Vizinhanças ou condomínios: uma análise da origem de *spams* com base na organização de sistemas autônomos

Osvaldo Fonseca[1], Pedro Henrique B. Las-Casas[1], Elverton Fazzion[1], Dorgival Guedes[1], Wagner Meira Jr.[1], Cristine Hoepers[2], Klaus Steding-Jessen[2], Marcelo H. P. Chaves[2]

[1] Departamento de Ciência da Computação
Universidade Federal de Minas Gerais

[2]CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
NIC.br - Núcleo de Informação e Coordenação do ponto BR

{osvaldo.morais,pedro.lascasas,elverton,dorgival,meira}@dcc.ufmg.br

{cristine,jessen,mhp}@cert.br

Abstract. *Despite the continuous efforts to mitigate spam, the volume of messages is huge and identifying spammers is still a challenge. Spam traffic analysis has been performed to determine the behavior of spammers, who are employing techniques more and more sophisticated to disseminate messages. This work analyzes the sources of spam towards understanding to what extent they explain the traffic. Our results show that, beyond a similar behavior among machines from the same autonomous system (AS), it is possible to separate them according to their sending characteristics. Further, the results also show that we may apply the concept of Internet BadNeighborhoods to ASes, once the machines from a given AS behave similarly.*

Resumo. *Apesar dos esforços contínuos para combater o envio de spam, o volume de mensagens enviadas é muito grande e a identificação dos responsáveis ainda é uma tarefa muito difícil. Análises do tráfego de mensagens de spam têm sido realizadas para determinar o comportamento dos spammers, que têm utilizado técnicas cada vez mais sofisticadas na disseminação dessas mensagens. Este trabalho analisa a origem dos remetentes das mensagens de spam visando entender sua influência sobre o tráfego de spam propagado pela rede. Nossos resultados mostram que, além de existir um comportamento semelhante entre as máquinas provenientes de um mesmo sistema autônomo (AS), é possível dividi-los em grupos de acordo com suas características de envio de spam. Além disso, os resultados mostram que podemos aplicar o princípio de Internet BadNeighborhoods a ASes, uma vez que as máquinas de um mesmo AS apresentam comportamento semelhante.*

1. Introdução

Nas últimas duas décadas houve um aumento muito grande na utilização da Internet, o que levou a um aumento dos problemas relacionados ao envio de *spam* em proporções ainda maiores. Além do grande volume de dados gerado, uma vez que os provedores de serviços de correio eletrônico estimam que entre 40% e 80% das mensagens

eletrônicas são mensagens de *spam*, muitas vezes elas estão relacionadas ao envio de *phishing* [Orman 2013] e propagação de *malware* [Newman et al. 2002]. Por causa desses fatores, os prejuízos gerados pelo tráfego de *spam* são estimados na ordem de bilhões de dólares [Sipior et al. 2004].

A batalha contra os *spammers* se trava em diversas frentes. Muito já foi feito no sentido de desenvolver filtros baseados no conteúdo da mensagem, definindo regras para identificar os padrões de ofuscação observados nas mensagens de *spam* [Guerra et al. 2010]. Nos últimos anos, muitos esforços têm focado no entendimento do tráfego de *spam* dentro da rede, a fim de levantar elementos que possam ser usados para identificar as máquinas que enviam as mensagens antes que estas percorram a rede e consumam recursos dos servidores de correio no destino. Este trabalho se encaixa nesta linha, analisando onde se encontram as máquinas usadas pelos *spammers*.

Recentemente, o termo *Internet Bad Neighborhoods* (vizinhanças ruins) foi criado para identificar faixas contíguas do espaço de endereçamento IP que contenham um número significativo de máquinas com comportamento indesejado [van Wanrooij and Pras 2010]. O princípio por trás do conceito original seria que redes, que compartilham um prefixo IP, contendo muitas máquinas com tal comportamento sugeririam uma rede com problemas. Posteriormente, o conceito foi estendido para se referir a segmentos de rede que emanam tráfego indesejado, independente do número de máquinas envolvidas [Moreira Moura et al. 2011].

Nossa análise parte de princípios semelhantes, porém escolhemos o nível dos Sistemas Autônomos (ASes, *Autonomous Systems*) para identificar possíveis *bad neighborhoods*. Sistemas Autônomos, por natureza, identificam faixas do espaço de endereço IP sob o controle de uma única entidade, responsável por definir políticas de uso, roteamento e procedimentos administrativos que serão aplicados a todas as máquinas instaladas naquele espaço. Nesse sentido, dois endereços IP pertencentes a um mesmo AS teriam uma chance muito maior de exibirem comportamentos semelhantes que dois endereços IP em sub-redes com endereços adjacentes (no espaço IP), mas pertencentes a ASes distintos. Afinal, um AS com falhas de segurança em suas políticas torna-se uma potencial *Bad Neighborhood*, pois a probabilidade das máquinas pertencentes àquele AS ficarem comprometidas e começarem a enviar *spam* é elevada.

Nossos dados contêm tráfego de *spam* coletado em diversos pontos do globo. Ao agrupar as máquinas que geram esse tráfego com base em seus ASes de origem podemos criar um perfil do comportamento de cada sistema autônomo observado durante a coleta. Nossos resultados mostram que a maior parte das máquinas que enviam *spam* se concentra realmente em alguns ASes e que apenas 15 deles são responsáveis por mais de 80% do tráfego observado. Ao utilizar técnicas de mineração de dados sobre esse material, observamos que há semelhanças entre algumas delas, sendo possível agrupá-las em quatro categorias representativas de ASes do ponto de vista de seu papel na distribuição de *spam*. Essa constatação constitui uma das principais contribuições deste trabalho, uma vez que, até então, era comum supor que haveria apenas dois tipos de geradores de *spam*: transmissores "leves" e "pesados" (LVS, de *low-volume spammers* e HVS, de *high-volume spammers*) [Pathak et al. 2008]. Nossa caracterização indica que, além de más vizinhanças, onde o mau comportamento (envio de *spam*) é bastante comum entre as máquinas de um AS, há também boas vizinhanças, onde tal comportamento é raro, normalmente desapa-

recendo rapidamente logo após seu surgimento em uma ou outra máquina, e vizinhanças coniventes, onde não se observa o mau comportamento como algo generalizado, mas limitado a apenas algumas máquinas, que por sua vezes são transmissores pesados.

2. Trabalhos Relacionados

A definição de *Bad Neighborhoods*, apresentada na introdução, é devida a van Wanrooij e Pras [2010], que propõem o conceito como uma extensão do uso de *blacklists* na detecção de *spam*. Naquele trabalho, cada um dos prefixos de 24 bits de endereçamento IP (/24) seria uma vizinhança e vizinhanças ruins seriam aquelas com um grande número de máquinas enviando *spam*. Moreira Moura et al. [2011] focam na análise dessas vizinhanças e estendem a definição para incluir redes com poucos IPs transmissores, mas com um alto volume de tráfego, seguindo a classificação de transmissores "pesados" e "leves" proposta anteriormente por Pathak, Hu e Mao [2008]. Neste trabalho, consideramos cada AS como sendo uma vizinhança, pois um sistema autônomo é naturalmente uma boa forma de definir a área de cada vizinhança, uma vez que existe para cada AS uma gerência única e uma política de roteamento comum a todas as máquinas.

Muitos trabalhos avaliam o tráfego de *spam* a partir de mensagens coletadas nos servidores de correio de destino. Gomes et al. [2005] têm como objetivo encontrar características que podem ser usadas para separar mensagens legítimas de mensagens de *spam*, e o trabalho utiliza apenas um ponto específico da rede na coleta. Neste trabalho, as mensagens de *spam* são coletadas por *honeypots* de baixa interatividade instalados em 10 países diferentes e localizados em redes intermediárias. Isso nos permite ter uma visão mais global do tráfego de *spam*, além de oferecer uma perspectiva diferente.

Kokkodis and Faloutsos [2009] mostram alguns resultados que indicam que as atividades de *botnets* estão espalhadas no endereçamento IP, reduzindo a eficácia dos filtros *anti-spam* e dificultando o trabalho dos administradores das redes. O nosso trabalho, apesar de confirmar a existência de *spammers* em um número muito grande de redes, mostra que a maior parte das mensagens de *spam* são provenientes de um número pequeno de ASes, resultado que pode ser usado no desenvolvimento de novas técnicas para a detecção de *spam*.

Las-Casas et al. [2013] realizam uma análise detalhada do tráfego de mensagens de *spam*, que oferece uma visão geral sobre o tráfego e mostra as diferenças existentes entre os pontos de coleta utilizados, por um período de 3 meses. Neste trabalho, coletamos mensagens de *spam* durante um período de aproximadamente um ano, permitindo uma análise mais abrangente do tráfego de *spam*. Além disso, aprofundamos os estudos sobre os sistemas autônomos, a fim de entender melhor a origem dos remetentes das mensagens de *spam*.

3. Metodologia

Para coletar a base de dados utilizada no trabalho, foram usados doze *honeypots* de baixa interatividade [Steding-jessen et al. 2007] instalados em dez países: dois no Brasil, dois nos Estados Unidos e um coletor em cada um dos seguintes países: Argentina, Austrália, Áustria, Equador, Holanda, Taiwan, Noruega e Uruguai. Pode-se notar que temos coletores presentes em vários continentes, permitindo ao estudo uma visão mais global do tráfego de mensagens de *spam*. Com isso, eliminamos alguns problemas presentes em

vários trabalhos encontrados na literatura, cujos dados utilizados vêm de um único coletor. Além disso, nenhum dos coletores utilizados na análise apresentou indício de ter sido alvo de algum ataque específico e a possibilidade de *spoofing* é reduzida no caso de conexões estáveis, pois seria necessário interceptar a rota de retorno dos pacotes.

Os *honeypots* usados no trabalho são coletores que simulam servidores vulneráveis, como *open relays* SMTP e *proxies* abertos HTTP e SOCKS. Seu objetivo é exatamente capturar as mensagens de *spam* enviadas por *spammers* que vêem um coletor como uma máquina vulnerável, que pode ser abusada a fim de usá-la para a entrega de mensagens. Na prática, o coletor não entrega as mensagens de *spam* aos destinatários pretendidos; ao invés disso, elas são armazenadas localmente. O comportamento dos *honeypots*, entretanto, é configurado para levar o *spammer* a crer que a entrega está funcionando corretamente. As mensagens são periodicamente recolhidas por um sistema de coleta.

Junto com cada mensagem recebida são armazenadas informações adicionais obtidas pelo sistema no momento do envio. Essa informações incluem o protocolo usado pelo *spammer* (SMTP, SOCKS ou HTTP), o prefixo de rede e o AS de origem, o status do IP de origem em *blacklists* como Spamhaus PBL[1] e XBL[2] , entre outras. Dessa forma, a análise posterior considera o status dessas informações no momento do envio da mensagem e não através de uma consulta posterior, que poderia gerar erros de interpretação.

Posteriormente, durante a análise, alguns ASes mereceram um estudo mais aprofundado. Nesses casos, com base nos seus números de AS, buscamos por dados disponíveis na Internet por mais detalhes sobre as suas atividades. Com base nas atividades que foram identificadas durante essa busca, classificamos os ASes como sendo provedores, provedores DSL, serviços de *hosting/colocation*, provedores de acesso a empresas, etc.

Nas análises deste trabalho consideramos aproximadamente um ano de coleta, do dia 9 de maio de 2012 até o dia 31 de março de 2013, resultando em quase quatro bilhões de mensagens e 14TB em volume de dados. Ao analisar um período grande do tráfego de mensagens de *spam*, evitamos associar um comportamento atípico, que ocorreu em um curto período de tempo, ao comportamento geral das mensagens de *spam*. Portanto, os indícios encontrados, por serem recorrentes, possuem maior confiabilidade e relevância.

4. Resultados

A tabela 1 mostra uma visão geral das mensagens de *spam* utilizadas no estudo, que foram coletadas pelos 12 *honeypots*, discriminadas pelo protocolo que foi utilizado pelo *spammer* no envio. Durante o período de quase um ano de coleta foram obtidas 3,97 bilhões de mensagens, que corresponderam a 14 TB de dados. Os endereços das máquinas que enviaram *spam* estão associados a 149 *country codes* distintos, que correspondem a cerca de 60% de todos os países. Também é possível notar um número grande sistemas autônomos, 3226, mostrando que a coleta conseguiu alcançar muitas sub-redes, permitindo uma visão

[1]**Policy Block List (PBL):** endereços IP de usuários finais que não deveriam estar disseminando emails com SMTP não autenticados para qualquer servidor de email, exceto quando especificado pelo ISP.

[2]**Spamhaus Exploits List (XBL):** Banco de dados em tempo real de endereços endereços IP infectados por *exploits*, incluindo *open proxies* (HTTP, socks, AnalogX, etc), *worms/virus* com *spam engines* e outros tipos de *trojan-horse exploits.*

mais global do tráfego de *spam*.

Tabela 1. Visão geral dos dados

	SMTP	SOCKS	HTTP	Total
Mensagens (x10^6)	690 (17,4%)	2.486 (62,5%)	799 (20,1%)	3.976
Endereços IP	294.072	34.397	11.449	328.050
Sistemas Autônomos	3.096	443	55	3.226
Contry Codes	146	66	14	149
Volume (GB)	2.564	8.522	3.3785	14.464

O volume de máquinas que utilizam o protocolo SOCKS e HTTP é bem menor, se comparado com o número de endereços IP que usam o protocolo SMTP. Apesar disso, o número de mensagens enviadas pelos protocolos SOCKS e HTTP é maior. Isso mostra que não há uma relação direta entre o número de máquinas e o número de mensagens enviadas, uma vez que aumentar o número de máquinas não significa aumentar na mesma proporção o volume de *spam*. Essa divisão é um indício da separação entre *spammers* de alto e baixo volume, mas durante a análise veremos que há mais elementos a considerar.

Pela tabela 1, podemos observar que as mensagens de spam são provenientes de muitas redes diferentes, uma vez que aparecem na coleta 3226 sistemas autônomos distintos. É interessante notar que grande parte dessas mensagens de *spam* são enviadas por um número muito pequeno de sistemas autônomos, sendo 50 deles reponsáveis por mais de 85% de todo o tráfego. Desta forma, analisar o comportamento das mensagens de *spam* na origem pode direcionar os esforços para a detecção de *spam*, pois podemos identificar quais são as vizinhanças que têm mal comportamento, e que, consequentemente, são mais propensas a enviar mensagens de *spam*.

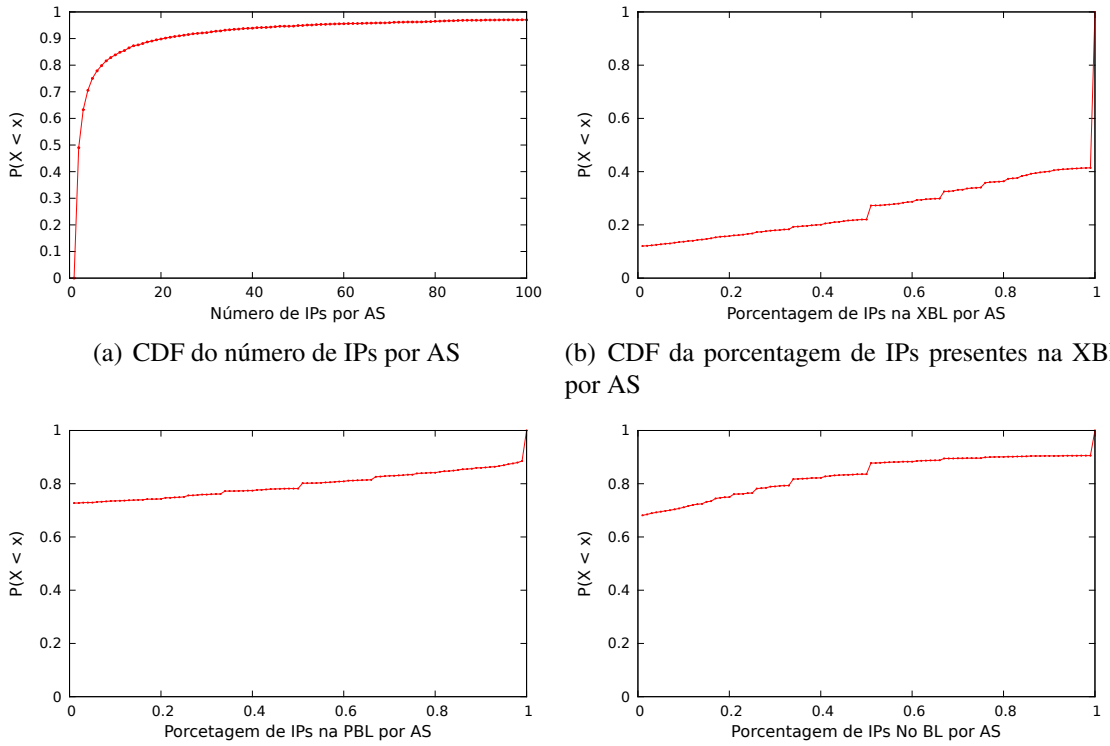
4.1. Distribuição dos endereços IP nos Sistemas Autônomos

A figura 1(a) mostra que, para a maior parte dos sistemas autônomos, poucas máquinas foram observadas contatando os *honeypots*. Em quase 90% dos ASes, o número de máquinas observadas foi inferior a 20. Pela tabela 2, podemos ver claramente a existência de um grupo grande de ASes com um número pequeno de endereços IP que enviam mensagens de *spam* e um outro grupo, muito menor, que contém a maior parte desses endereços. Isso mostra que as máquinas que enviam mensagens de *spam* não estão distribuídas uniformemente pelos sistemas autônomos.

Tabela 2. Número de endereços IP observados por AS

Nº de endereços IP por AS (x)	#ASes	#Mensagens (x10^6)	#endereços IP
x = 1	1581 (49,0%)	108 (2,7%)	1.581 (0,5%)
x <10	2705 (83,9%)	305 (7,7%)	5.635 (1,7%)
x <50	3061 (94,9%)	797 (20,0%)	13.309 (4,6%)
x <100	3131 (97,1%)	1.150 (28,9%)	18.159 (5,5%)
x $\geq$ 100	95 (2,9%)	2.825 (71,1%)	319.554 (97,4%)

Aqueles ASes que têm menos de 10 máquinas que enviam *spam*, correspondem a mais de 83% do total. Apesar disso, eles enviam apenas 7,66% das mensagens e correspondem, em número de máquinas, a 1,7% do total. Desta forma, acreditamos que, em termos de vizinhanças, esses ASes não caracterizam uma má vizinhança, mas sim que suas políticas de segurança estão sendo bem implementadas, por causa do reduzido número



(a) CDF do número de IPs por AS

(b) CDF da porcentagem de IPs presentes na XBL por AS

(c) CDF da porcentagem de IPs presentes na PBL por AS

(d) CDF da porcentagem de IPs que não estão presentes em nenhuma *blacklist*

Figura 1. CDFs sobre a distribuição dos endereços IP

de endereços IP e baixo tráfego gerado por elas. Por outro lado, 95 sistemas autônomos (2,94%) contêm mais de 319 mil endereços IP (97,41%) e são responsáveis por 71% do tráfego das mensagens de *spam*, que corresponde a quase 3 bilhões de mensagens. Essas vizinhanças mostram um mau comportamento, possivelmente gerado devido a políticas de segurança fracas. Dessa forma, direcionar os esforços para entender o comportamento dessas redes é muito importante.

A figura 1 também mostra a distribuição dos endereços IP presentes em cada uma das *blacklists*. Existe uma quantidade muito pequena de sistemas autônomos que não têm endereços IP na XBL, cerca de 15%, como podemos ver na figura 1(b). Além disso, aproximadamente 60% dos ASes têm todos os seus endereços IP na XBL. Esse resultado nos faz acreditar que a maioria dos endereços IP estão na XBL, mas o que acontece é que uma boa parte dos ASes (49%) têm um único endereço IP e a maioria desses estão somente na XBL.

Tabela 3. Visão geral das *blacklists*

	#IPs	#Msgs (10^6)
XBL	66.388 (20,2%)	594 (14,9%)
PBL	282.599 (86,2%)	789 (19,8%)
No BL	41005 (12,5%)	2.714 (68,3%)

Dessa forma, as informações sobre os endereços IP que estão na PBL e aqueles que não participam de nenhuma *blacklist* (NoBL) acabam ficando distorcidas, como apresentado nas figuras 1(c) e 1(d). No gráfico da figura 1(c), por exemplo, mais de 70% dos

sistemas autônomos não têm nenhum endereço IP presente na PBL, sendo que mais de 85% dos endereços IP encontrados no período de análise estão na PBL, conforme representado na tabela 3. Já os endereços IP que não estão em nenhuma *blacklist*, além de não pertencerem à maioria dos ASes, representam uma parcela muito pequena dos endereços IP, menos de 12%. Porém, esse baixo número de máquinas são responsáveis por mais de 68% de todo o tráfego das mensagens de *spam*, como apresentado na tabela 3.

4.2. Análise das vizinhanças com maior poder de envio

Tabela 4. 15 principais ASes

AS	Msgs (10^6)	end. IP	IP SMTP	IP SOCKS	IP HTTP	IP XBL	IP PBL	IP No BL	vol.(GB)	Classificação
10297	1.857	182	22,5%	77,5%	77,5%	17,0%	0,0%	83,0%	5.475	hosting/colocation
3462	359	100.395	78,7%	22,1%	6,8%	7,7%	99,8%	0,1%	1.320	dsl/provedor de Internet
29802	298	25	16,0%	84,0%	84,0%	12,0%	0,0%	88,0%	781	hosting
9299	148	82	39,0%	61,0%	26,8%	34,2%	1,2%	65,9%	342	dsl/business
2497	141	1.185	0,2%	99,6%	99,0%	0,2%	19,4%	80,4%	559	hosting/clouding
4134	126	110.123	99,7%	0,3%	0,2%	15,8%	81,8%	17,1%	2.446	dsl
6648	124	54	9,3%	90,7%	40,7%	9,3%	90,7%	1,9%	279	dsl/business
4725	31	215	0,9%	99,1%	98,6%	0,9%	95,8%	3,3%	120	clouding/business
27699	31	1.382	7,7%	92,3%	0,0%	9,2%	95,2%	2,7%	114	dsl/business
18881	28	3.091	10,7%	89,3%	0,0%	8,6%	96,1%	2,0%	97	colocation/provedor
8167	25	198	38,9%	61,1%	0,0%	37,4%	34,8%	41,4%	95	clouding/provedor
4837	23	20.551	99,9%	0,1%	0,0%	26,5%	78,4%	18,5%	97	-
9924	22	1.959	1,3%	82,1%	98,6%	2,8%	99,6%	0,1%	77	-
28573	21	700	75,7%	24,3%	0,0%	46,9%	98,4%	0,9%	76	provedor
4230	20	429	21,7%	78,3%	78,3%	31,0%	67,6%	11,0%	67	hosting/provedor

A tabela 4 mostra os 15 ASes que mais enviaram mensagens de *spam* no período analisado, sendo, sozinhos, responsáveis por mais de 80% de todo o tráfego de *spam*. Essa informação pode ser incorporada aos filtros de *spam* e utilizada pelos administradores das redes para reduzir o volume de *spam*, uma vez que mensagens enviadas por esses ASes tendem a ser *spam*. Ao analisar esses sistemas autônomos, apesar de todos enviarem um número alto de mensagens de *spam*, vemos que existem algumas vizinhanças que têm características muito diferentes umas das outras. Por outro lado, é possível notar que algumas delas são muito semelhantes, apesar de não terem nenhuma relação direta.

Alguns sistemas autônomos (10297 e 29802) têm características semelhantes em praticamente todos os aspectos. Esses dois ASes têm um número muito pequeno de endereços IP, sendo que a maioria deles utiliza os protocolos SOCKS e HTTP para enviar as mensagens de *spam* e não estão em nenhuma *blacklist*. O AS 2497 também é muito parecido, apesar de ter um número de máquinas maior. O AS 4725, por sua vez, diverge apenas por ter um número grande de endereços IP na *blacklist* PBL. As máquinas dessas vizinhanças se comportam de forma semelhante a servidores dedicados ao envio de *spam*, pois utilizam os protocolos SOCKS e HTTP, e a maior parte dos endereços IP não está em nenhuma *blacklist*, permitindo o envio de um número grande de mensagens pela mesma máquina.

Em contrapartida, podemos encontrar algumas vizinhanças com características completamente diferentes, como os sistemas autônomos 3462 e 4134. Ambos têm mais de 100 mil endereços IP, a grande maioria das máquinas observadas utilizou o protocolo SMTP para enviar *spam* e a maior parte deles estava em alguma *blacklist*. Além disso, o AS 4134 tem características muito marcantes, com mais de 99% dos seus endereços IP enviando mensagens de *spam* utilizando o protocolo SMTP e cerca de 17 mil deles estão

na XBL[3].

4.3. Agrupamento dos sistemas autônomos

Por conta dos indícios mencionandos na seção 4.2, buscamos uma forma de agrupar melhor os ASes observados e assim classificá-los de acordo com suas características. Para isso, utilizamos o algoritmo de agrupamento X-means, considerando as características das vizinhanças como atributos. O algoritmo tem a qualidade de definir automaticamente o número ideal de *clusters* a ser usado, ao contrário de outros algoritmos de agrupamento.

Para realização do agrupamento, utilizamos como atributos características que consideramos representar os sistemas autônomos. Os atributos envolvem diversas informações de cada AS, tais como: número de endereços IP, número de mensagens por dia, porcentagem de endereços IP em cada uma das *blacklists*, porcentagem de endereços IP que utilizam cada um dos protocolos e o número médio de mensagens enviadas por cada endereço IP. Esses atributos determinam bem as vizinhanças, pois definem os tipos de comportamento que as máquinas de uma rede podem assumir.

Tabela 5. Atributos de cada um dos agrupamentos

	Grupo 1	Grupo 2	Grupo 3	Grupo 4
N^o ASes	2.064	449	359	354
N^o Msgs (x10^6)	379	2.602	88	907
N^o Endereços IP	8.426	16.024	11.503	301.760
Msgs/IP (x10^3)	45,0	162,4	7,6	3,0
Atividade[4]	48,8	63,4	67,1	85,3
N^o Msgs SMTP	85,3%	1,5%	71,4%	29,2%
N^o Msgs SOCKS	13,5%	75,3%	23,2%	50,3%
N^o Msgs HTTP	1,2%	23,2%	5,4%	20,5%
N^o Msgs Xbl	81,9%	1,7%	68,6%	20,0%
N^o Msgs Pbl	2,8%	1,4%	52,0%	76,8%
N^o Msgs No Bl	17,2%	97,2%	15,0%	11,7%
N^o IPs Xbl	83,5%	13,2%	64,7%	16,5%
N^o IPs Pbl	5,2%	12,9%	86,6%	89,5%
N^o IPs No Bl	15,2%	77,7%	7,1%	8,8%
Volume (TB)	1,2	7,55	0,36	4,98
N^o IPs SMTP	97,43%	84,62%	99,19%	89,01%
N^o IPs SOCKS	2,67%	15,27%	0.82%	11,12%
N^o IPs HTTP	0,33%	9,52%	0,02%	3,44%

A tabela 5 exibe as propriedades de cada um dos quatro grupos gerados. O grupo 1 reúne 64% dos ASes, sendo que a maioria deles tem um número muito pequeno de endereços IP. A maior parte das máquinas desse grupo utiliza o protocolo SMTP e estão na XBL. Já o grupo 2, apesar de também ter um número pequeno de endereços IP, é responsável pela maior parte das mensagens de *spam* enviadas (65%). Além disso, mais de 98% das mensagens são enviadas utilizando os protocolos SOCKS e HTTP, apesar de grande parte dos endereços IP (84%) utilizar o protocolo SMTP para enviar *spam*. A grande maioria das mensagens (97%) foi enviada por máquinas que não estavam em nenhuma *blacklist*. O grupo 3 se diferencia dos demais por ter mais de 99% dos endereços IP enviando mensagens pelo protocolo SMTP e ter grande parte deles na PBL e XBL. Por último, o grupo 4, reúne os ASes que têm um número elevado de máquinas. A maioria de seus endereços IP estão na PBL, e apenas um número menor está na XBL. Apesar da

[3] *blacklist* que registra o endereço IP de máquinas infectadas por algum *malware*

[4] Média de dias, no período avaliado, em que as máquinas do grupo ficaram ativas.

maior parte das máquinas ter usado SMTP, o maior volume de *spam* foi enviado usando SOCKS.

Se considerarmos as vizinhanças que mais enviaram mensagens de *spam*, estudadas na seção 4.2, vemos que o agrupamento consegue colocar os ASes com características semelhantes em um mesmo grupo, e separar aqueles com comportamentos diferentes. Os sistemas autônomos 10297, 29802 e 2497, cujas máquinas se comportam como servidores dedicados, ficaram no grupo 2, responsável pela maior parte do tráfego de *spam*, mesmo tendo poucos endereços IP. Além disso, esse grupo tem poucas máquinas em *blacklist*, uma característica necessária à máquinas que enviam um grande volume de mensagens.

A maioria das máquinas dos sistemas autônomos 3462 e 4134 se comportam como *bots* e essas duas vizinhanças fazem parte do grupo 4. Esse grupo inclui os ASes que têm um número grande de endereços IP e que têm a maioria deles em *blacklists*. Observa-se também que, a maioria dos endereços IP desse grupo envia uma quantidade pequena de mensagens.

Ao analisar as 15 vizinhanças destacadas na seção 4.2, verificamos que nenhuma delas está no grupo 1 ou 3, como podemos verificar na tabela 4. Esse resultado já era esperado, uma vez que os ASes no grupo 1 têm o número de endereços IP muito reduzido e os ASes do grupo 3, além de terem poucas máquinas, enviam poucas mensagens de *spam*. Desta forma, as vizinhanças que mais enviam *spam* foram alocadas para os outros dois grupos: dos ASes que contêm um número elevado de endereços IP ou daqueles que enviam uma grande quantidade de mensagens de *spam*.

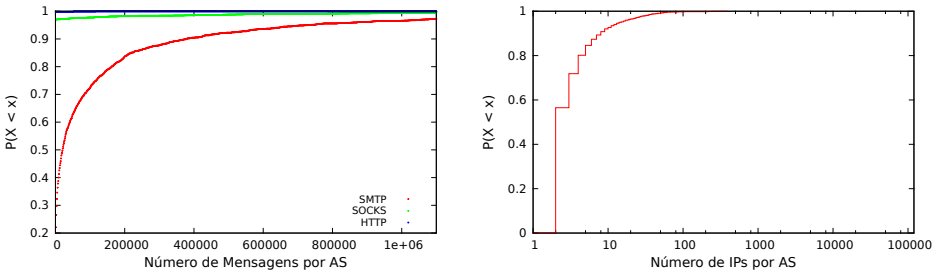
Tabela 6. Grupos dos AS que mais enviam *spam*

AS	Classificação	Grupo	AS	Classificação	Grupo
10297	hosting/colocation	2	27699	dsl/business	4
3462	dsl/provedor de Internet	4	18881	colocation/provedor	4
29802	hosting	2	8167	clouding/provedor	2
9299	dsl/business	2	4837	-	4
2497	hosting/clouding	2	9924	-	4
4134	dsl	4	28573	provedor	4
6648	dsl/business	4	4230	hosting/provedor	4
4725	clouding/business	4			

4.3.1. Grupo 1

O gráfico da figura 2(a) mostra que uma porcentagem muito pequena das vizinhanças deste grupo utilizam os protocolos SOCKS e HTTP para enviar mensagens de *spam* e que mais de 70% dos ASes enviam menos de 100 mil mensagens em todo período. Apesar de não ser um número muito grande, uma vez que coletamos por quase um ano, ao observar a tabela 5 notamos que esse grupo tem um número muito pequeno de endereços IP, resultando em um número de mensagens por endereço IP relativamente alto.

A principal característica dos ASes desse grupo é o baixo número de máquinas, como podemos ver pela figura 2(b). Quase 60% dos sistemas autônomos têm apenas um único endereço IP e nenhum deles tem mais de cem endereços IP. Isso explica o fato desse grupo, mesmo englobando 64% dos AS, ser responsável por apenas 9,5% do tráfego de *spam* gerado. Além disso, a maioria dos endereços IP desse grupo estão na XBL, o que caracteriza máquinas infectadas, provavelmente pertencentes a *botnets*.

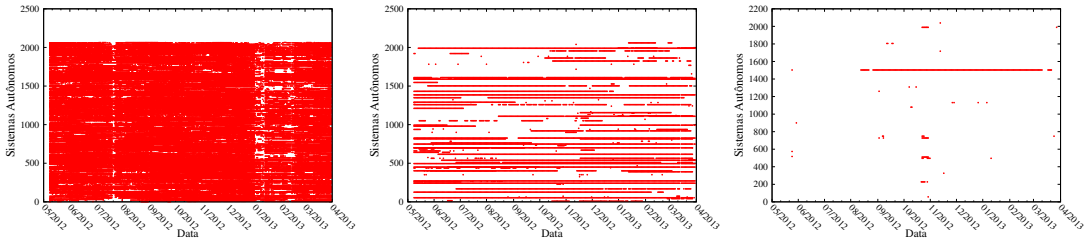


(a) CDF do número de mensagens enviadas por AS

(b) CDF do número de IPs por AS

Figura 2. CDFs para análise do grupo 1

O período de atividade das máquinas nos ASes desse grupo mostram atividade constante utilizando o protocolo SMTP em quase todos os ASes, como apresentado na figura 3(a). Por outro lado, o gráfico da figura 3(c) mostra que poucos ASes utilizam o protocolo HTTP e, em apenas um, esse protocolo esteve ativo por um período maior que dez dias. Essa grande quantidade de mensagens enviadas pelo protocolo SMTP, juntamente com um número alto de endereços IP na XBL, sugere a existência de *bots*. Como há poucos endereços comprometidos nesses ASes, é possível que essas máquinas constituam exceções na política de segurança de um sistema em geral seguro e que, por algum motivo, passem despercebidas à gerência dessas redes.



(a) SMTP

(b) SOCKS

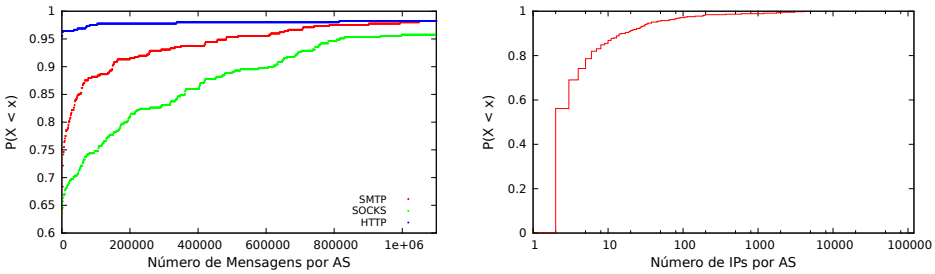
(c) HTTP

Figura 3. Período de atividade dos ASes do grupo 1, por protocolo

4.3.2. Grupo 2

Este grupo contém os ASes que mais enviam mensagens de *spam*, sendo responsáveis por mais de 65% de todas as mensagens. Como mostrado na figura 4(a), 5% dos ASes estão associados a um número maior que um milhão de mensagens e são eles os responsáveis pela maior parte do tráfego de *spam*. Neste grupo, quase nenhuma mensagem é enviada pelo protocolo SMTP, uma vez que 98% das mensagen são enviadas pelos protocolos SOCKS e HTTP.

Os sistemas autônomos desse grupo também têm um número muito baixo de endereços IP, pois cerca de 57% deles contêm um único endereço IP. Além disso, uma porcentagem muito pequena dessas vizinhanças têm um número de máquinas superior a cem, apenas 2%. Porém, mesmo tendo um número baixo de endereços IP, a quantidade média de mensagens de *spam* enviadas por cada um deles é muito grande, superior a 162



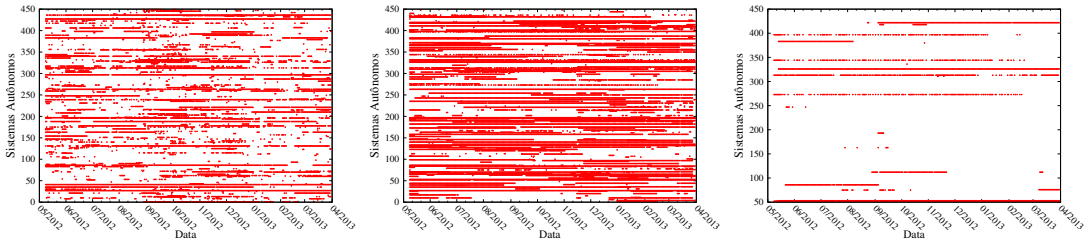
(a) CDF do número de mensagens enviadas por AS

(b) CDF do número de IPs por AS

Figura 4. CDFs para análise do grupo 2

mil, como podemos verificar na tabela 5. Um outro aspecto interessante é que, nesse grupo, um número muito grande de endereços IP não fazem parte de nenhuma *blacklist*. Todas as características encontradas para esse grupo sugerem que a maior parte dos ASes abrigam máquinas que funcionam como servidores dedicados ao envio de *spam*, provavelmente com a conivência dos administradores, já que não aparecem em *blacklists*.

Se comparado aos demais grupos, o período de atividade dos ASes utilizando os protocolos SOCKS e HTTP são maiores para esse grupo. Podemos ver que existe um número maior de ASes que utilizam esses protocolos, além de ficarem ativos por um período maior, como os gráficos da figura 5 mostram claramente.



(a) SMTP

(b) SOCKS

(c) HTTP

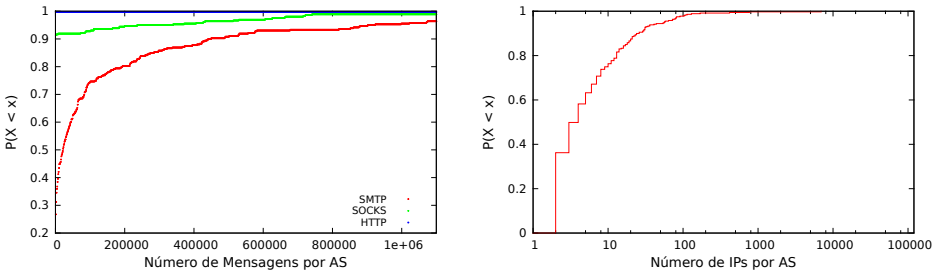
Figura 5. Período de atividade dos ASes do grupo 2, por protocolo

Como mencionado anteriormente, os AS 10297, 29802 e 2497 foram assinalados a esse grupo. Como outros do grupo que foram estudados, esses ASes se caracterizam por oferecerem serviços de *hosting* e *co-location*.

4.3.3. Grupo 3

Pela tabela 5, podemos ver que, nesse grupo, mais de 70% das mensagens de *spam* são enviadas utilizando o protocolo SMTP e que os ASes do grupo são responsáveis por apenas 2,2% do total das mensagens. O gráfico da figura 6(a) mostra que mais de 80% das vizinhanças enviam menos de 200 mil mensagens, explicando o fato deste grupo ser responsável por um número comparativamente menor de mensagens.

O gráfico da figura 6(b) mostra um comportamento semelhante ao visto nos grupos 1 e 2, mas o número de ASes com apenas um endereço IP é menor, pouco menos de 40%.



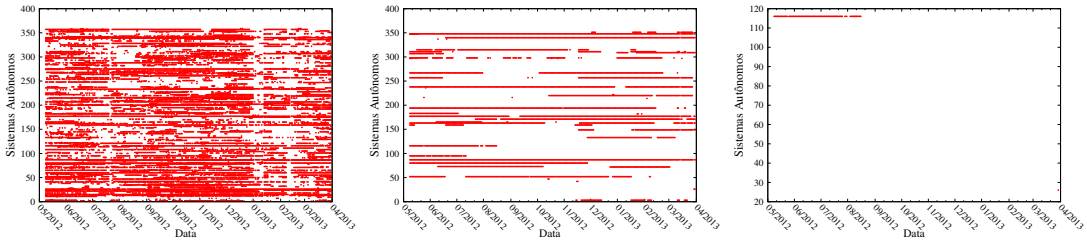
(a) CDF do número de mensagens enviadas por AS

(b) CDF do número de IPs por AS

Figura 6. CDFs para análise do grupo 3

O que marca esse grupo é o número muito alto de endereços IP que utilizam o protocolo SMTP, mais de 99% deles, superando qualquer outro grupo. Além disso, cerca de 64% das máquinas desse grupos estão na XBL. Isso sugere a presença de *bots*, mas o baixo número de endereços IP sugere que há menos máquinas comprometidas nesses ASes.

O gráfico da figura 7(c) mostra que apenas um AS desse grupo enviou mensagens de *spam* pelo protocolo HTTP, e mesmo assim por um curto período de tempo. Como era esperado, para o protocolo SMTP, todos os ASes são muito ativos durante todo o período, como pode ser visto na figura 7(a).



(a) SMTP

(b) SOCKS

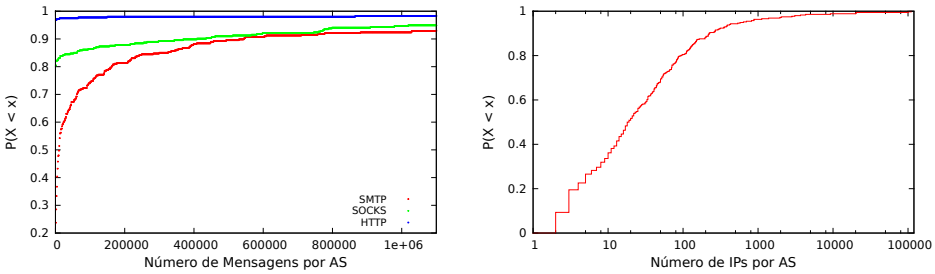
(c) HTTP

Figura 7. Período de atividade dos ASes do grupo 3, por protocolo

4.3.4. Grupo 4

Pela figura 8(a) podemos ver que a maioria dos ASes utiliza o protocolo SMTP para enviar mensagens de *spam*, mas os poucos sistemas autônomos que utilizam os protocolos SOCKS e HTTP enviam um número de mensagens maior que um milhão. As vizinhanças desse grupo são responsáveis por grande parte das mensagens de *spam*, aproximadamente 23% do total.

Esse grupo contém os ASes com o maior número de máquinas observadas, como podemos verificar na figura 8(b), com mais de 20% das vizinhanças com mais de 1000 endereços IP, em que algumas delas têm o número de máquinas superior a 100 mil. Dessa forma, mesmo sendo responsável por boa parte do tráfego de *spam*, o número de mensagens por endereço IP é o menor entre os grupos, apenas 3 mil. Além disso, a grande maioria dos endereços estão em *blacklists* e utilizam o protocolo SMTP. Por tudo isso, temos fortes indícios de que muitas das máquinas pertencentes a esse grupo fazem parte



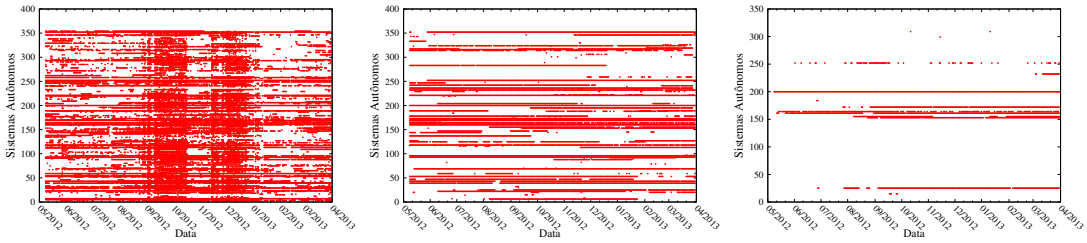
(a) CDF do número de mensagens enviadas por AS

(b) CDF do número de IPs por AS

Figura 8. CDFs para análise do grupo 4

de *botnets*. Pelo grande número de máquinas nessa situação, esses ASes se classificam na categoria de vizinhanças ruins, onde aparentemente as políticas de gerência e manutenção da rede não são capazes de evitar a proliferação de máquinas infectadas.

Como os ASes desse grupo têm um número muito grande de endereços IP, é comum que o mesmo AS utilize os três protocolos diferentes na disseminação de *spam*. Esse comportamento é explicitado pelas figuras 9(b) e 9(c). Já era de se esperar um período de atividade intenso no uso do protocolo SMTP, uma vez que máquinas pertencentes a *botnets* tendem a utilizar esse protocolo. Logo, o gráfico da figura 9(a) reforça as suspeitas sobre as *botnets*.



(a) SMTP

(b) SOCKS

(c) HTTP

Figura 9. Período de atividade dos AS do grupo 4, por protocolo

Os ASes 3462 e 4134, classificados como sendo de provedores de Internet com redes DSL, fazem parte desse grupo. Isso sugere que, realmente, a composição desse grupo é predominantemente de máquinas domésticas de usuários, infectadas por algum tipo de *malware*.

5. Conclusão

Vários esforços estão sendo aplicados na tentativa de combater o envio de *spam*, mas essa tarefa vem sendo dificultada devido à sofisticação das técnicas dos *spammers*. Este trabalho mostra que, apesar das mensagens de *spam* serem enviadas a partir de diversas redes, essa disseminação está concentrada em poucos sistemas autônomos e isso pode ser usado para direcionar os esforços na detecção de *spam*. Além disso, conseguimos agrupar os ASes em quatro categorias representativas, onde cada um dos grupos reúne os ASes com características de disseminação de *spam* semelhantes. Mostramos ainda que alguns

dos grupos definem ASes que são boas vizinhanças, uma vez que eles têm um número pequeno de endereços IP e enviam poucas mensagens de *spam*.

Como trabalhos futuros, pretendemos realizar análises mais profundas sobre cada uma das categorias encontradas, para entender melhor todas as diferenças entre os grupos. Também queremos entender melhor o comportamento da categoria de ASes considerada como sendo uma boa vizinhança e verificar se são as políticas de segurança utilizadas que definem o comportamento desses sistemas autônomos.

Agradecimentos

Este trabalho foi parcialmente financiado por NIC.Br, Fapemig, CAPES, CNPq e InWeb.

Referências

Gomes, L. H., Almeida, R. B., Bettencourt, L. M. A., Almeida, V., and Almeida, J. M. (2005). Comparative Graph Theoretical Characterization of Networks of Spam and Legitimate Email. In *Proceedings of the Second Conference on Email and Anti-Spam - CEAS 2005*, Stanford, CA, USA. CEAS.

Guerra, P. H. C., Guedes, D., Wagner Meira, J., Hoepers, C., Chaves, M. H. P. C., and Steding-Jessen, K. (2010). Exploring the spam arms race to characterize spam evolution. In *Proceedings of the 7th Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (CEAS)*, Redmond, WA.

Kokkodis, M. and Faloutsos, M. (2009). Spamming botnets: Are we losing the war? ? In *Proceedings of the 6th Conference on e-mail and anti-spam (CEAS)*.

Las-Casas, P. H. B., Guedes, D., Jr., W. M., Hoepers, C., Steding-Jessen, K., Chaves, M. H. P., Fonseca, O., Fazzion, E., and Moreira, R. E. A. (2013). Análise do tráfego de spam coletado ao redor do mundo. In *Anais do simpósio brasileiro de redes de computadores e sistemas distribuídos (SBRC)*. SBC.

Moreira Moura, G. C., Sadre, R., and Pras, A. (2011). Internet bad neighborhoods: the spam case. In Festor, O. and Lupu, E., editors, *7th International Conference on Network and Services Management (CNSM 2011), Paris, France*, pages 1–8, USA. IEEE Communications Society.

Newman, M. E. J., Forrest, S., and Balthrop, J. (2002). Email networks and the spread of computer viruses. *Phys. Rev. E*, 66:035101.

Orman, H. (2013). The compleat story of phish. *Internet Computing, IEEE*, 17(1):87–91.

Pathak, A., Hu, Y. C., and Mao, Z. M. (2008). Peeking into spammer behavior from a unique vantage point. In *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, LEET'08, pages 3:1–3:9, Berkeley, CA, USA. USENIX Association.

Sipior, J. C., Ward, B. T., and Bonner, P. G. (2004). Should spam be on the menu? *Commun. ACM*, 47(6):59–63.

Steding-jessen, K., Vijaykumar, N. L., and Montes, A. (2007). Using low-interaction honeypots to study the abuse of open proxies to send spam.

van Wanrooij, W. and Pras, A. (2010). Filtering spam from bad neighborhoods. *International Journal of Network Management*, 20(6):433–444.