Praticas Anti-Spam para ISPs

Diogo Corteletti de Oliveira

diogo_c@brturbo.com.br

Motivação

- Crescimento exponencial do SPAM.
- Escalada dos prejuízos causados a empresas.
- Falta de padrão para o combate a SPAM por ISPs.
- Profissionalização dos SPAMMERS.
- SPAM a serviço do crime cibernético.

Objetivos

- Definir boas práticas que podem ser seguidas pelos provedores de serviço da Internet para combate a atividade de SPAM através de Blacklists, Monitoração e controle do fluxo de e-mail em suas redes.

- Melhor utilização dos recursos computacionais envolvidos na Internet.

- Evitar prejuízos devido ao trafego de SPAM.

Papai-Noel

- Primeiro alvo de SPAMMERS.

- Recebia SPAM antes mesmo do e-mail existir.

Problemas com SPAM

-Hoje é estimado que 40% do trafego de e-mail se trata de SPAM e os prejuízos calculados nos Estados Unidos devido a prática chega a marca de 8.9 Bilhões de Dólares.
(Fonte: http://www.spamfilterreview.com)

-Os perpetradores estão se profissionalizando e dificultando cada vez mais sua detecção e combate.

-Um dos grandes problemas que facilita a prática de SPAM é a falta de mecanismos para detecção do usuário que envia o Comando "MAIL FROM:" para o servidor (RFC-821).

-Existem sites na Internet que vendem serviço de SPAM publicamente.

SpamVertise

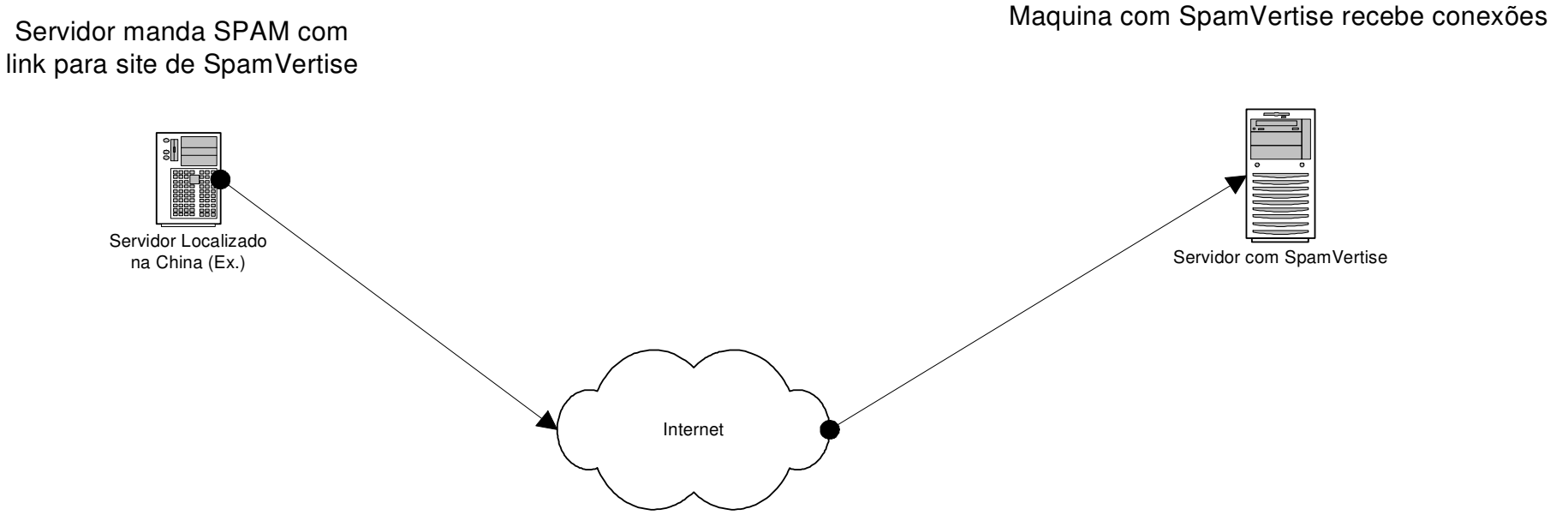
- É a promoção de sites comercias através do envio de SPAM.

- Relacionado a prática de IP Hijacking.

- Pode ser usado para pratica de Joe-Job.

Técnicas de SPAMMERS

-Envio de SPAM por servidores localizados em países como a China com links para SpamVertise que pode estar localizado em qualquer servidor no mundo.



SPAM a serviço do crime

- SPAM com conteúdo associado a pedofilia

- Fraude Bancaria.

- Tentativa de furto de informações pessoais

Estatísticas do SPAM no Brasil

- Em três meses houve um crescimento de 39,7% no número de reclamações ao NBSO.

- Do total de reclamações mais de 30% são de Open Proxy.

		SpamCop				
Mês	**Total**	**Spamvetised**	**Proxy**	**Relay**	**Outras**	**Outras Fontes**
Abr	322.614	19,68%	42,08%	0,04%	24,94%	13,27%
Mai	385.401	30,78%	35,18%	0,04%	22,46%	11,55%
Jun	450.560	36,77%	30,36%	0,03%	23,30%	9,55%
Total	1.158.575	30,02%	35,22%	0,03%	23,47%	11,25%

(Fonte: http://www.nbso.nic.br)

PUA – (Política de Uso Aceitável)

- Dentro da PUA do provedor deve estar especificado que é Proibido o uso dos recursos de sua rede para SPAM e Atividades relacionadas.

- É o documento que ampara ações contra usuários Maliciosos.

- Deve ser redigido em conjunto com o Departamento Jurídico.

Sistema Centralizado de Identificação de usuários

- Grande número de IPs alocados a um Provedor.

- Caráter dinâmico do "leasing".

- Correlacionamento com reclamações que contenham IP e Hora.

- Precisa possuir controle de acesso e os dados só devem ser fornecidos a terceiros via mandado Judicial.

- Comitê Gestor da Internet recomenda 3 anos de guarda.

Práticas

- Uso de Blacklists.

- Scans por Open Proxy e Open Relay

- Posicionamento de Relays (Gateways de e-mail) na planta.

- Análise e tratamento de reclamações via e-mail.

- Sistema correlacionador de eventos.

Blacklists

- São entidades que fazem listas de IPs que tenham praticado SPAM ou atividade relacionada.

-Surgiram devido a demanda por algum mecanismo que identificasse usuários infratores.

- Não bloqueiam IP.

- Cada pessoa é livre para usar a lista para bloqueio.

Blacklists

- Existem milhares de Blacklists na Internet, onde cada uma tem autonomia para listar o que bem entender.

- Pode bloquear trafego legítimo de e-mail.

- É interessante manter contato com as blacklists mais usadas.

- Pode servir como fonte informante para consulta aos Blocos do AS do provedor que estejam listados.

Blacklists

- www.spamhaus.org (ROCKSO list)
- www.spamcop.net
- www.sorbs.net
- www.senderbase.org (não é blacklist)

Scans por Open Proxys/Relays

- Open Proxys/Relays são servidores configurados para servir como "Gateway" de conexão de terceiros para terceiros.

- Podem e são usados para SPAM, escondendo a identidade do verdadeiro SPAMMER.

- No brasil mais que 30% das reclamações de SPAM são de Open Proxy.

Scans por Open Proxys/Relays

- O Scan tem por objetivo identificar na rede usuários que possuam servidores com má configuração.

- Deve ser feito nas portas padrão.

- Pela possibilidade de ser considerada uma prática abusiva é necessário amparo Judicial e deve constar no contrato de prestação de serviço do Provedor.

-Existem na Internet várias ferramentas para a execução do scan.

Scans por Open Proxys/Relays

Web-based Proxy Checkers

Advanced Proxy Checker - www.astalavista.net/new/network.php?cmd=proxy - only HTTP
P r o x y s c a n n e r - www.fr2.cyberabuse.org/?page=proxyscanner - self-testing. down?
Open proxy check - www.richard.zonnet.nl/cgi-bin/nph-proxycheck - self-testing
Hatcheck - hatcheck.org/proxy/, www.ghost.ru - temporarily (?) down

Script Proxy Checkers

SocksCap and Socks Perl Scripts - www.socks.nec.com/cgi-bin/download.pl - Win, Perl
proxycheck - www.corpit.ru/mjt/proxycheck.html - *nix
pxytest - www.unicom.com/sw/pxytest/ - Perl
Blitzed Open Proxy Monitor - blitzed.org/bopm/ - with IRCd. Whitelisting plugin: www.nedworks.org/bopm/
DSBL Test Program Suite - dsbl.org/programs - *nix
YAPH - yaph.sourceforge.net - *nix
SORBS - sorbs.sourceforge.net - checks incoming servers for open relays and proxies
ScanSSH - www.monkey.org/~provos/scanssh/ - *nix
ProxyBuster - www.fi.uu.nl/~ftu/proxybuster/ - *nix

Posicionamento estratégico de Relays

- Tem como alvo o usuário residencial.

- Deve ser a única maneira de saída pela porta 25 para estes usuários.

- Serve de limitador do número de e-mails por sessão.

- Impede que o usuário utilize Open Relay da Internet.

- Pode ter solução de baixo custo.

- Contrato de prestação de serviço tem que estar de acordo.

Uso das caixas de e-mail abuse e spam

- Tem como objetivo receber reclamações de usuários e entidades.

- Caixa "abuse" é sugerida pela RFC-2142.

- É interessante disponibilizar a caixa spam@provedor .

- Reclamações referentes a SPAM devem ser coletadas dessas duas caixas

-As caixas podem ser tratadas via "script" caso o numero De reclamações seja muito grande.

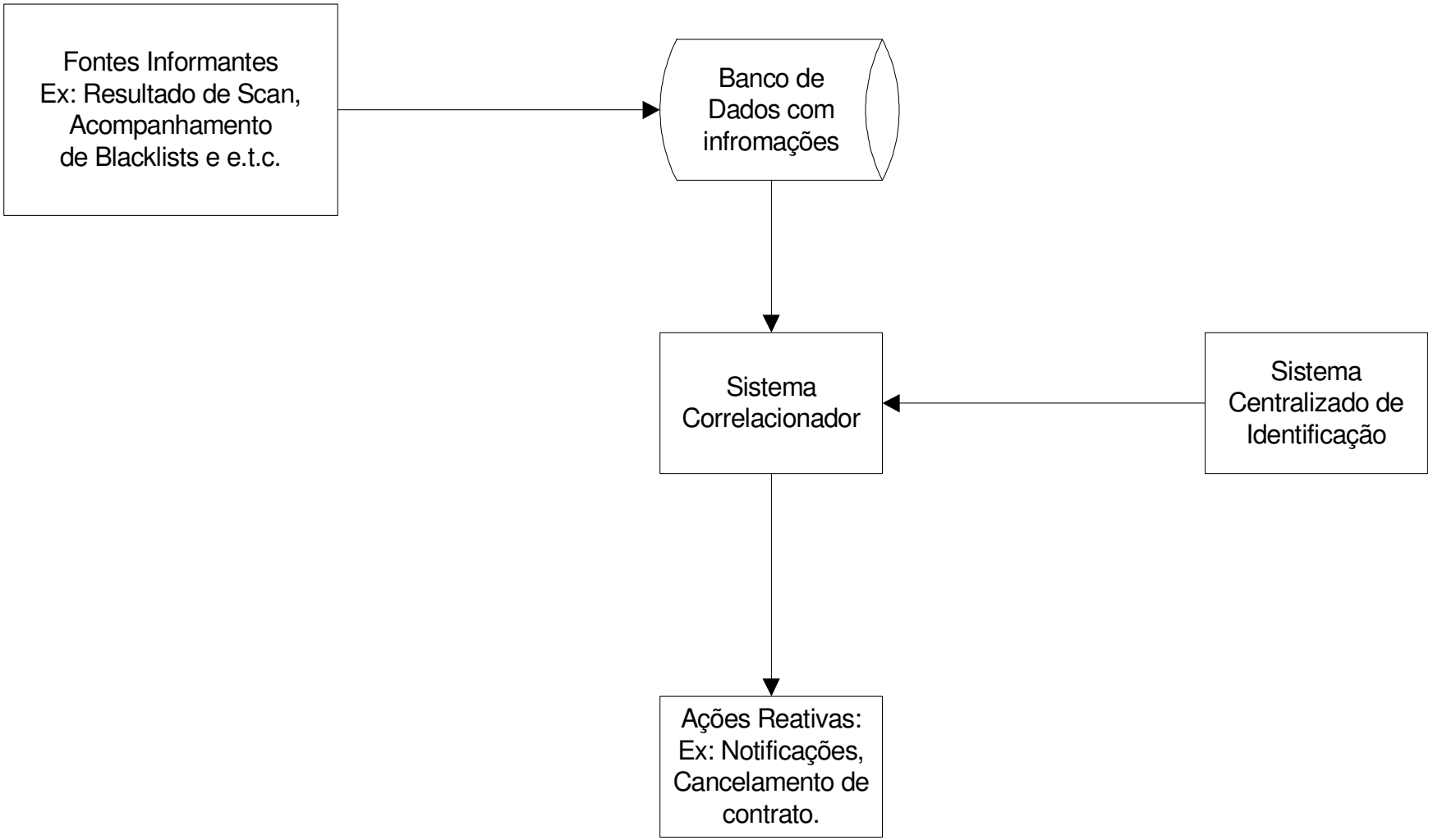
Sistema de Correlação

- Faz-se necessário devido ao fluxo de informações proveniente das fontes informantes e devido a redundância de dados.

- Tem o propósito de relacionar um usuário à atividade de SPAM para que o mesmo possa ser notificado e/ou instruído.

- Deve estar relacionado as Fontes Informantes e ao Sistema Centralizado de Identificação de Usuários.

Fluxo de Identificação e Notificação



Notificação

Caro Sr. <Nome do usuário>
Informamos que o(s) IP(s) <IP(s) notificado(s)> - alocado(s) para o
cliente <Nome do cliente >, estão relacionados a <Tipo de Incident

Segue em anexo a este email – em formato XML - evidências dest
relacionadas a <Tipo de Incidente>.

Desta forma, solicitamos a gentileza de verificar a configuração do
servidores de forma a interromper tal prática.
Atenciosamente,
<Nome da Empresa>

Obs: É interessante enviar o anexo com evidências em format

SPF - (Sender Policy Framework) e Sender ID

- SPF tem como objetivo criar uma lista de servidores que são confiáveis para envio de e-mail através da checagem via DNS.

- Sender ID tem uma abordagem parecida mas checa o usuário (Iniciativa da Microsoft).

- Também são soluções paleativas.

- De acordo com o site http://www.theregister.co.uk passam 30% a mais de e-mail pelo SPF do que pelo caminho normal.

Conclusão

- É essencial para a longevidade do e-mail combater o SPAM.

- Nada é 100% seguro e o SPAM nunca vai acabar.

- Com o uso das práticas descritas certamente o número de e-mails que constituem SPAM diminuíram consideravelmente a níveis administráveis e os prejuízos devido a prática serão menores.

O bom SPAM

OBRIGADO

Perguntas?