PARANÁ
GOVERNO DO ESTADO

COPEL

Pura Energia

COPEL
Pura Energia

PARANÁ
GOVERNO DO ESTADO

Experiência da Copel Telecomunicações na gerência da porta 25

Giovani Colombo

Joelson Tadeu Vendramin

II Semana da Infraestrutura da Internet no Brasil

GTER 34 / GTS 20

Agenda

- COPEL;
- Copel Telecomunicações;
- Produtos de internet;
- *Blacklists*;
- *Blacklist* UCEProtect-Network;
- Ferramentas na internet;
- Cenário 2010;
- Procedimento da aplicação do filtro da porta 25;
- Resultados;
- Cenário 2012;
- Considerações finais.

COPEL – Companhia Paranaense de Energia

- COPEL – Companhia Paranaense de Energia;
- Maior empresa do estado;
- Criada em 26 de outubro de 1954 (58 anos);
- Presente em 396 municípios e 1.114 localidades (distritos, vilas e povoados);
- Atua nas áreas de geração, transmissão, distribuição e telecomunicações;
- Produção de 7% da energia elétrica consumida no Brasil;
- Site: http://www.copel.com

COPEL Telecomunicações

- Criada em 1970 (42 anos) para atender a COPEL – telefonia corporativa, sistemas VHF, UHF e Carrier;
- 1998 – licença SLE – Serviço Limitado Especializado;
- 1999 – primeiro cliente;
- 2001 – COPEL Telecomunicações (COPEL Telecom);
- 2002 – licença SCM – Serviço de Comunicação Multimídia – Área II;
- Presente em todas as 399 cidades (PR) e 2 (SC);
- Infovia do Paraná – 8.397km de OPGW e 19.620km de cabos autossustentados;
- Clientes: COPEL (rede administrativa; automação de SEs e chaves; oscilopertubografia; medições de grandes clientes e entre concessionárias); Paraná Digital; Rede do Governo, operadoras e outros clientes;
- Site: http://www.copeltelecom.com

Produtos de Internet

- IP Direto:
  - Pequenas, médias e grandes empresas;
  - Banda simétrica (upload e download);
  - 5 IPs fixos;
  - Sem franquia de consumo.

- BEL:
  - BEL Profissional – Mercado residencial e profissionais liberais;
  - BEL Empresa – Pequenas empresas;
  - Banda simétrica (upload e download);
  - 1 IP dinâmico;
  - Sem franquia de consumo.

COPEL
Pura Energia

PARANÁ
GOVERNO DO ESTADO

Técnicas anti-spam

Principais técnicas anti-spam

- Listas de bloqueios:
  - Listas negras (*Blacklists*);
  - Linhas discadas;
  - *Relay* e *Proxies* abertos.
- Listas de exceção (*Whitelists*);
- Filtros de conteúdo:
  - Anti-vírus;
  - Filtros Bayesianos;
  - Bloqueio de anexos.
- *Greylisting*.

- (Fonte: CERT.BR, 2006)

Listas Negras (*Blacklists*)

- Mensagens vindas de endereços IPs contidos nesta lista poderão ser:
  - descartadas, notificando ou não a origem que a mensagem foi classificada como spam;
  - marcadas essas mensagens como [spam] e enviadas assim mesmo.
- Implementação fácil e praticamente todo MTA (*Mail Transfer Agent*) possui suporte para este recurso;
- Critérios de inclusão:
  - Somente IPs;
  - Blocos;
  - AS (*Autonomous System*).

- (Fontes: ANTISPAM.BR, 2012; CERT.BR, 2006)

Listas Negras (*Blacklists*)

- É possível criar sua própria lista negra;
- Problemas encontrados:
  - Endereços IPs são listados por pertencer a blocos “sujos”;
  - O IP permanecer listado por muito tempo, mesmo depois de sanado o problema;
  - Problemas com a inexistência ou inconsistência do DNS Reverso.

- (Fontes: CERT.BR, 2006)

Blacklist: UCEPROTECT-NETWORK

- UCEPROTECT – www.uceprotect.net
- Trabalha com 3 políticas de níveis:
  - Nível 1 (*conservative*) – lista IPs isolados;
  - Nível 2 (*strict*) – escalona para a alocação do bloco de IPs;
  - Nível 3 (draconic) – lista o espaço de IPs e também os ASNs.
- Nível 1 – lista os IPs e as recorrências (*hits*). O IP permanece na lista por 7 dias, caso não haja nenhuma recorrência. Enquanto houver recorrências, o IP continua listado até passar o prazo de 7 dias da última recorrência.

Blacklist: UCEPROTECT-NETWORK

- Nível 2 – A alocação de bloco segue os seguintes critérios:

Máscara	Quantidade de IPs
/26	1
/25	2
/24	**5**
/23	10
/22	15

Máscara	Quantidade de IPs
/21	25
/20	40
/19	65
/18	105
/17	170
/16	275

Blacklist: UCEPROTECT-NETWORK

- Nível 2 (cont.): $$x = \frac{\text{nº IPs listados}}{\text{Limite máscara}}$$

Critério (x)	Status
x < 0,25	Not listed
0,25 <= x < 0,50	Attention
0,50 <= x < 0,75	Warning
0,75 <= x < 1,00	Alert
x >= 1,00	Listed

Blacklist: UCEPROTECT-NETWORK

- Nível 2 (cont.):

[redacted].84.0/22	NOT LISTED	0	15
[redacted].128.0/20	ALERT Extreme Listingrisk	31	40
---> [redacted].132.0/24	LISTED	7	5
---> [redacted].136.0/24	LISTED	5	5
[redacted].128.0/21	WARNING High Listingrisk	16	25
[redacted].136.0/21	WARNING High Listingrisk	15	25
[redacted].144.0/20	NOT LISTED	7	40
[redacted].144.0/21	NOT LISTED	4	25
[redacted].152.0/21	NOT LISTED	3	25
[redacted].160.0/20	ATTENTION Increased Listingrisk	18	40

Blacklist: UCEPROTECT-NETWORK

- Nível 3 – Segue o critério da tabela abaixo, conforme a equação, sendo valor mínimo de n = 100:

$$x = \frac{\text{nº IPs listados nível 1}}{n} \qquad n = \frac{\text{nº total IPs AS}}{0{,}2\%}$$

Critério (x)	Status
x < 0,25	Not listed
0,25 <= x < 0,50	Attention
0,50 <= x < 0,75	Warning
0,75 <= x < 1,00	Alert
x >= 1,00	Listed

Ferramentas na internet

- MXToolBox (www.mxtoolbox.com):
  - *Blacklist*;
  - Resolução do DNS reverso;
  - Testar o servidor de *e-mail*;
  - Testar portas abertas.

- IPOK (www.ipok.com.br):
  - *Blacklist*;
  - Resolução do DNS reverso;
  - Análise completa do domínio.

- IP-Lookup (http://ip-lookup.net/)
  - Resolução do DNS reverso.

COPEL
Pura Energia

PARANÁ
GOVERNO DO ESTADO

CENÁRIO - 2010

Cenário - 2010

- Cenário até agosto de 2010:
  - Aumento das ordens de serviço (OS):
    - IPs listados em várias *blacklists*;
    - Clientes não conseguiam mandar *e-mail*:
      - IPs listados da sua própria sub-rede;
      - IPs listados de sub-redes vizinhas (outros clientes).
  - Solicitação para retirada dos IPs listados:
    - Alguns IPs retornavam para as *blacklists;*
    - *Algumas blacklists cobram para retirar os IPs;*
    - *Troca de rede:*
      - *Reconfiguração do circuito;*
      - *Designação Registro.BR;*
      - *Bloco sujo.*
  - Comprometimento de vários blocos de IPs listados.

Cenário - 2010

THIS INFO IS FOR PROVIDERS. IF YOU ARE ENDUSER PLEASE TEST IP INSTEAD

Informations for AS14868 - Companhia Paranaense de Energia - COPEL

23 Networks are assigned to you.

UCEPROTECT-Level2

Networks of your Allocation

Networks	Status	Level 1 listed spammers within the last 7 days	Level 2 Escalation limit by Level 1 records	Optional Expressdelisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
187.95.96.0/19	NOT LISTED	0	65	Not available
187.95.96.0/20	NOT LISTED	0	40	Not available
187.95.112.0/20	NOT LISTED	0	40	Not available
187.95.126.0/24	NOT LISTED	0	5	Not available
187.95.127.0/24	NOT LISTED	0	5	Not available
200.150.64.0/20	ATTENTION Increased Listingrisk	17	40	Not available
200.150.74.0/24	LISTED	11	5	Expressdelisting available
200.150.64.0/21	NOT LISTED	3	25	Not available
200.150.72.0/21	WARNING High Listingrisk	14	25	Not available
200.150.80.0/21	NOT LISTED	0	25	Not available
200.150.80.0/22	NOT LISTED	0	15	Not available
200.150.84.0/22	NOT LISTED	0	15	Not available
200.195.128.0/20	ALERT Extreme Listingrisk	31	40	Not available
200.195.132.0/24	LISTED	7	5	Expressdelisting available
200.195.136.0/24	LISTED	5	5	Expressdelisting available
200.195.128.0/21	WARNING High Listingrisk	16	25	Not available
200.195.136.0/21	WARNING High Listingrisk	15	25	Not available
200.195.144.0/20	NOT LISTED	7	40	Not available
200.195.144.0/21	NOT LISTED	4	25	Not available
200.195.152.0/21	NOT LISTED	3	25	Not available
200.195.160.0/20	ATTENTION Increased Listingrisk	18	40	Not available
200.195.160.0/24	LISTED	7	5	Expressdelisting available
200.195.160.0/21	ATTENTION Increased Listingrisk	11	25	Not available
200.195.168.0/21	ATTENTION Increased Listingrisk	7	25	Not available
200.195.176.0/20	WARNING High Listingrisk	25	40	Not available
200.195.176.0/21	WARNING High Listingrisk	13	25	Not available
200.195.184.0/21	ATTENTION Increased Listingrisk	12	25	Not available

What means listed at UCEPROTECT-Level 2?
UCEPROTECT Network operates three levels of blacklisting, so our users can make the decision how strong they want to filter.
While UCEPROTECT-Level 1 lists single IP's only, UCEPROTECT Level 2 is an escalation list.
According to the table above allocations get listed at Level 2 if there are too many Level 1 listings (spam sending IP's) in that ranges.
Level 2 is basically nothing more than pure mathematics based on the number of Level 1 listed IP's.
To get escalated to Level 2 is almost always an indicator, that you don't act fast enough on spammers.
From our point of view it looks like you did miss to install preventive-measures to keep abusers off your ranges.

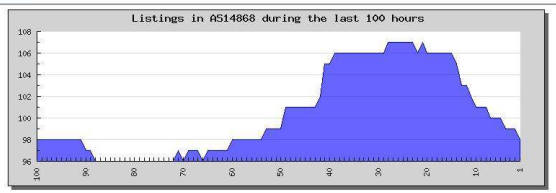
We recommend you should do so by now.
The earlier you start, the faster will your ranges expire from Level 2.

How can our netranges be removed from UCEPROTECT-Level 2?
After you have fixed the problems which caused the escalation, the UCEPROTECT-Level 2 listing will be removed automatically and free of charge as soon as the causal Level 1 listings will expire and decrease below Level 2 escalation limit. Every IP temporary listed at Level 1 expires 7 days after we have seen the last abusive action originating from it.

UCEPROTECT-Level3

Reputation of ASN 14868 | Companhia Paranaense de Energia - COPEL

AS	Status	Provider has total IP's	Level 1 listed spammers within the last 7 days	Level 3 Escalation limit by Level 1 records	Optional Expressdelisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
14868	ALERT Extreme Listingrisk	30720	98 (0.319 %) 60 Min.	100	Not available



- Em 09/09/2010 - 111 IPs listados (0,361%);

- Em 16/09/2010:
  - IPs listados = 98 (30);
  - Total de IPs = 30720;
  - Percentual= 0,319%;
  - Hits = 1243 (59);
  - Blocos listados = 04 blocos /24 (128 clientes);
  - Vários outros blocos em alerta.

Fonte: UCEPROTECT-NETWORK

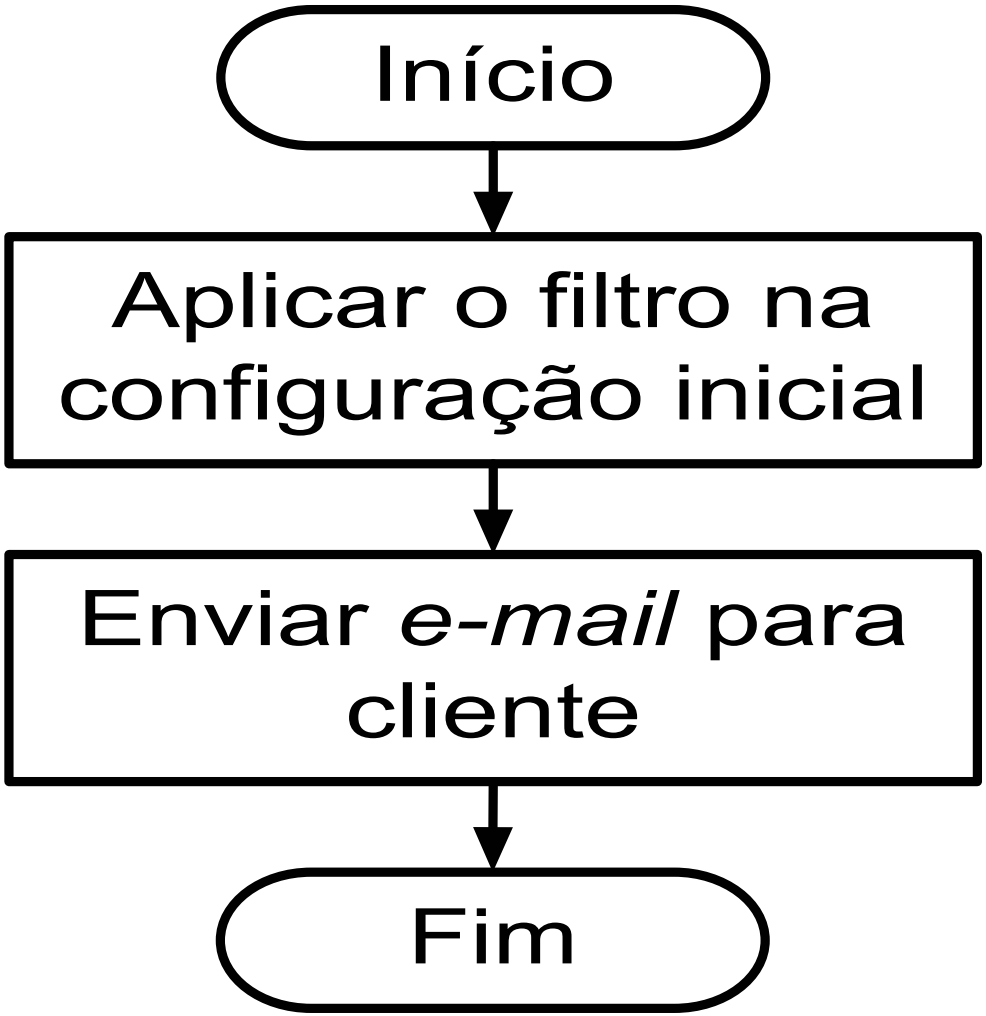
Estratégia adotada

- Definida a aplicação do filtro da porta 25:
  - Somente para clientes que utilizam IPs da COPEL;
- Clientes (BGP) com CIDRs próprios não são escopo desse controle;
- Utilizar a *blacklist* UCEPROTECT;
- Clientes novos – aplicação do filtro na configuração;
- Clientes ativos – aplicação do filtro de forma gradual, conforme os IPs entravam na *blacklist.*

Estrutura do Filtro

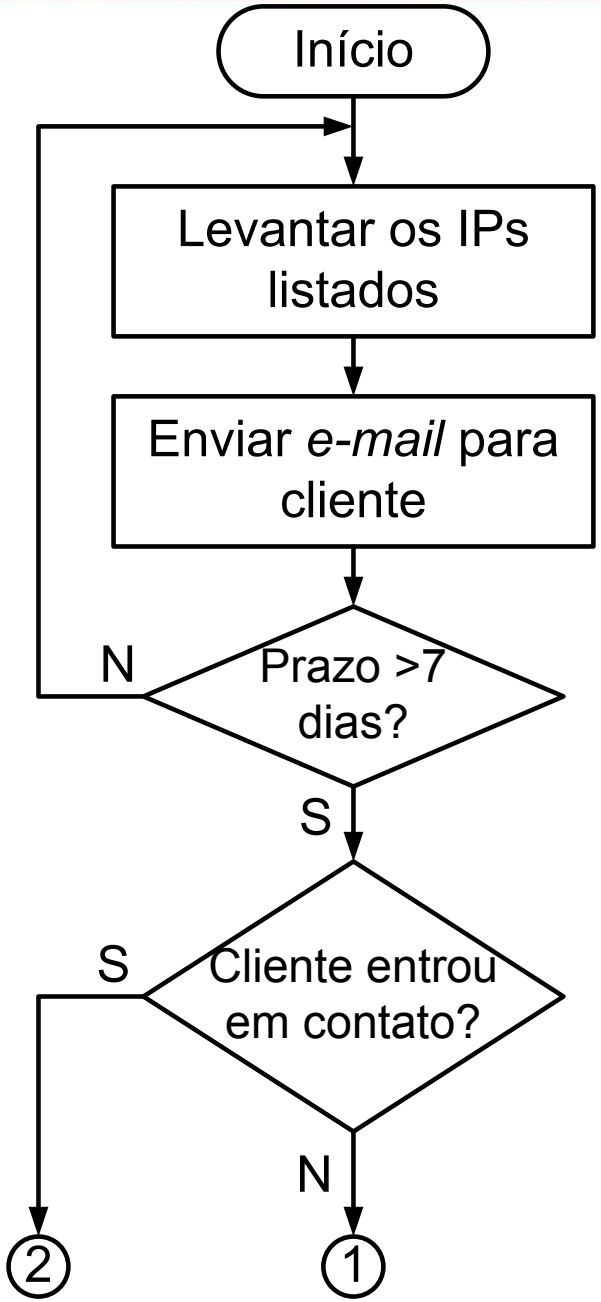
- A estrutura do filtro é muito simples;
- Consiste de 3 regras de ACLs (Access Control Lists):
  - Regra 1: Lista os IPs de origem (rede do cliente) que estão autorizados a enviar pacotes com destino para a porta 25 (TCP);
  - Regra 2: Lista os IPs de destino (SMTP servers) de alguns servidores externos que ainda não se adaptaram para receber e-mail pela porta 587 (TCP);
  - Regra 3: Bloqueia todo o tráfego com destino a porta 25 que não tenha sido explicitamente liberado pelas 2 regras anteriores.
- Aplicado no roteador que atende o cliente;
- Filtro compartilhado por todos os clientes.

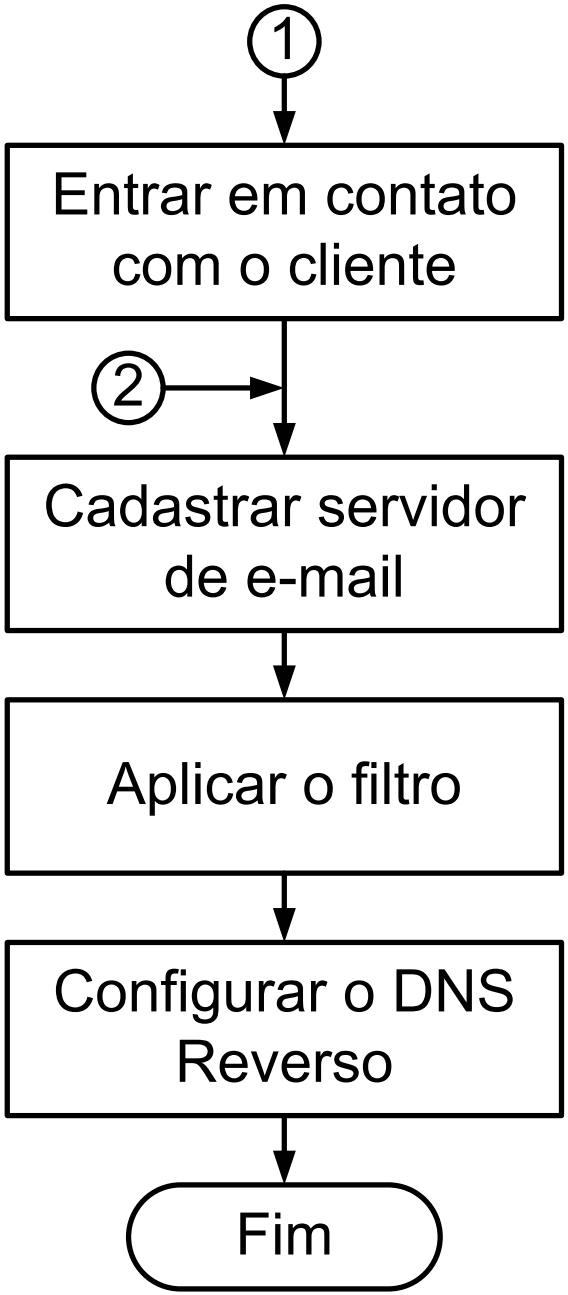
Procedimento – Clientes Novos



- *E-mail*:
  - Informando sobre o bloqueio;
  - Solicitação dos IPs – servidor de *e-mail* e o DNS Reverso;
  - Recomendação para utilizar a porta 587/TCP para submissão de *e-mails.*

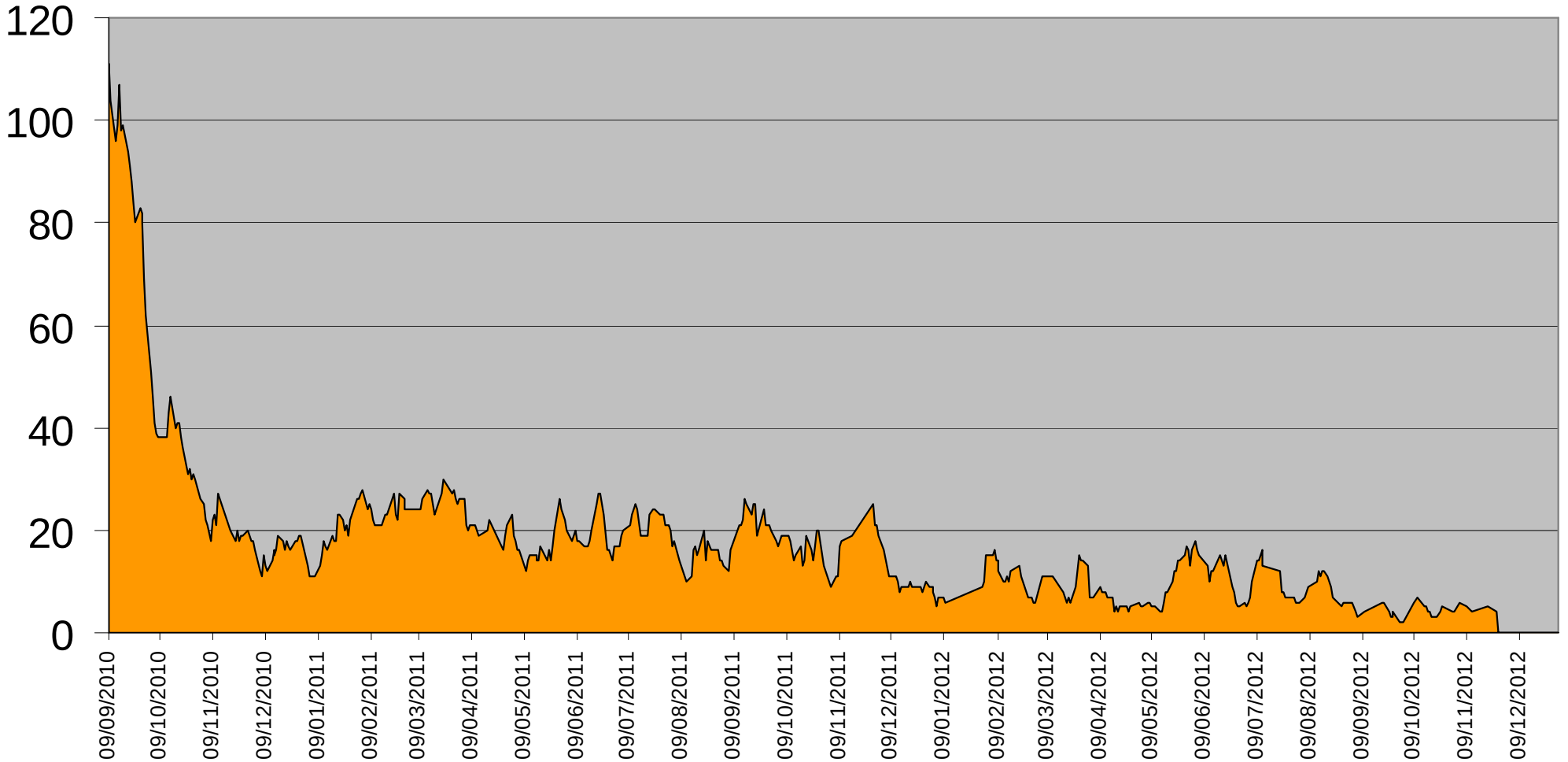
Procedimento – Clientes ativos





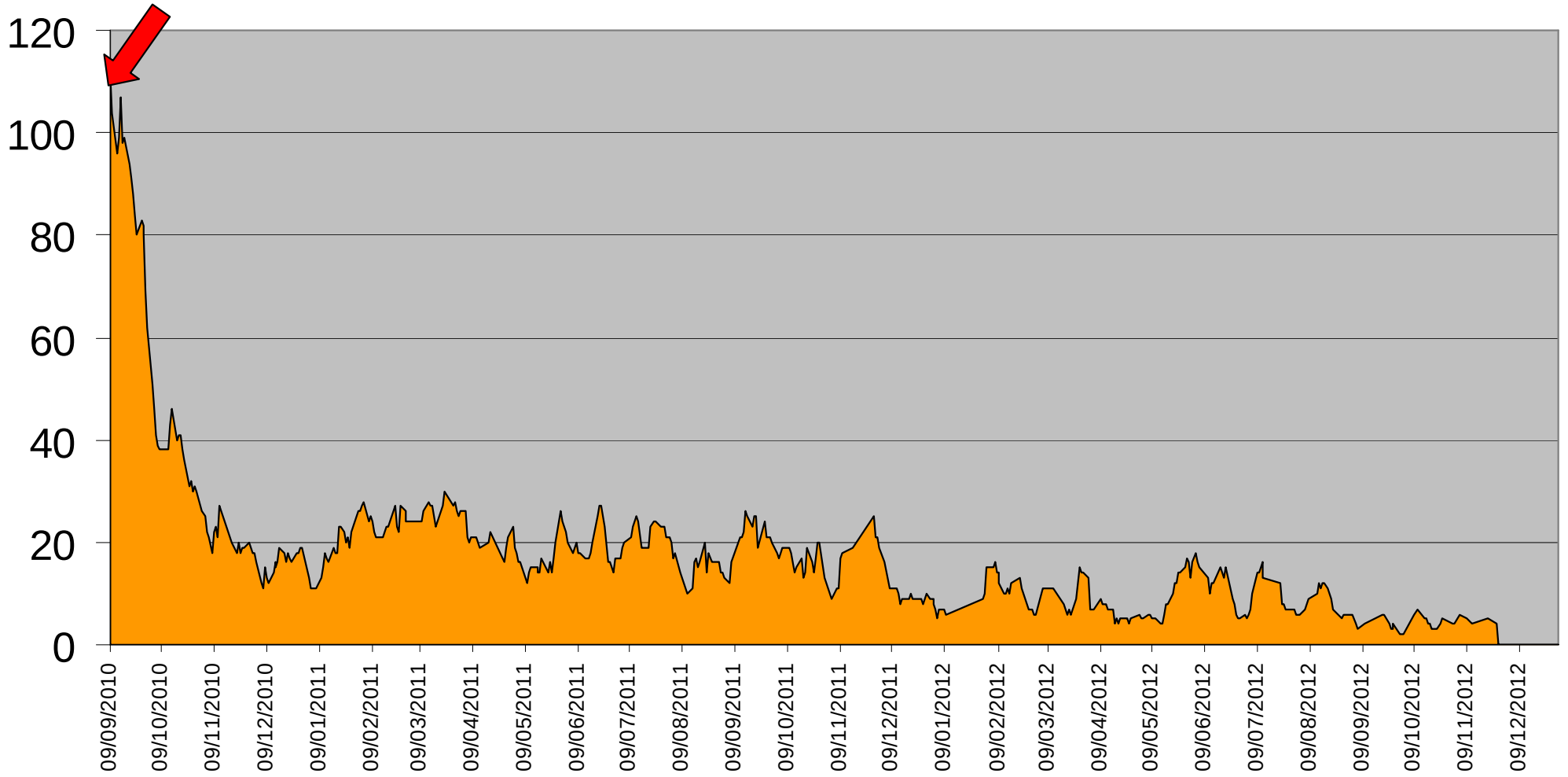
Evolução dos IPs listados

Quantidade de IPs listados



Evolução dos IPs listados

09/09/2010
111 IPs



THIS INFO IS FOR PROVIDERS. IF YOU ARE ENDUSER PLEASE TEST IP INSTEAD

Informations for AS14868 - Companhia Paranaense de Energia - COPEL

23 Networks are assigned to you.

UCEPROTECT-Level2

Networks of your Allocation

Networks	Status	Level 1 listed spammers within the last 7 days	Level 2 Escalation limit by Level 1 records	Optional Expressdelisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
187.95.96.0/19	NOT LISTED	0	65	Not available
187.95.96.0/20	NOT LISTED	0	40	Not available
187.95.112.0/20	NOT LISTED	0	40	Not available
187.95.126.0/24	NOT LISTED	0	5	Not available
187.95.127.0/24	NOT LISTED	0	5	Not available
200.150.64.0/20	ATTENTION Increased Listingrisk	17	40	Not available
---> 200.150.74.0/24	LISTED	11	5	Expressdelisting available
200.150.64.0/21	NOT LISTED	3	25	Not available
200.150.72.0/21	WARNING High Listingrisk	14	25	Not available
200.150.80.0/21	NOT LISTED	0	25	Not available
200.150.80.0/22	NOT LISTED	0	15	Not available
200.150.84.0/22	NOT LISTED	0	15	Not available
200.195.128.0/20	ALERT Extreme Listingrisk	31	40	Not available
---> 200.195.132.0/24	LISTED	7	5	Expressdelisting available
---> 200.195.136.0/24	LISTED	5	5	Expressdelisting available
200.195.128.0/21	WARNING High Listingrisk	16	25	Not available
200.195.136.0/21	WARNING High Listingrisk	15	25	Not available
200.195.144.0/20	NOT LISTED	7	40	Not available
200.195.144.0/21	NOT LISTED	4	25	Not available
200.195.152.0/21	NOT LISTED	3	25	Not available
200.195.160.0/20	ATTENTION Increased Listingrisk	18	40	Not available
---> 200.195.160.0/24	LISTED	7	5	Expressdelisting available
200.195.160.0/21	ATTENTION Increased Listingrisk	11	25	Not available
200.195.168.0/21	ATTENTION Increased Listingrisk	7	25	Not available
200.195.176.0/20	WARNING High Listingrisk	25	40	Not available
200.195.176.0/21	WARNING High Listingrisk	13	25	Not available
200.195.184.0/21	ATTENTION Increased Listingrisk	12	25	Not available

What means listed at UCEPROTECT-Level 2?
UCEPROTECT Network operates three levels of blacklisting, so our users can make the decision how strong they want to filter.
While UCEPROTECT-Level 1 lists single IP's only, UCEPROTECT Level 2 is an escalation list.
According to the table above allocations get listed at Level 2 if there are too many Level 1 listings (spam sending IP's) in that ranges.
Level 2 is basically nothing more than pure mathematics based on the number of Level 1 listed IP's.
To get escalated to Level 2 is almost always an indicator, that you don't act fast enough on spammers.
From our point of view it looks like you did miss to install preventive-measures to keep abusers off your ranges.

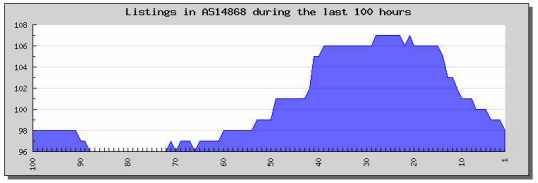
We recommend you should do so by now.
The earlier you start, the faster will your ranges expire from Level 2.

How can our netranges be removed from UCEPROTECT-Level 2?
After you have fixed the problems which caused the escalation, the UCEPROTECT-Level 2 listing will be removed automatically and free of charge as soon as the causal Level 1 listings will expire and decrease below Level 2 escalation limit. Every IP temporary listed at Level 1 expires 7 days after we have seen the last abusive action originating from it.

UCEPROTECT-Level3

Reputation of ASN 14868 | **Companhia Paranaense de Energia - COPEL**

AS	Status	Provider has total IP's	Level 1 listed spammers within the last 7 days	Level 3 Escalation limit by Level 1 records	Optional Expressdelisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
14868	ALERT Extreme Listingrisk	30720	98 (0.319 %)	100	Not available

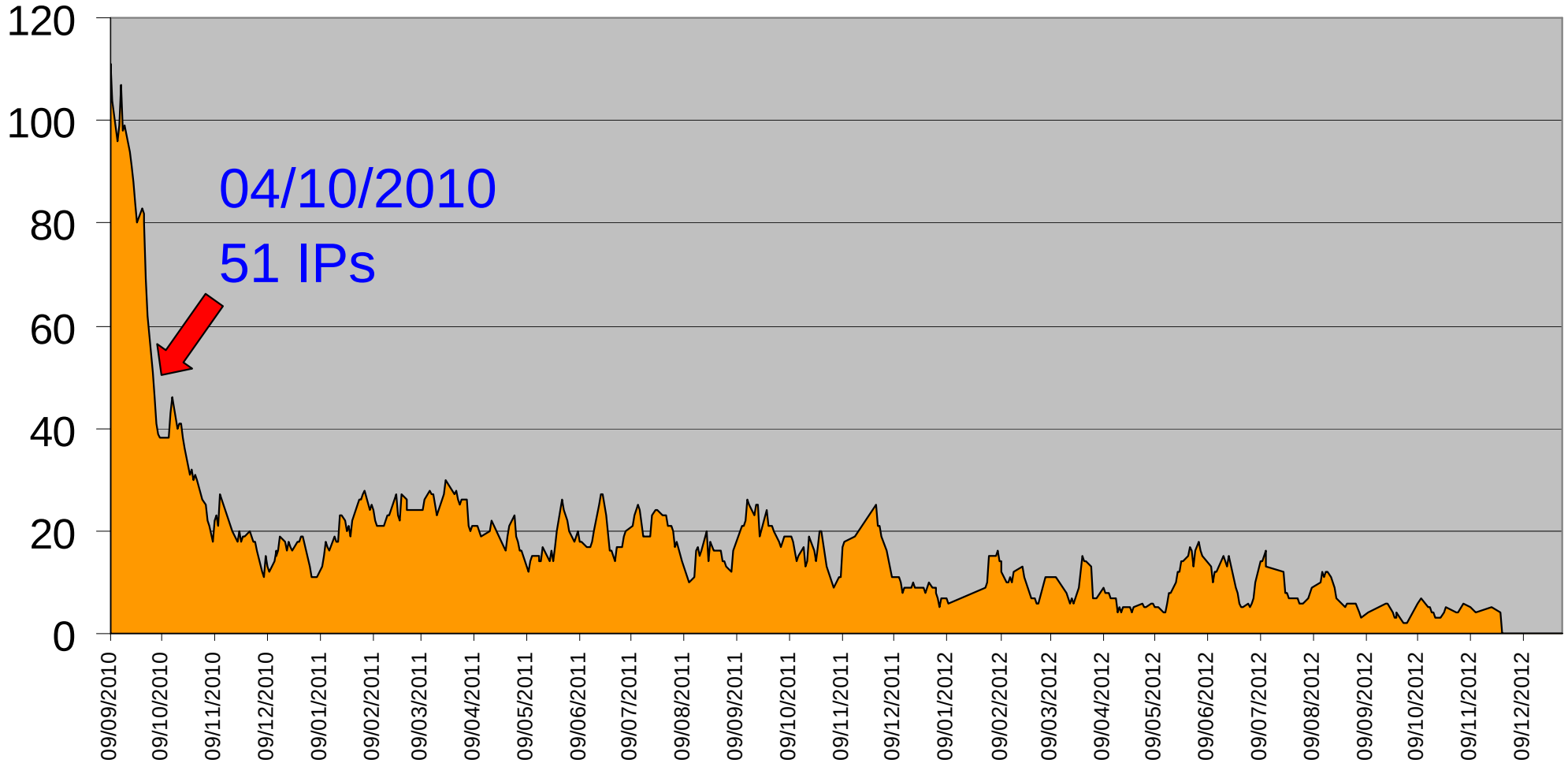


- Em 16/09/2010:
  - IPs listados = 98 (30);
  - Total de IPs = 30720;
  - Percentual= 0,319%;
  - Hits = 1243 (59);
  - Blocos listados = 04 blocos /24 (128 clientes);
  - Vários outros blocos em alerta.

Fonte: UCEPROTECT-NETWORK

Evolução dos IPs listados

Quantidade de IPs listados



THIS INFO IS FOR PROVIDERS. IF YOU ARE ENDUSER PLEASE TEST IP INSTEAD

Informations for AS14868 - Companhia Paranaense de Energia - COPEL

23 Networks are assigned to you.

UCEPROTECT-Level2

Networks of your Allocation

Networks	Status	Level 1 listed spammers within the last 7 days	Level 2 Escalation limit by Level 1 records	Optional Expressdelisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
187.95.96.0/19	NOT LISTED	0	65	Not available
187.95.96.0/20	NOT LISTED	0	40	Not available
187.95.112.0/20	NOT LISTED	0	40	Not available
187.95.126.0/24	NOT LISTED	0	5	Not available
187.95.127.0/24	NOT LISTED	0	5	Not available
200.150.64.0/20	ATTENTION Increased Listingrisk	14	40	Not available
--> *200.150.74.0/24*	LISTED	9	5	Expressdelisting available
200.150.64.0/21	NOT LISTED	4	25	Not available
200.150.72.0/21	ATTENTION Increased Listingrisk	10	25	Not available
200.150.80.0/21	NOT LISTED	0	25	Not available
200.150.80.0/22	NOT LISTED	0	15	Not available
200.150.84.0/22	NOT LISTED	0	15	Not available
200.195.128.0/20	ATTENTION Increased Listingrisk	14	40	Not available
200.195.128.0/21	ATTENTION Increased Listingrisk	8	25	Not available
200.195.136.0/21	NOT LISTED	6	25	Not available
200.195.144.0/20	NOT LISTED	8	40	Not available
200.195.144.0/21	NOT LISTED	6	25	Not available
200.195.152.0/21	NOT LISTED	2	25	Not available
200.195.160.0/20	NOT LISTED	5	40	Not available
200.195.160.0/21	NOT LISTED	1	25	Not available
200.195.168.0/21	NOT LISTED	4	25	Not available
200.195.176.0/20	ATTENTION Increased Listingrisk	10	40	Not available
200.195.176.0/21	NOT LISTED	6	25	Not available
200.195.184.0/21	NOT LISTED	4	25	Not available

What means listed at UCEPROTECT-Level 2?
UCEPROTECT Network operates three levels of blacklisting, so our users can make the decision how strong they want to filter.
While UCEPROTECT-Level 1 lists single IP's only, UCEPROTECT Level 2 is an escalation list.
According to the table above allocations get listed at Level 2 if there are too many Level 1 listings (spam sending IP's) in that ranges.
Level 2 is basically nothing more than pure mathematics based on the number of Level 1 listed IP's.
To get escalated to Level 2 is almost always an indicator, that you don't act fast enough on spammers.
From our point of view it looks like you did miss to install preventive-measures to keep abusers off your ranges.

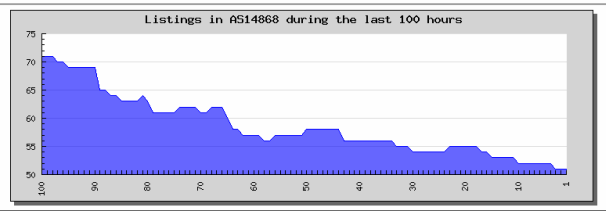
We recommend you should do so by now.
The earlier you start, the faster will your ranges expire from Level 2.

How can our netranges be removed from UCEPROTECT-Level 2?
After you have fixed the problems which caused the escalation, the UCEPROTECT-Level 2 listing will be removed automatically and free of charge as soon as the causal Level 1 listings will expire and decrease below Level 2 escalation limit. Every IP temporary listed at Level 1 expires 7 days after we have seen the last abusive action originating from it.

UCEPROTECT-Level3

Reputation of ASN 14868 | **Companhia Paranaense de Energia - COPEL**

AS	Status	Provider has total IP's	Level 1 listed spammers within the last 7 days	Level 3 Escalation limit by Level 1 records	Optional Expressdelisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
14868	WARNING High Listingrisk	30720	51 (0.166 %) 60 Min.	100	Not available

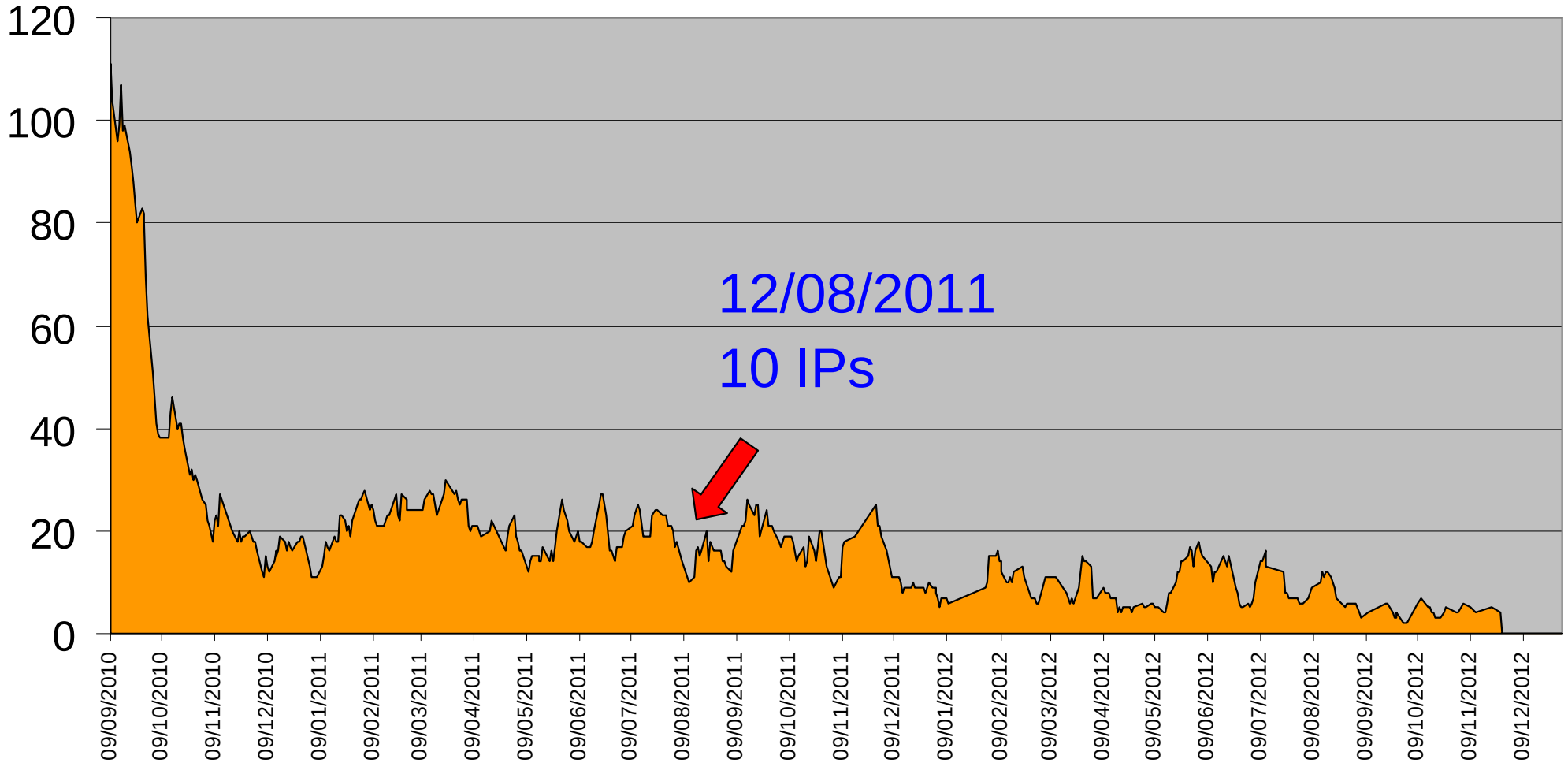


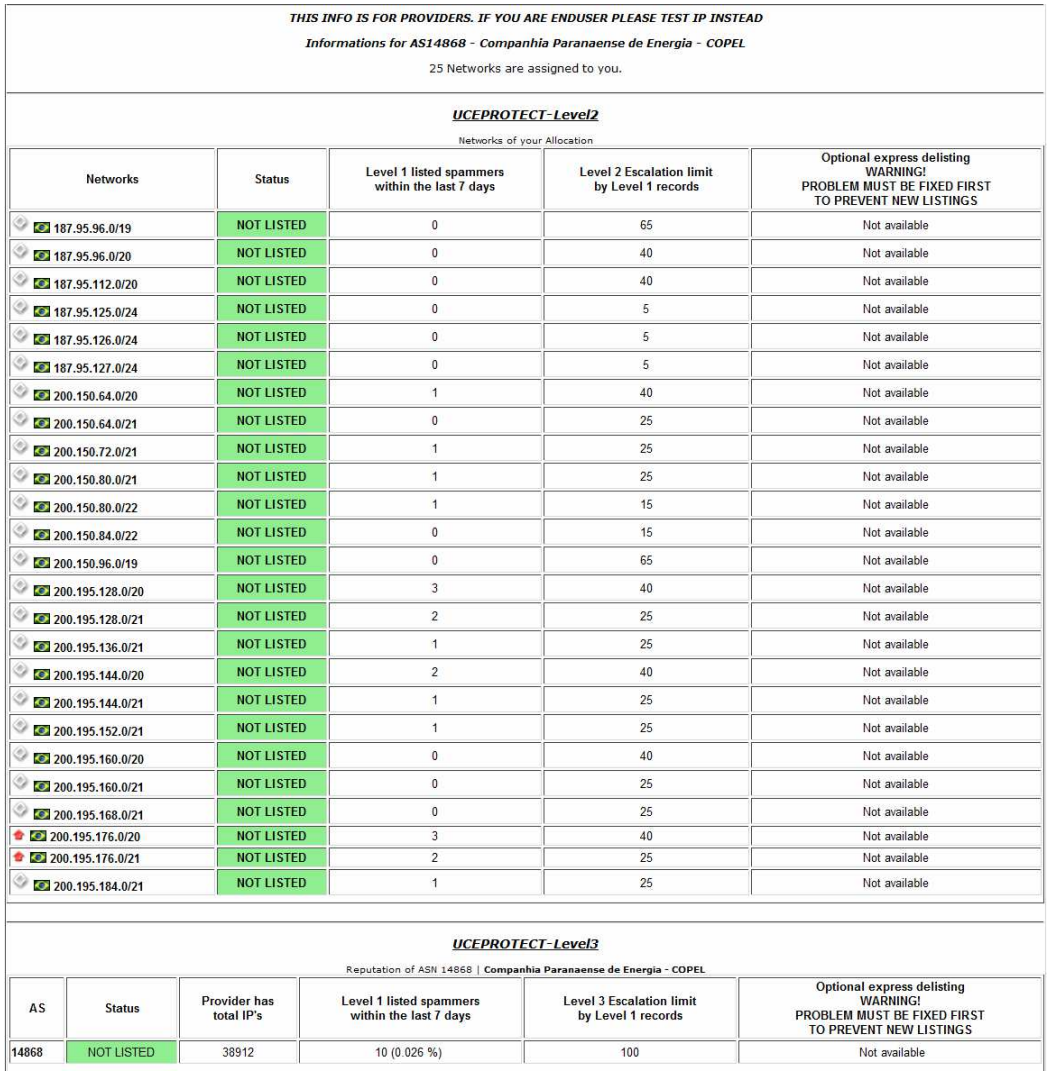
- Em 04/10/2010:
  - IPs listados = 51 (9);
  - Total de IPs = 30720;
  - Percentual= 0,166%;
  - Hits = 399 (65);
  - Blocos listados = 01 blocos /24 (32 clientes);
  - Alguns blocos em alerta.

Fonte: UCEPROTECT-NETWORK

Evolução dos IPs listados

Quantidade de IPs listados





THIS INFO IS FOR PROVIDERS. IF YOU ARE ENDUSER PLEASE TEST IP INSTEAD

Informations for AS14868 - Companhia Paranaense de Energia - COPEL

25 Networks are assigned to you.

UCEPROTECT-Level2

Networks of your Allocation

Networks	Status	Level 1 listed spammers within the last 7 days	Level 2 Escalation limit by Level 1 records	Optional express delisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
187.95.96.0/19	NOT LISTED	0	65	Not available
187.95.96.0/20	NOT LISTED	0	40	Not available
187.95.112.0/20	NOT LISTED	0	40	Not available
187.95.125.0/24	NOT LISTED	0	5	Not available
187.95.126.0/24	NOT LISTED	0	5	Not available
187.95.127.0/24	NOT LISTED	0	5	Not available
200.150.64.0/20	NOT LISTED	1	40	Not available
200.150.64.0/21	NOT LISTED	0	25	Not available
200.150.72.0/21	NOT LISTED	1	25	Not available
200.150.80.0/21	NOT LISTED	1	25	Not available
200.150.80.0/22	NOT LISTED	1	15	Not available
200.150.84.0/22	NOT LISTED	0	15	Not available
200.150.96.0/19	NOT LISTED	0	65	Not available
200.195.128.0/20	NOT LISTED	3	40	Not available
200.195.128.0/21	NOT LISTED	2	25	Not available
200.195.136.0/21	NOT LISTED	1	25	Not available
200.195.144.0/20	NOT LISTED	2	40	Not available
200.195.144.0/21	NOT LISTED	1	25	Not available
200.195.152.0/21	NOT LISTED	1	25	Not available
200.195.160.0/20	NOT LISTED	0	40	Not available
200.195.160.0/21	NOT LISTED	0	25	Not available
200.195.168.0/21	NOT LISTED	0	25	Not available
200.195.176.0/20	NOT LISTED	3	40	Not available
200.195.176.0/21	NOT LISTED	2	25	Not available
200.195.184.0/21	NOT LISTED	1	25	Not available

UCEPROTECT-Level3

Reputation of ASN 14868 | **Companhia Paranaense de Energia - COPEL**

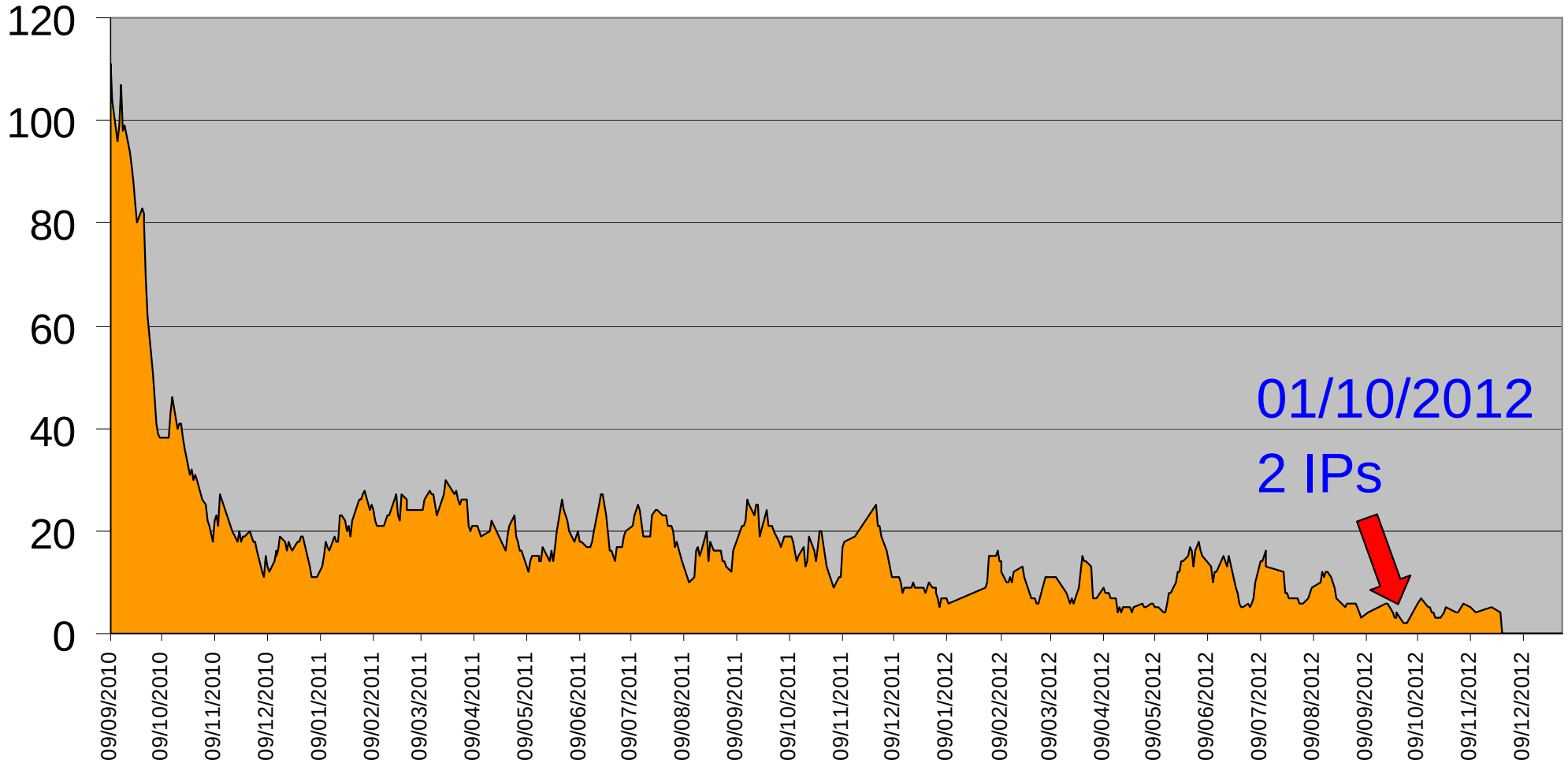
AS	Status	Provider has total IP's	Level 1 listed spammers within the last 7 days	Level 3 Escalation limit by Level 1 records	Optional express delisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
14868	NOT LISTED	38912	10 (0.026 %)	100	Not available

- Em 12/08/2011:
  - IPs listados = 10;
  - Total de IPs = 38912;
  - Percentual= 0,026%;
  - Hits = 127 (70);
  - Todos os blocos estavam limpos.

Fonte: UCEPROTECT-NETWORK

Evolução dos IPs listados

Quantidade de IPs listados



THIS INFO IS FOR PROVIDERS. IF YOU ARE ENDUSER PLEASE TEST IP INSTEAD

Informations for AS14868 - Companhia Paranaense de Energia - COPEL

22 Networks are assigned to you.

UCEPROTECT-Level2

Networks of your Allocation

Networks	Status	Level 1 listed spammers within the last 7 days	Level 2 Escalation limit by Level 1 records	Optional express delisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
187.95.96.0/19	NOT LISTED	0	65	Not available
187.95.96.0/20	NOT LISTED	0	40	Not available
187.95.112.0/20	NOT LISTED	0	40	Not available
200.150.64.0/20	NOT LISTED	1	40	Not available
200.150.64.0/21	NOT LISTED	1	25	Not available
200.150.72.0/21	NOT LISTED	0	25	Not available
200.150.80.0/21	NOT LISTED	0	25	Not available
200.150.80.0/22	NOT LISTED	0	15	Not available
200.150.84.0/22	NOT LISTED	0	15	Not available
200.150.96.0/19	NOT LISTED	0	65	Not available
200.195.128.0/20	NOT LISTED	1	40	Not available
200.195.128.0/21	NOT LISTED	0	25	Not available
200.195.136.0/21	NOT LISTED	1	25	Not available
200.195.144.0/20	NOT LISTED	0	40	Not available
200.195.144.0/21	NOT LISTED	0	25	Not available
200.195.152.0/21	NOT LISTED	0	25	Not available
200.195.160.0/20	NOT LISTED	0	40	Not available
200.195.160.0/21	NOT LISTED	0	25	Not available
200.195.168.0/21	NOT LISTED	0	25	Not available
200.195.176.0/20	NOT LISTED	0	40	Not available
200.195.176.0/21	NOT LISTED	0	25	Not available
200.195.184.0/21	NOT LISTED	0	25	Not available

UCEPROTECT-Level3

Reputation of ASN 14868 | **Companhia Paranaense de Energia - COPEL**

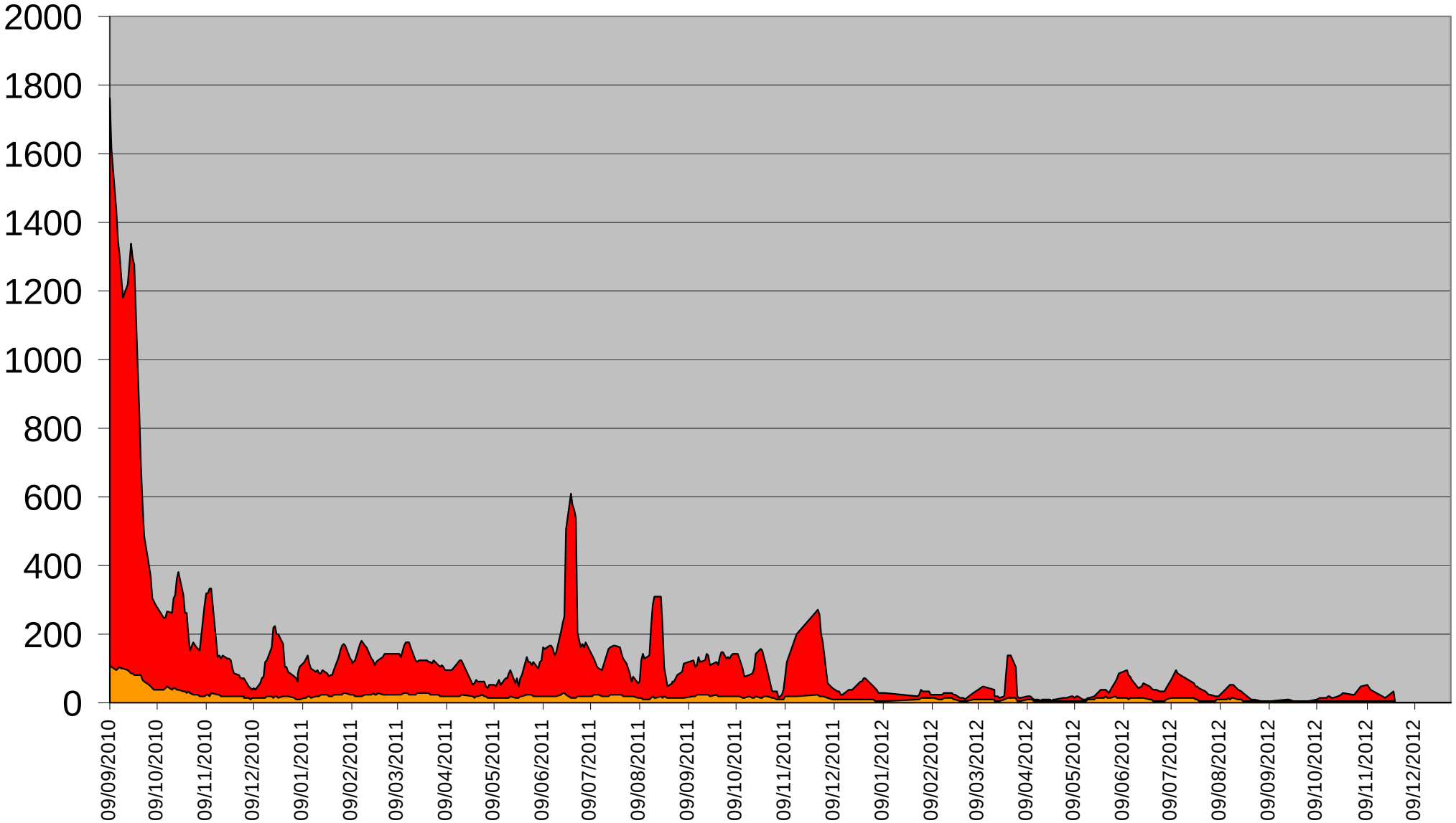
AS	Status	Provider has total IP's	Level 1 listed spammers within the last 7 days	Level 3 Escalation limit by Level 1 records	Optional express delisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
14868	NOT LISTED	38912	2 (0.005 %)	100	Not available

Em 01/10/2012:

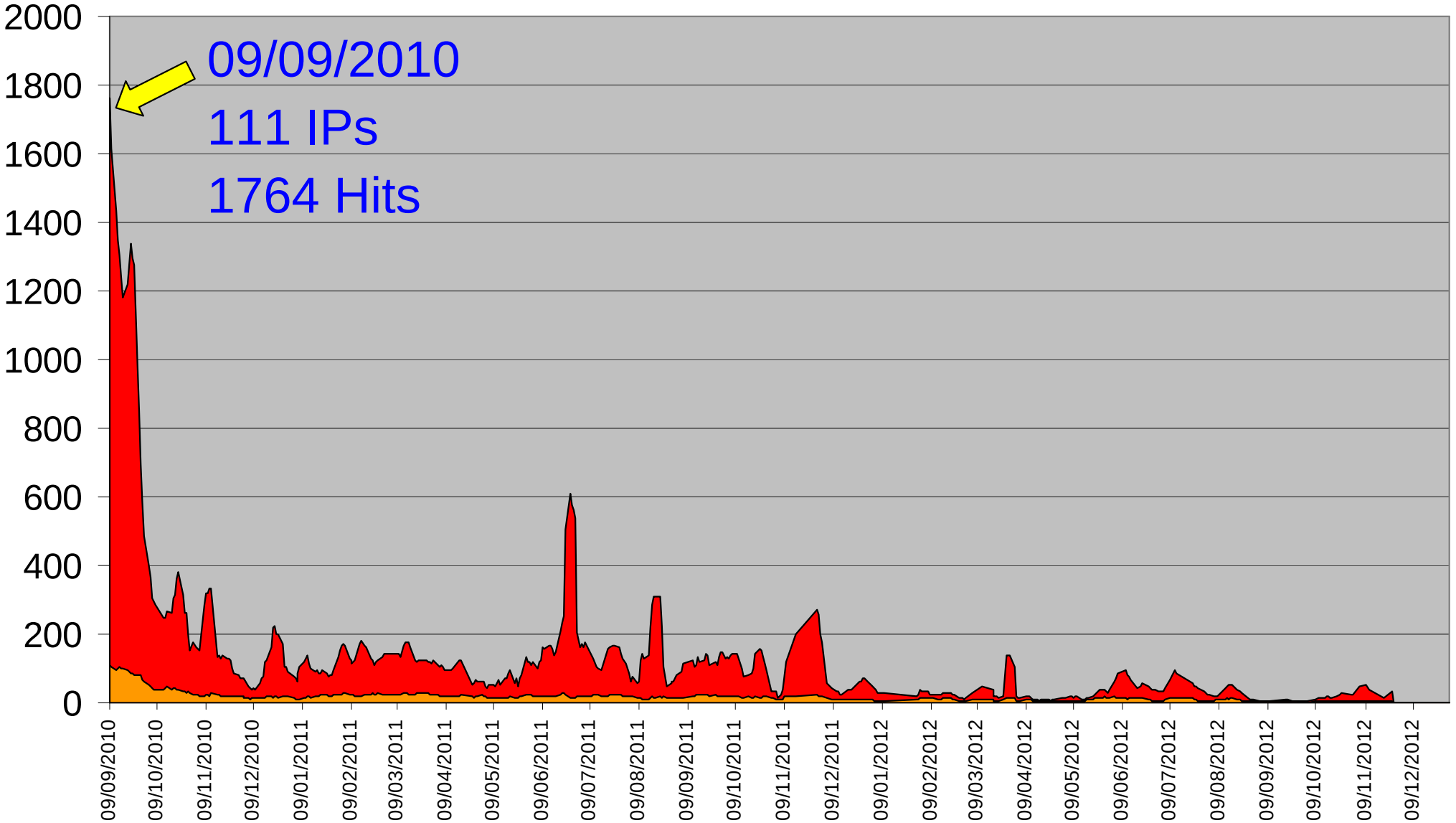
- IPs listados = 2;
- Total de IPs = 38912;
- Percentual= 0,005%;
- Hits = 3 (2);
- Todos os blocos estavam limpos;
- Clientes com servidores liberados.

Fonte: UCEPROTECT-NETWORK

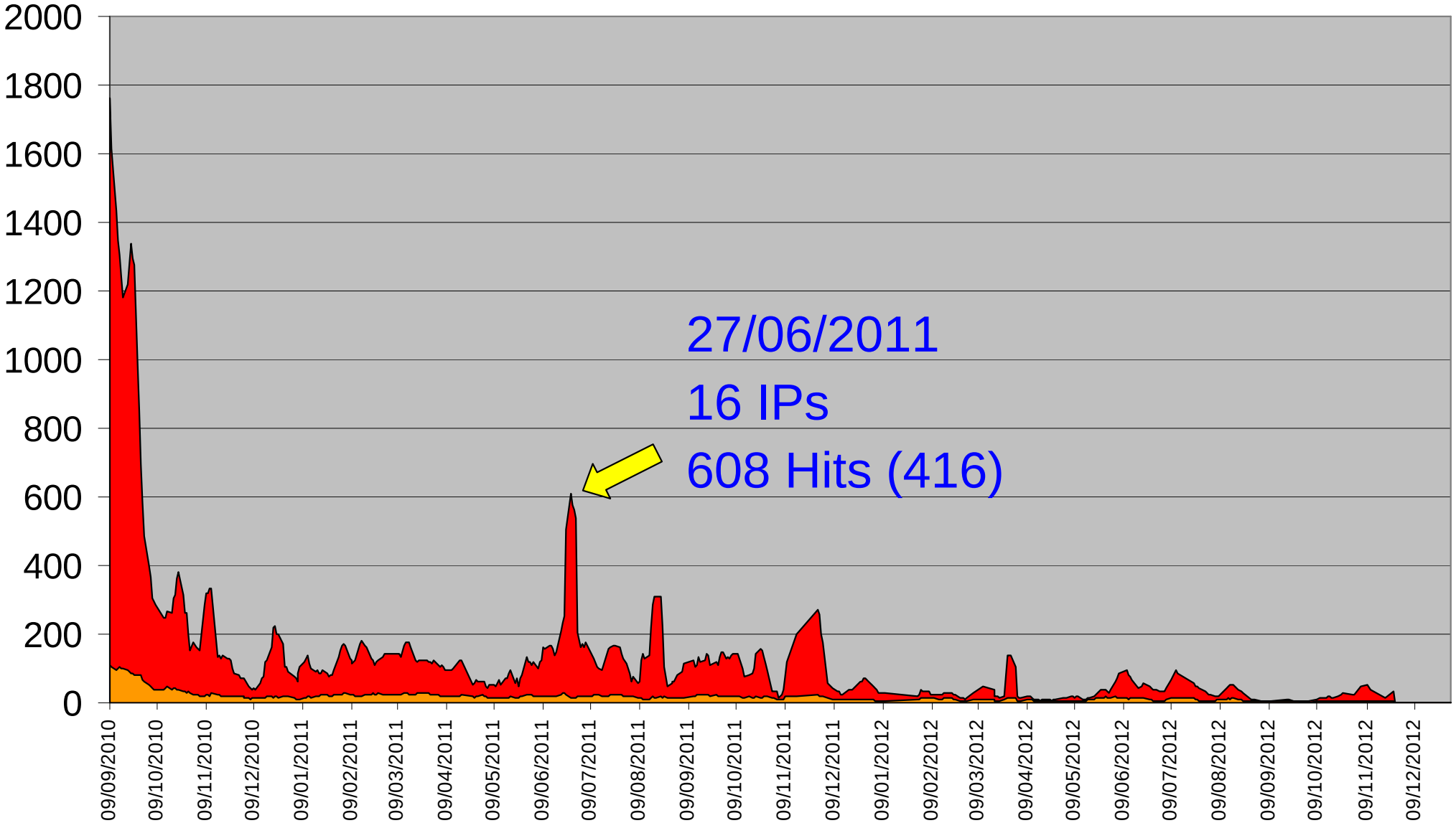
IPs listados e Hits



IPs listados e Hits



IPs listados e Hits



COPEL
Pura Energia

PARANÁ
GOVERNO DO ESTADO

CENÁRIO - 2012

Cenário - 2012

- Cenário até novembro de 2012:
  - Ordens de serviço (OS):
    - Configurar ou alterar o IP de servidor de *e-mail*;
    - Configurar ou alterar o DNS Reverso.
  - Todos os nossos blocos de IPs estão limpos;
  - Alguns IPs estão sendo listados porque são servidores de *e-mail* e tem seus IPs liberados em nosso filtro.

	16/09/2010	07/12/2012	Percentual (%)
Nível 1 (IPs)	3.150.812	780.466	24,77
Nível 2 (Blocos)	27.919	10.793	38,66
Nível 3 (ASNs)	788	264	33,50

Fonte: UCEPROTECT-NETWORK

CONSIDERAÇÕES FINAIS

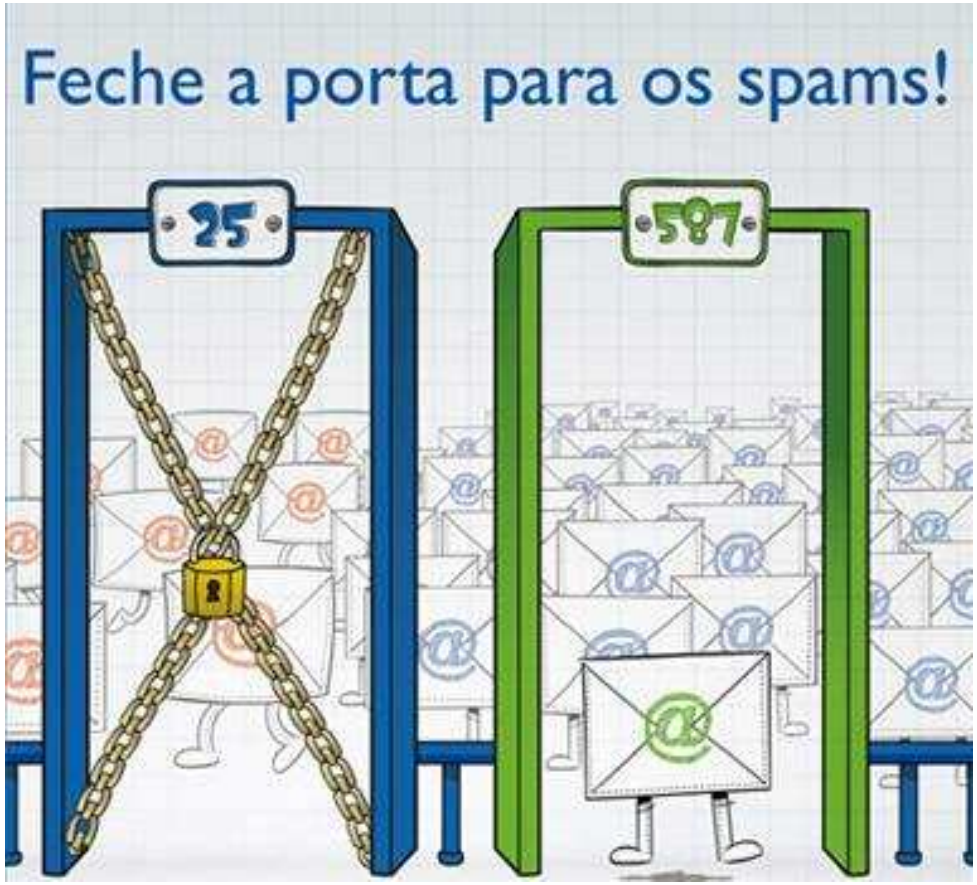
- O filtro da porta 25 é simples. As dificuldades foram:
  - Definição dos procedimentos;
  - A efetiva aplicação;
  - Manutenção.
- Nossos clientes conseguem enviar *e-mails* e não estão sendo mais punidos pelas *blacklists;*
- Incentivamos nossos clientes a utilizar a porta 587(TCP):
  - Essa medida não elimina totalmente o problema de envio de *spams*;
  - Exigência de autenticação, o *spammer* deixa de ser “anônimo”.
- Proteção dos nossos blocos de endereçamento IP;
- Contribuição para a diminuição de *spams;*
- Vários outros provedores tem adotado medidas semelhantes;
- A aplicação do filtro da porta 25 foi um sucesso.

Referências

- ANTISPAM.BR. **Prevenção**. ANTISPAM.BR. 2012. Disponível em: <http://antispam.br/prevencao/filtros/>. Acesso em: 12 nov. 2012

- CERT.BR. **Spam e fraudes**: Técnicas de mitigação para administradores de redes. CERT.BR. SSI. 2006. Disponível em: <http://www.cert.br/docs/palestras/certbr-ssi2006-2.pdf>. Acesso em: 12 nov. 2012

Compre essa idéia!



Saiba mais em www.antispam.br

Fonte: ANTISPAM.BR

Agradecimentos

- CGI.br e NIC.br
- II Semana da Infraestrutura da Internet no Brasil:
  - GTER 34 / GTS 20.
- Centro de Operações de Telecomunicações (COT) da COPEL:
  - Divisão de Ativação de Configuração;
  - Divisão de Monitoração e Suporte;
  - Divisão de Engenharia de Operação e Manutenção.
- Departamento de Engenharia de Redes e Serviços IP:
  - Divisão de Engenharia de Redes IP.

Giovani Colombo
gcolombo@copel.com

Joelson Tadeu Vendramin
joelson.vendramin@copel.com

http://www.copeltelecom.com

COPEL
Pura Energia

PARANÁ
GOVERNO DO ESTADO

Obrigado!!!