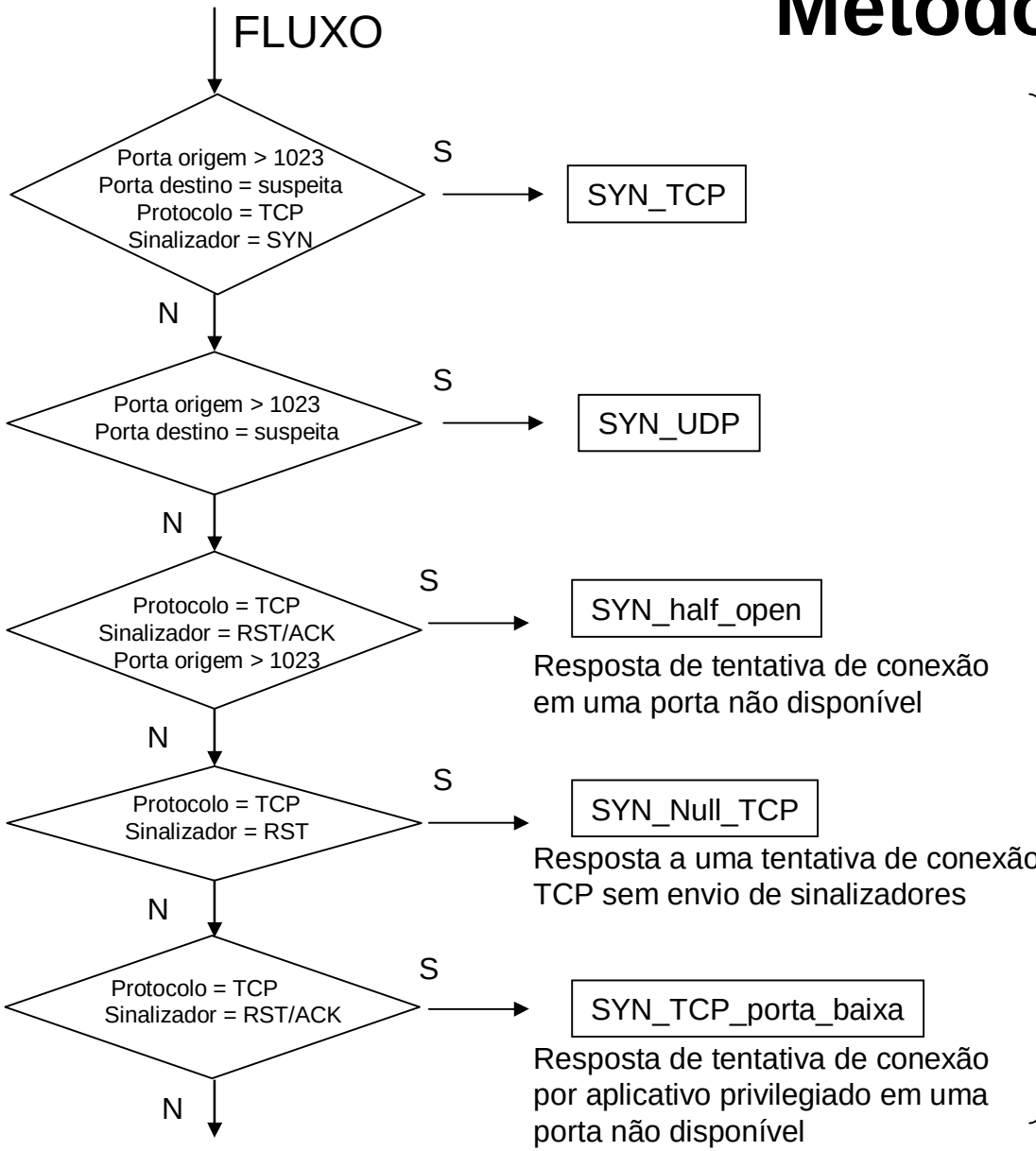
Apresentação gráfica do resultado

Contabilização

Registro das ocorrências anômalas.

Atualização automática da base de dados de referência.

Metodologia Utilizada



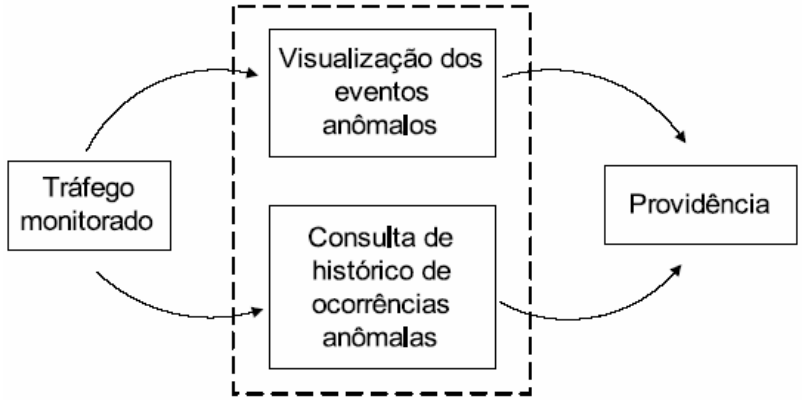
Apresentar graficamente

Contabilizar

Registrar no histórico

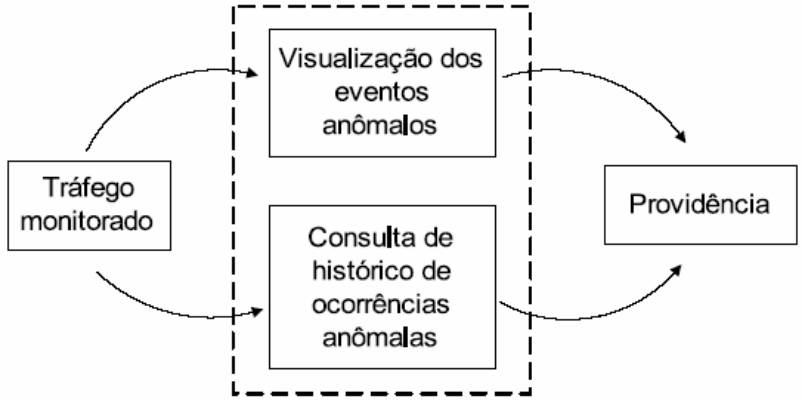
Metodologia Utilizada

Análise dos cabeçalhos dos fluxos.



Metodologia Utilizada

Análise dos cabeçalhos dos fluxos.

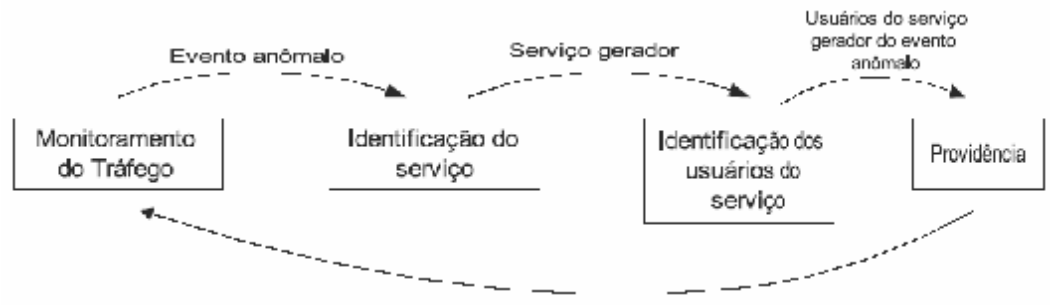


Alteração de volume de tráfego;

Elevação do número de sessões estabelecidas;

Conteúdo da área de dados dos pacotes;

Periodicidade de ocorrências de fluxos.

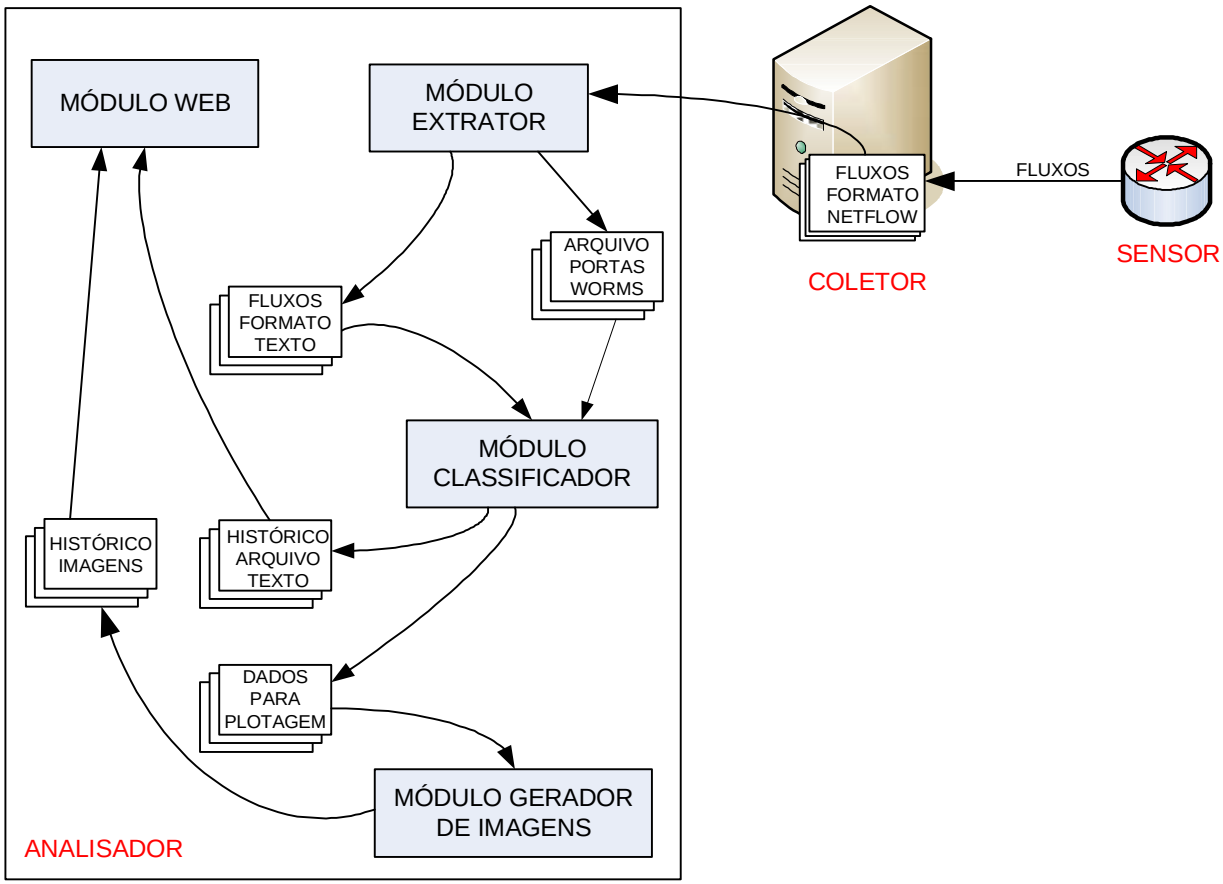


Roteiro

- Introdução;
- Trabalhos Relacionados;
- Metodologia utilizada;
- **A Ferramenta para Gerência de Segurança Usando Análise de Tráfego em Backbones IP** ;
- Aplicação da Ferramenta em um Cenário Real;
- Resultados Obtidos;
- Conclusões e Trabalhos Futuros.

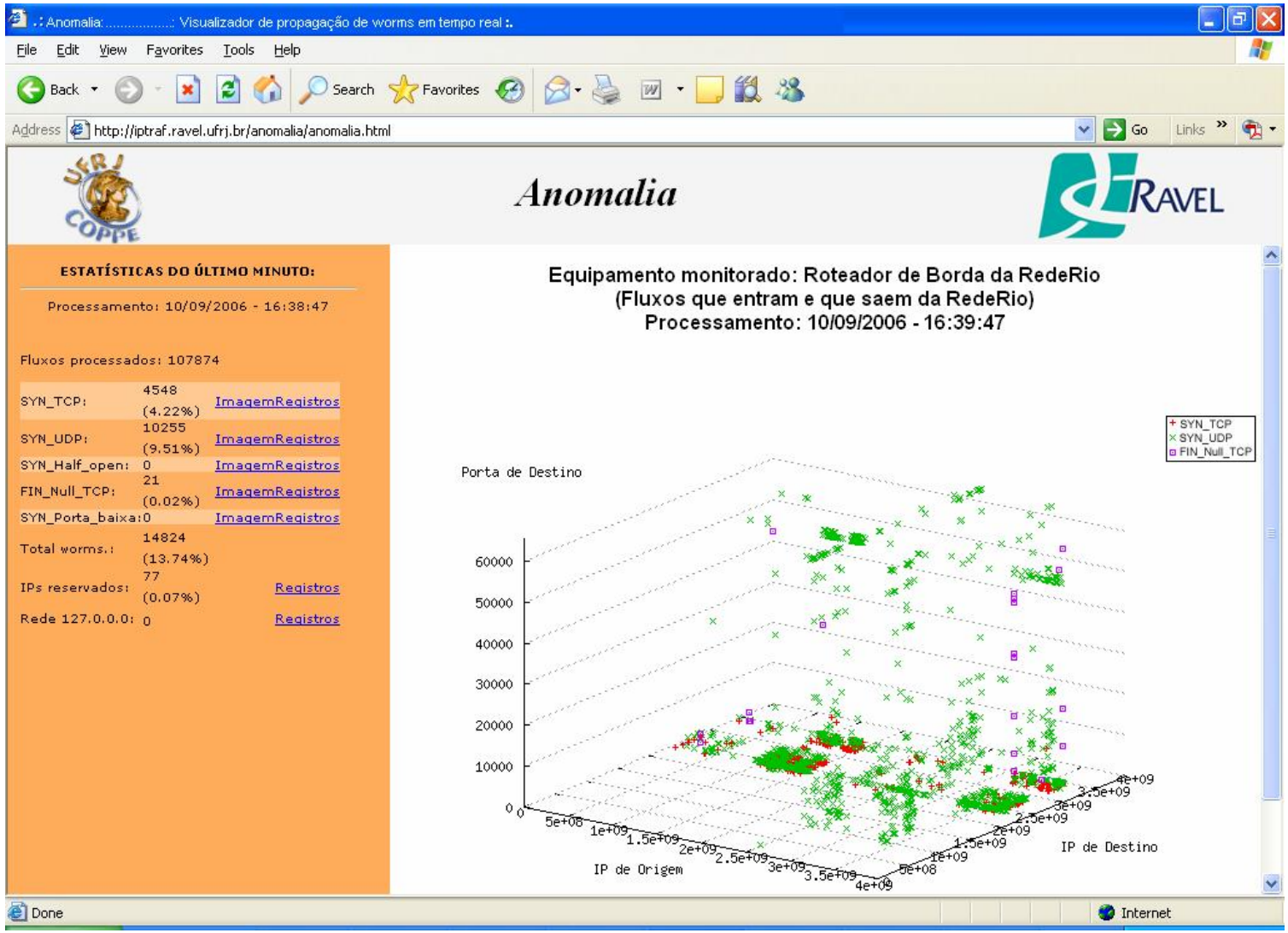
Ferramenta Proposta

Componentes do Sistema



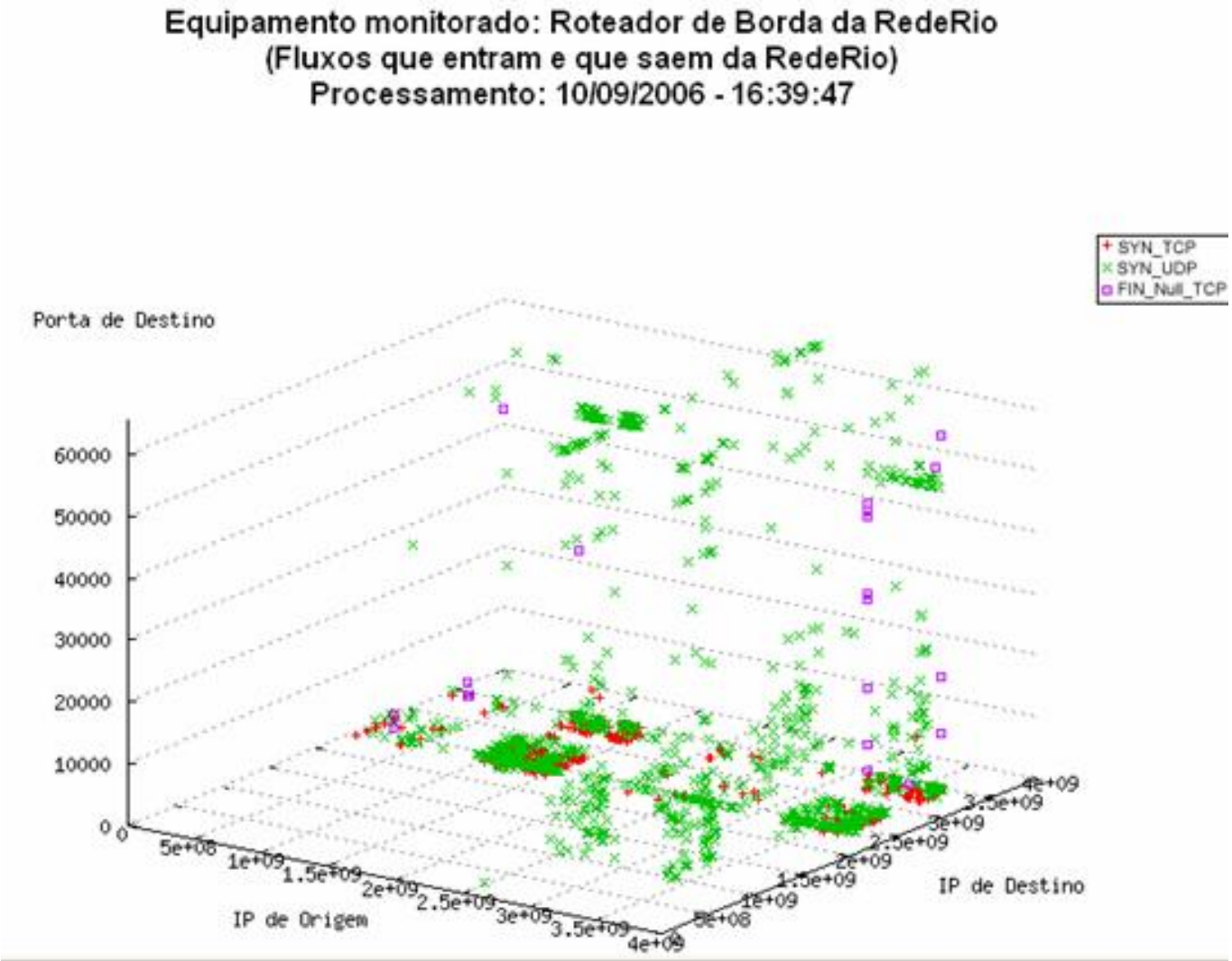
Ferramenta Proposta

Funcionalidades



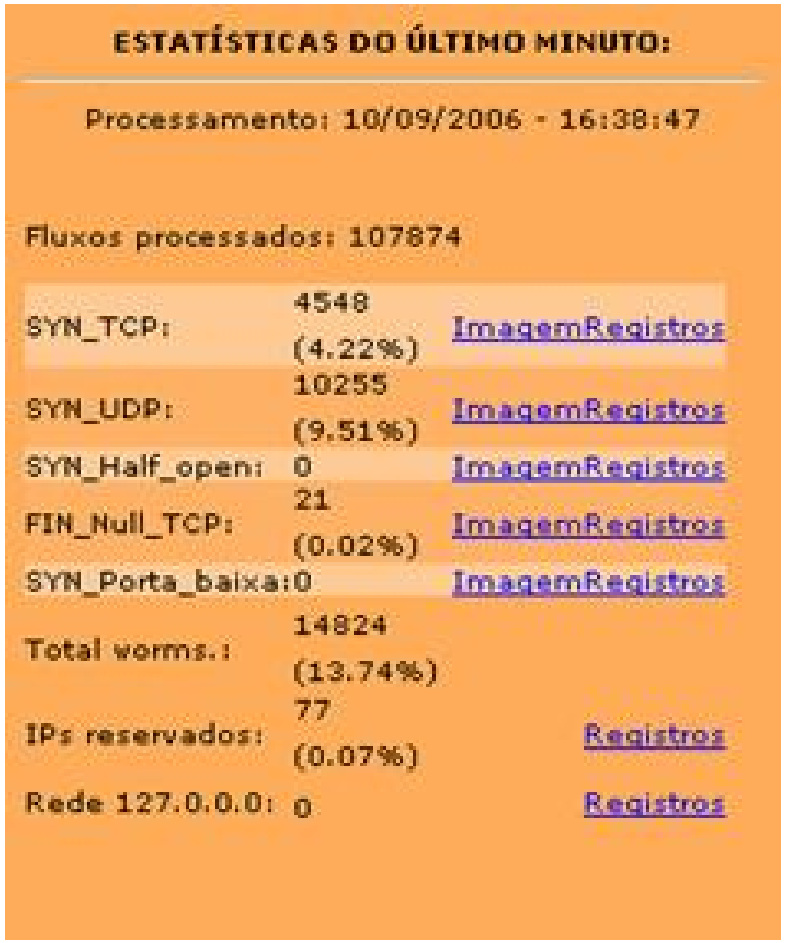
Ferramenta Proposta

Funcionalidades



Ferramenta Proposta

Funcionalidades



ESTATÍSTICAS DO ÚLTIMO MINUTO:

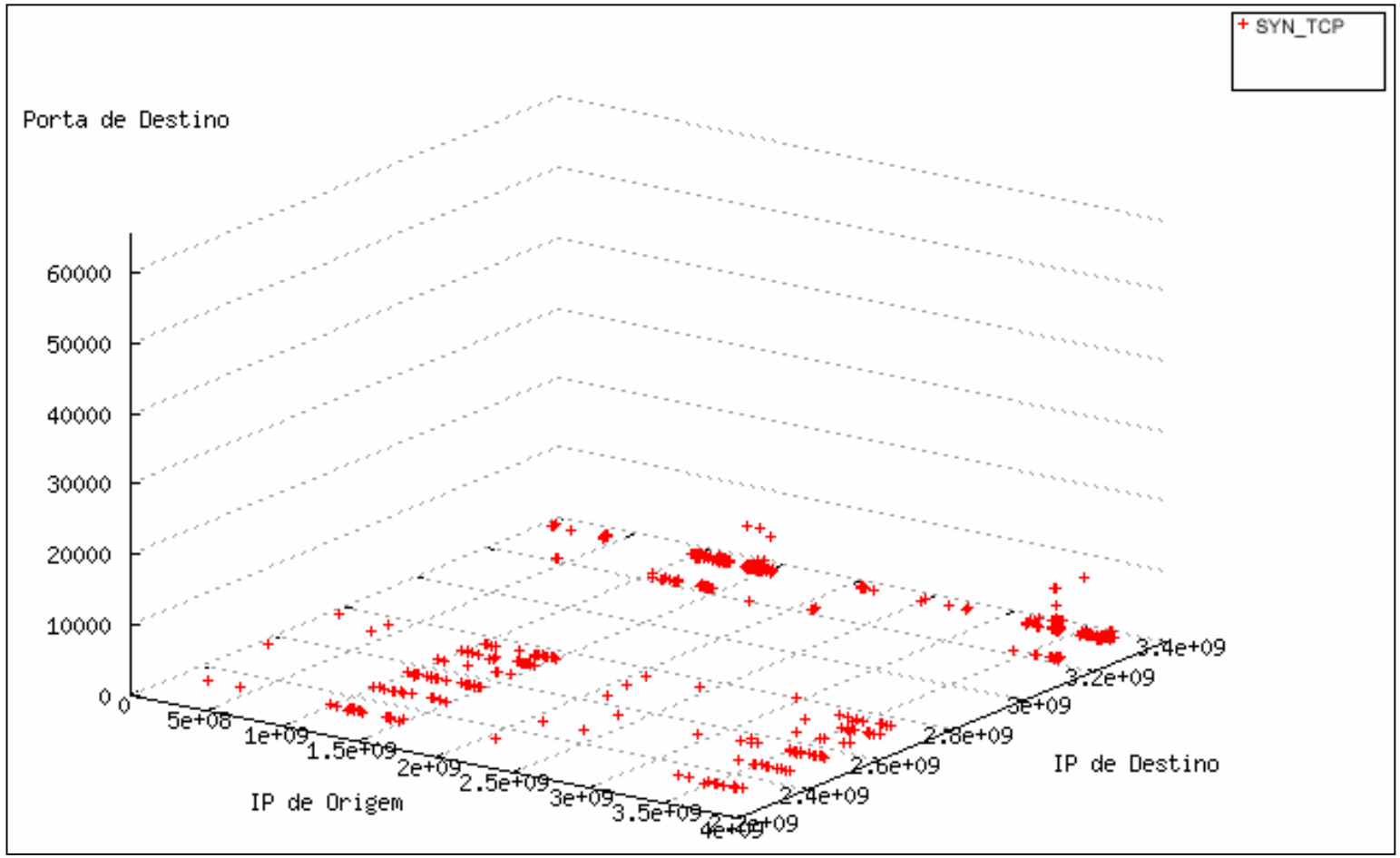
Processamento: 10/09/2006 - 16:38:47

Fluxos processados: 107874

SYN_TCP:	4548 (4.22%)	ImagemRegistros
SYN_UDP:	10255 (9.51%)	ImagemRegistros
SYN_Half_open:	0	ImagemRegistros
FIN_Null_TCP:	21 (0.02%)	ImagemRegistros
SYN_Porta_baixa:	0	ImagemRegistros
Total worms.:	14824 (13.74%)	
IPs reservados:	77 (0.07%)	Registros
Rede 127.0.0.0:	0	Registros

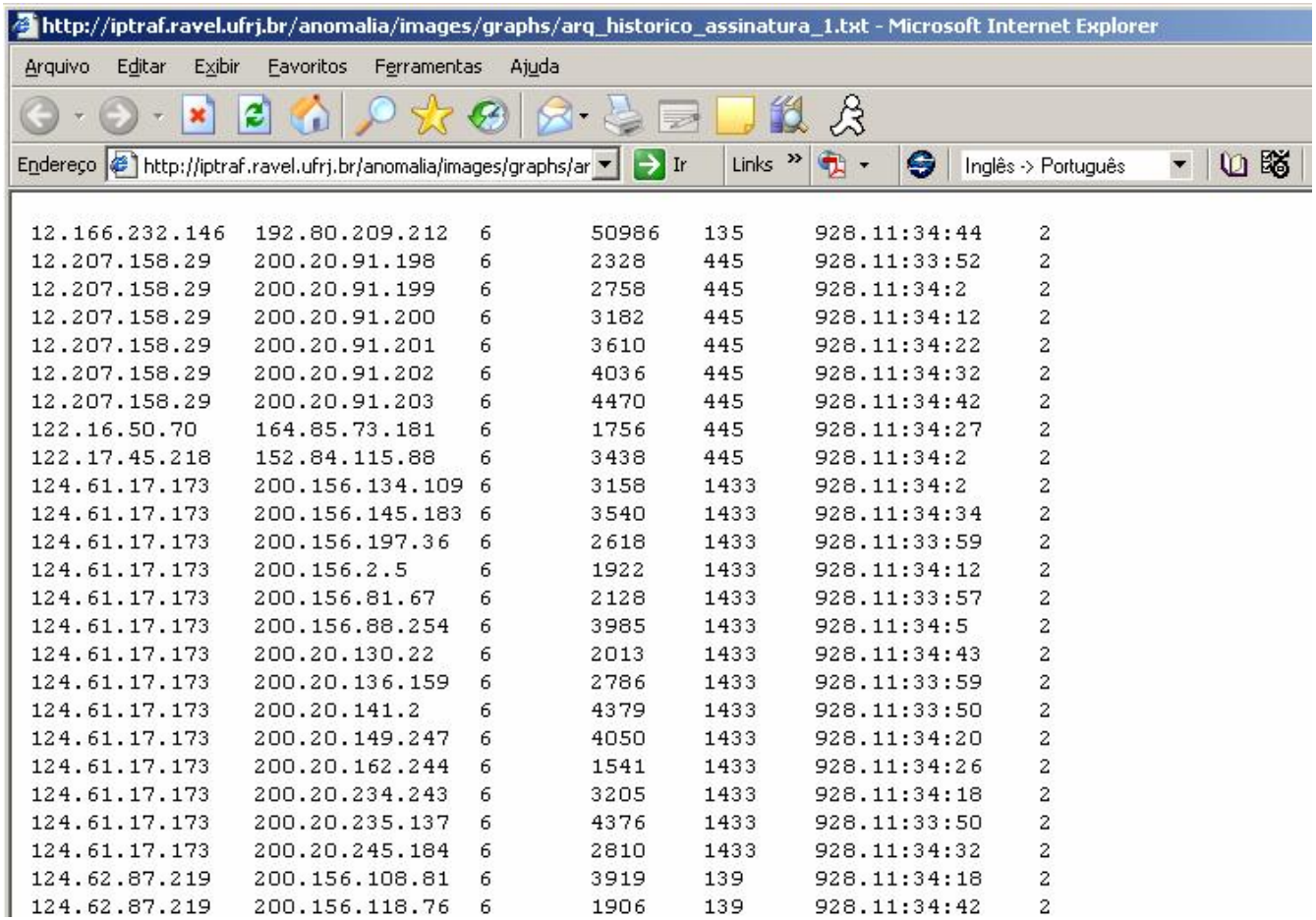
Ferramenta Proposta

Funcionalidades



Ferramenta Proposta

Funcionalidades

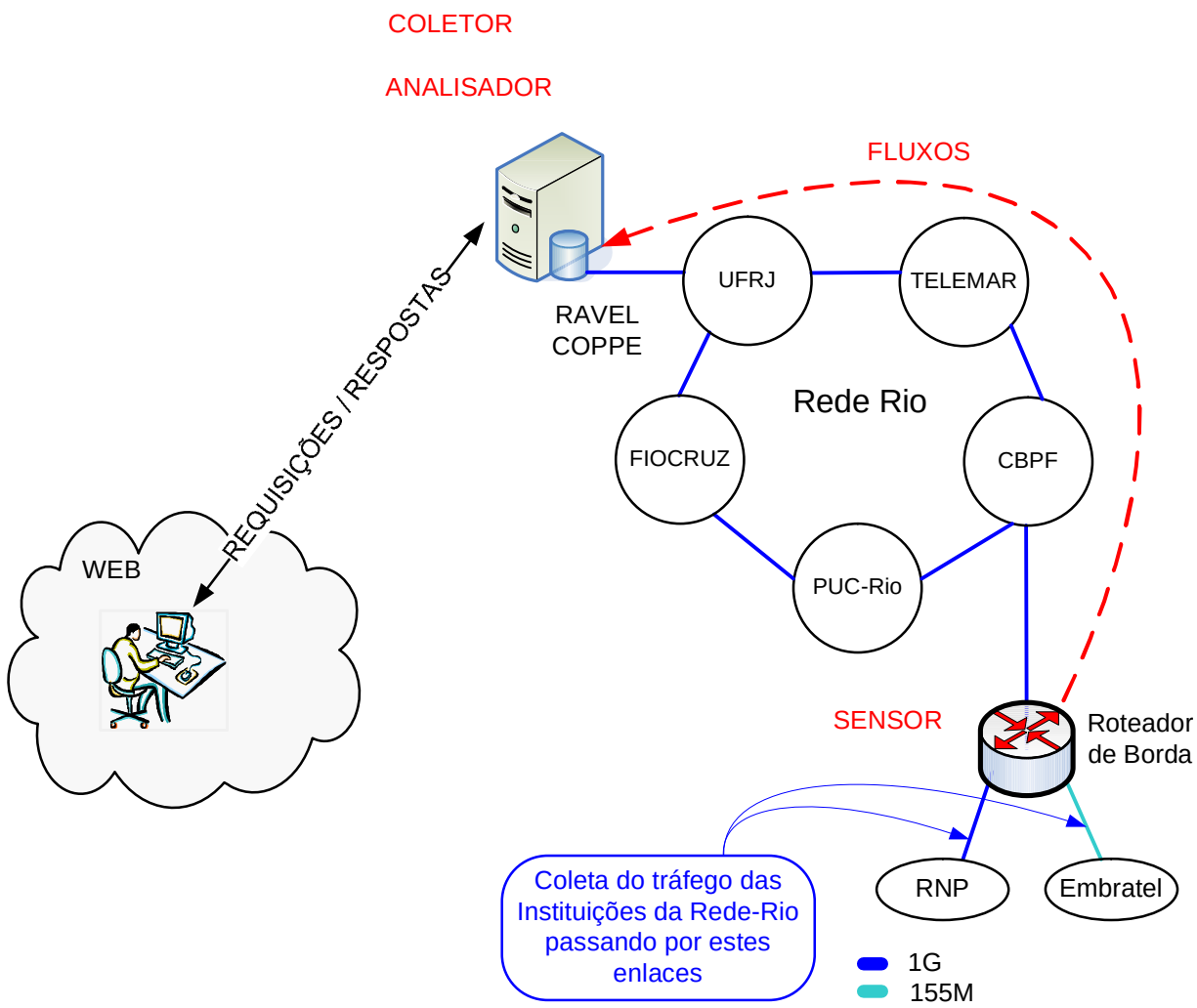


12.166.232.146	192.80.209.212	6	50986	135	928.11:34:44	2
12.207.158.29	200.20.91.198	6	2328	445	928.11:33:52	2
12.207.158.29	200.20.91.199	6	2758	445	928.11:34:2	2
12.207.158.29	200.20.91.200	6	3182	445	928.11:34:12	2
12.207.158.29	200.20.91.201	6	3610	445	928.11:34:22	2
12.207.158.29	200.20.91.202	6	4036	445	928.11:34:32	2
12.207.158.29	200.20.91.203	6	4470	445	928.11:34:42	2
122.16.50.70	164.85.73.181	6	1756	445	928.11:34:27	2
122.17.45.218	152.84.115.88	6	3438	445	928.11:34:2	2
124.61.17.173	200.156.134.109	6	3158	1433	928.11:34:2	2
124.61.17.173	200.156.145.183	6	3540	1433	928.11:34:34	2
124.61.17.173	200.156.197.36	6	2618	1433	928.11:33:59	2
124.61.17.173	200.156.2.5	6	1922	1433	928.11:34:12	2
124.61.17.173	200.156.81.67	6	2128	1433	928.11:33:57	2
124.61.17.173	200.156.88.254	6	3985	1433	928.11:34:5	2
124.61.17.173	200.20.130.22	6	2013	1433	928.11:34:43	2
124.61.17.173	200.20.136.159	6	2786	1433	928.11:33:59	2
124.61.17.173	200.20.141.2	6	4379	1433	928.11:33:50	2
124.61.17.173	200.20.149.247	6	4050	1433	928.11:34:20	2
124.61.17.173	200.20.162.244	6	1541	1433	928.11:34:26	2
124.61.17.173	200.20.234.243	6	3205	1433	928.11:34:18	2
124.61.17.173	200.20.235.137	6	4376	1433	928.11:33:50	2
124.61.17.173	200.20.245.184	6	2810	1433	928.11:34:32	2
124.62.87.219	200.156.108.81	6	3919	139	928.11:34:18	2
124.62.87.219	200.156.118.76	6	1906	139	928.11:34:42	2

Roteiro

- Introdução;
- Trabalhos Relacionados;
- Metodologia utilizada;
- A Ferramenta para Gerência de Segurança Usando Análise de Tráfego em Backbones IP ;
- **Aplicação da Ferramenta em um Cenário Real;**
- Resultados Obtidos;
- Conclusões e Trabalhos Futuros.

Aplicação da Ferramenta ao Monitoramento da Segurança de Redes



Roteiro

- Introdução;
- Trabalhos Relacionados;
- Metodologia utilizada;
- A Ferramenta para Gerência de Segurança Usando Análise de Tráfego em Backbones IP ;
- Aplicação da Ferramenta em um Cenário Real;
- **Resultados Obtidos;**
- Conclusões e Trabalhos Futuros..

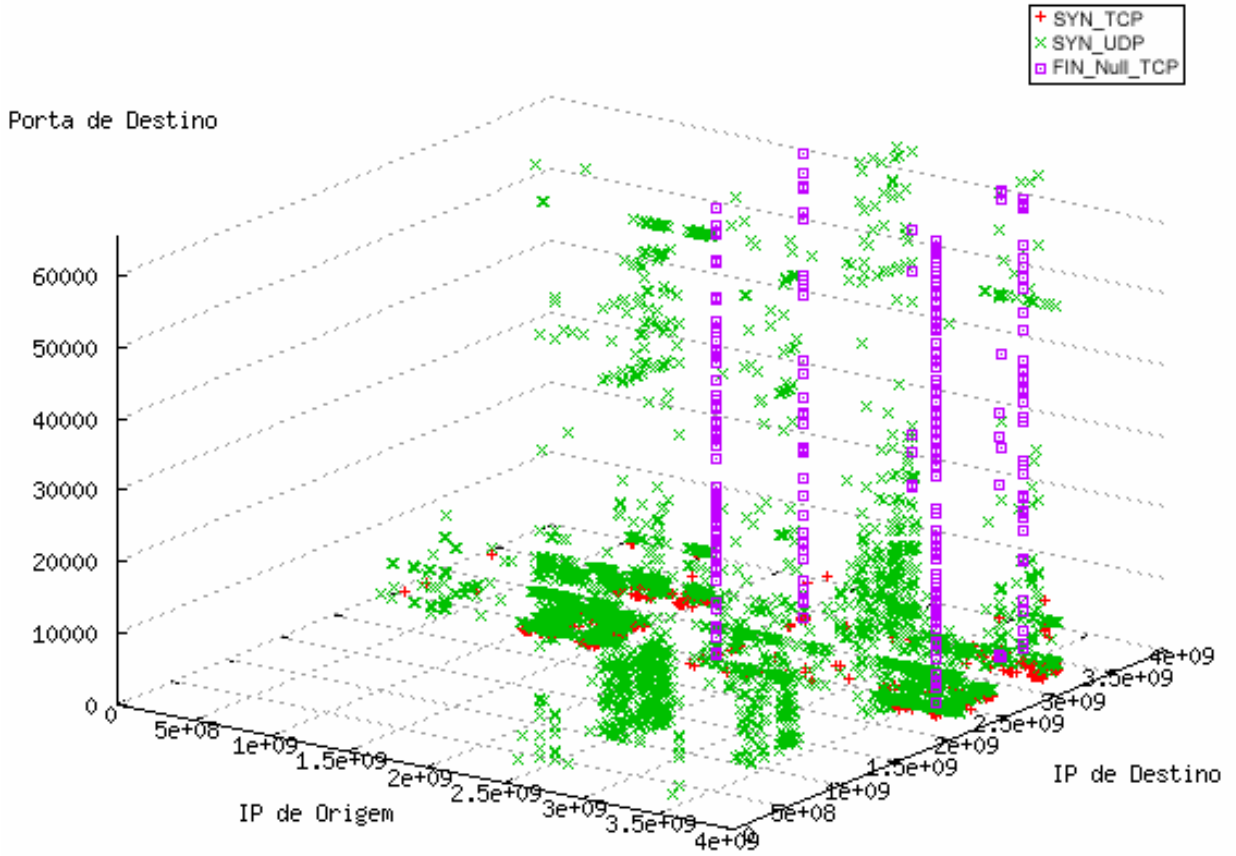
Resultados Obtidos

- Visualização Global de Propagações de Worms

Intervalo de observação: 1 min

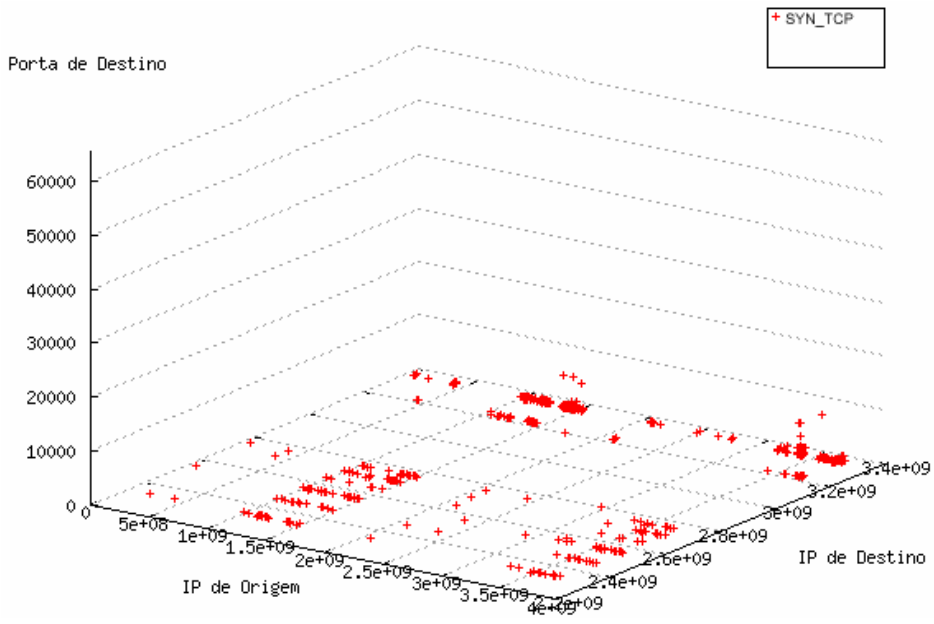
Fluxos analisados: 387.835

Fluxos classificados como Propagação de worm:
30.575 (7,88%)



Resultados Obtidos

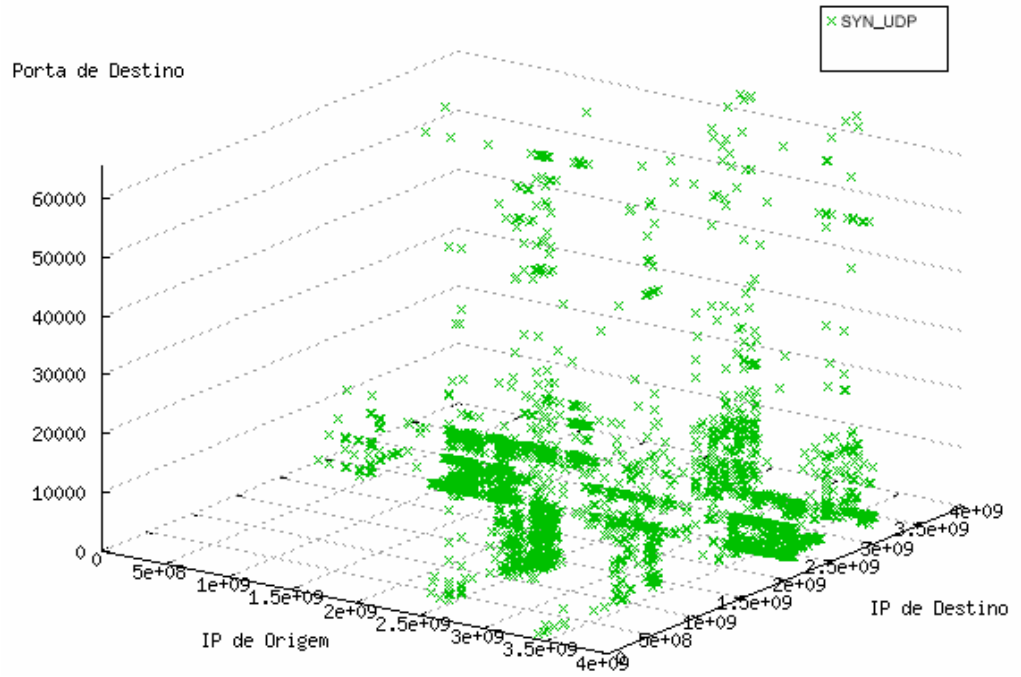
- Visualização de Propagações de Worms – SYN_TCP



Seqüência	IP de origem	IP de destino	Prot.	P. Orig.	P. Dest.	Timestamp	Flag
1	24.109.180.253	200.156.186.139	6	2198	135	824.12:49:56	2
2	24.109.180.253	200.156.190.235	6	2224	135	824.12:49:57	2
...							
3864	89.236.74.250	200.156.82.90	6	2681	135	824.12:49:7	2
3865	89.236.74.250	200.20.151.249	6	2551	135	824.12:49:5	2
3866	89.236.74.250	200.20.26.46	6	3025	135	824.12:49:10	2
3867	24.173.101.217	192.80.209.198	6	1972	139	824.12:49:58	2
...							
3868	69.221.123.255	200.156.13.233	6	4049	139	824.12:50:0	2
3869	69.221.123.255	200.156.140.30	6	3665	139	824.12:49:14	2
...							
6576	86.197.27.82	139.82.54.8	6	2775	139	824.12:49:48	2
6577	86.197.27.82	139.82.54.9	6	2776	139	824.12:49:48	2
6578	4.154.111.133	200.156.77.7	6	2985	445	824.12:49:45	2
6579	4.226.111.108	152.92.88.87	6	2815	445	824.12:49:27	2
...							
6580	4.233.143.149	152.92.118.236	6	3212	445	824.12:49:16	2
6581	4.235.206.103	200.20.106.26	6	4529	445	824.12:49:23	2
...							
9680	89.50.118.205	200.156.41.157	6	3831	445	824.12:49:50	2
9681	89.51.127.200	164.85.124.221	6	4045	445	824.12:49:30	2

Resultados Obtidos

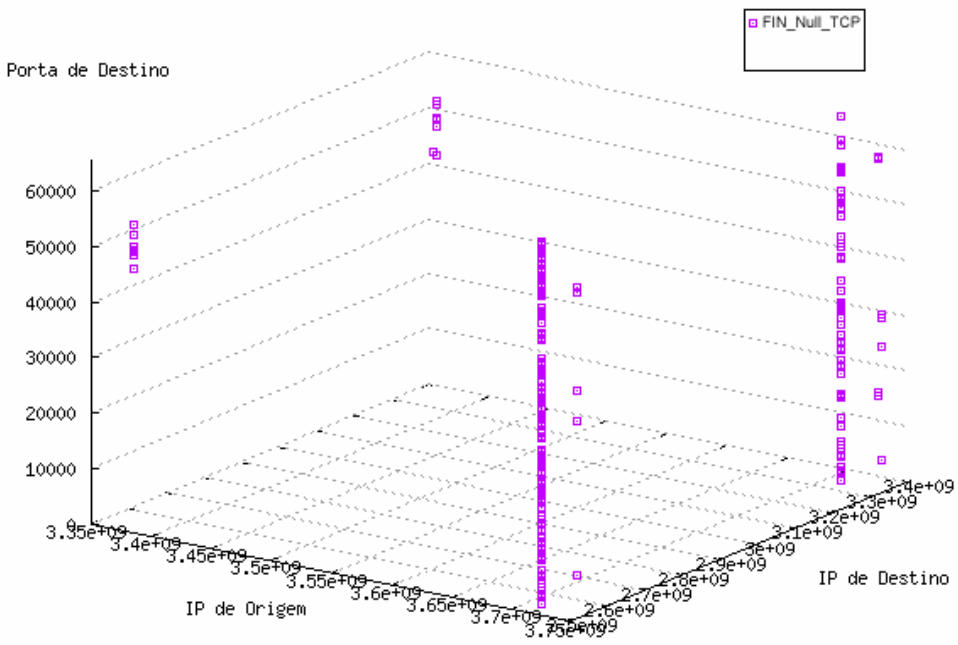
- Visualização de Propagações de Worms – SYN_UDP



Seqüência	IP de origem	IP de destino	Prot.	P.orig.	P.dest.	Timestamp	Flag
1	70.104.130.122	200.156.205.100	17	1030	137	824.12:50:04	0
2	70.104.130.122	200.156.205.102	17	1030	137	824.12:50:05	0
...					...		
3266	85.97.108.174	152.92.81.98	17	1030	137	824.12:49:08	0
3267	200.20.217.63	199.146.22.106	17	1027	137	824.12:49:26	0
3268	200.20.217.63	199.146.22.107	17	1027	137	824.12:49:26	0
3269	200.20.217.63	199.146.22.108	17	1027	137	824.12:49:26	0
3270	200.20.217.63	199.146.22.109	17	1027	137	824.12:49:27	0
3271	200.20.217.63	199.146.22.110	17	1027	137	824.12:49:27	0
3272	200.20.217.63	199.146.22.111	17	1027	137	824.12:49:27	0
3273	200.20.217.63	199.146.22.112	17	1027	137	824.12:49:27	0
3274	200.20.217.63	199.146.22.113	17	1027	137	824.12:49:27	0
3275	200.20.217.63	199.146.22.114	17	1027	137	824.12:49:28	0
...							
6076	4.154.214.121	200.20.89.35	17	2145	1434	824.12:49:19	0
6077	24.165.194.156	161.79.118.135	17	2503	1434	824.12:49:27	0
6078	61.175.163.195	139.82.153.30	17	1048	1434	824.12:49:17	0
6079	61.175.163.195	139.82.160.85	17	1048	1434	824.12:49:24	0
6080	61.175.163.195	139.82.167.140	17	1048	1434	824.12:49:30	0
6081	61.175.163.195	139.82.174.195	17	1048	1434	824.12:49:37	0
6082	61.175.163.195	139.82.22.1	17	1048	1434	824.12:49:54	0
6083	61.175.163.195	139.82.236.182	17	1048	1434	824.12:49:15	0
6084	61.175.163.195	139.82.243.237	17	1048	1434	824.12:49:21	0
6085	61.175.163.195	139.82.36.111	17	1048	1434	824.12:50:07	0
6086	61.175.163.195	139.82.63.79	17	1048	1434	824.12:49:13	0
6087	61.175.163.195	139.82.77.189	17	1048	1434	824.12:49:26	0
6088	61.175.163.195	139.82.84.244	17	1048	1434	824.12:49:32	0
6089	61.175.163.195	139.82.91.43	17	1048	1434	824.12:49:39	0
6090	61.175.163.195	139.82.98.98	17	1048	1434	824.12:49:45	0
6091	61.175.163.195	146.164.10.170	17	1048	1434	824.12:49:52	0
6092	61.175.163.195	146.164.100.38	17	1048	1434	824.12:49:04	0
6093	61.175.163.195	146.164.22.27	17	1048	1434	824.12:49:09	0
...							

Resultados Obtidos

- Visualização de Propagações de Worms – FIN_Null_TCP



Seqüência	IP de origem	IP de destino	Prot.	P.orig.	P.dest.	Timestamp	Flag
1	221.5.2.72	152.84.10.37	6	80	48685	824.12:49:36	4
2	221.5.2.72	152.84.10.94	6	80	27661	824.12:49:54	4
3	221.5.2.72	152.84.103.126	6	80	14436	824.12:49:34	4
...							
130	221.5.2.72	152.84.96.111	6	80	59933	824.12:49:30	4
131	221.5.2.72	152.84.98.20	6	80	30746	824.12:49:55	4
132	221.5.2.72	200.20.100.90	6	80	29030	824.12:49:52	4
133	221.5.2.72	200.20.106.123	6	80	40207	824.12:49:31	4
134	221.5.2.72	200.20.124.87	6	80	43868	824.12:49:47	4
135	221.5.2.72	200.20.125.43	6	80	4193	824.12:50:8	4
136	221.5.2.72	200.20.127.35	6	80	39734	824.12:49:23	4
137	221.5.2.72	200.20.127.88	6	80	4478	824.12:49:46	4
184	221.5.2.72	200.20.88.16	6	80	33852	824.12:49:43	4
185	221.5.2.72	200.20.89.77	6	80	55123	824.12:50:10	4
186	221.5.2.72	200.20.97.92	6	80	89	824.12:50:10	4
187	222.216.109.73	200.156.113.102	6	80	30260	824.12:49:36	4
188	222.216.109.73	152.84.121.88	6	80	34169	824.12:49:44	4
189	222.216.109.73	152.84.152.120	6	80	6472	824.12:49:33	4
...							
198	222.216.109.73	200.20.148.50	6	80	17031	824.12:49:44	4
199	222.216.109.73	200.20.220.25	6	80	16573	824.12:49:35	4
200	200.203.183.25	200.156.169.126	6	443	49649	824.12:49:49	4
201	200.203.183.25	200.156.218.201	6	443	52767	824.12:50:11	4
202	200.203.183.25	152.84.129.128	6	443	48325	824.12:49:27	4
203	200.203.183.25	152.84.137.113	6	443	49275	824.12:50:0	4
204	200.203.183.25	152.84.175.122	6	443	47705	824.12:49:21	4
205	200.203.183.25	152.84.18.145	6	443	48814	824.12:49:40	4
206	200.203.183.25	152.84.228.171	6	443	45427	824.12:50:18	4
207	200.203.183.25	152.84.31.12	6	443	51546	824.12:50:8	4
208	200.203.183.25	152.84.83.155	6	443	53304	824.12:50:17	4
209	200.203.183.25	200.156.143.32	6	443	48433	824.12:49:28	4
210	200.203.183.25	200.156.212.60	6	443	52371	824.12:50:16	4
211	200.203.183.25	200.156.89.61	6	443	43342	824.12:49:30	4
212	200.203.183.25	200.156.91.188	6	443	49736	824.12:49:49	4
213	200.203.183.25	200.20.48.147	6	443	44171	824.12:49:47	4

Resultados Obtidos

- Monitoramento de Fluxos Oriundos de Endereçamento Reservado:

IP de origem	IP de destino	Prot.	P.orig.	P. Dest.	Timestamp	Flag
-- corta --						
10.10.100.39	82.129.35.231	17	137	137	825.21:39:40	0
10.10.100.39	82.129.35.235	17	137	137	825.21:39:41	0
10.10.100.39	82.129.35.237	17	137	137	825.21:39:41	0
10.10.100.39	85.17.34.14	17	137	137	825.21:39:10	0
10.10.100.39	88.213.35.5	17	137	137	825.21:39:25	0
10.10.100.39	96.121.34.0	17	137	137	825.21:39:05	0
10.10.100.39	96.67.34.0	17	137	137	825.21:39:05	0
10.10.13.3	200.20.186.75	17	1024	123	825.21:38:48	0
10.24.24.50	66.61.36.127	6	25	1300	825.21:39:20	0
139.82.74.4	172.16.129.109	6	51749	25	825.21:39:34	2
139.82.74.4	172.16.129.109	6	51749	25	825.21:40:20	2
146.164.34.145	172.28.1.10	6	1507	9876	825.21:39:37	2
146.164.34.145	172.28.1.10	6	1508	9876	825.21:39:47	2
146.164.34.145	172.28.1.10	6	1509	9876	825.21:39:57	2
146.164.34.145	172.28.1.10	6	1510	9876	825.21:40:07	2
146.164.34.145	172.28.1.10	6	1511	9876	825.21:40:17	2
152.84.252.236	10.0.0.1	6	4619	80	825.21:39:53	0
152.84.252.236	10.0.0.1	6	4620	80	825.21:39:17	0
152.84.252.236	10.0.0.1	6	4621	80	825.21:39:41	0
152.84.253.2	172.16.129.107	6	60174	25	825.21:40:27	2

Resultados Obtidos

- Volume Médio de Fluxos classicados como propagação de Worms:

Período de análise: 23 a 31 de agosto de 2006

Descrição	Número de fluxos	Percentual
Total analisado	2.212.189.939	
SYN_TCP	71.623.813	3,24%
SYN_UDP	139.748.823	6,31%
SYN_Half_open	0	0
FIN_Null_TCP	932.873	0,04%
SYN_Porta_baixa	0	0
Total de tráfego de propagação de *worms*	212.305.509	9,59%

Resultados Obtidos

- Volume Médio de Fluxos oriundos de Endereçamento Reservado:

Período de análise: 25 a 31 de agosto de 2006

Fluxos analisados: ≈ 1,5 bilhões de fluxos

≈ 1,4 milhões (0,096%) oriundos de endereçamento reservado

Roteiro

- Introdução;
- Trabalhos Relacionados;
- Metodologia utilizada;
- A Ferramenta para Gerência de Segurança Usando Análise de Tráfego em Backbones IP ;
- Aplicação da Ferramenta em um Cenário Real;
- Resultados Obtidos;
- **Conclusões e Trabalhos Futuros.**

Conclusões e Trabalhos Futuros

Com o uso da metodologia proposta, mostrou-se que é possível, rapidamente, localizar equipamentos contaminados com *worms* em um backbone IP Gigabit Ethernet.

Explorou-se o recurso visual como meio de divulgação do resultado da análise, em tempo próximo do real e sem interferência no tráfego benigno.

Os resultados obtidos mostram que, em média, 10 % de todos os fluxos trafegados, são oriundos de propagação de *worms* ou de utilização indevida de endereçamento reservado.

O fornecimento de informações estatísticas, em tempo próximo do real e com a preservação de seu histórico, garante uma entendimento mais realístico dos eventos anômalos na rede.

Conclusões e Trabalhos Futuros

Objetivos:

Fornecer, em tempo real, subsídios necessários para a reação em casos de atividades maliciosas em ambientes livres de restrições de acesso e em grandes volumes de dados trafegados;	OK
Automatizar os procedimentos utilizados para a identificação do(s) elemento(s) gerador(es) do tráfego anômalo;	OK
Apresentar visualmente o resultado das análises do tráfego classificado;	OK
Prover um histórico das anormalidades identificadas;	OK
Não interferir no tráfego benigno.	OK

Conclusões e Trabalhos Futuros

Trabalhos futuros:

- Análise de novos parâmetros visando criação de novos perfis de comportamentos anômalos.

- Integração da ferramenta implementada com sistemas de rastreamento de atacantes (IP Traceback).

Perguntas / Comentários

Ferramenta para Gerência de Segurança Usando Análise de Tráfego em Backbones IP

Cláudia de Abreu Silva [1,2]
claudia@dtm.mar.mil.br

Luís Felipe Magalhães de Moraes [1]
moraes@ravel.ufrj.br

[1] Universidade Federal do Rio de Janeiro (UFRJ)

[2] Marinha do Brasil