Análise do tráfego de spam coletado ao redor do mundo

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

[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

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

{cristine,klaus,mhp}@cert.br

{osvaldo.morais,elverton,rubens}@dcc.ufmg.br

Abstract. *Several efforts have been pursued to create a comprehensive view of spam traffic. However, observations at isolated points of the Internet are always limited by factors of spatial locality. This work aims to add a dimension to this analysis by contrasting samples of spam traffic collected simultaneously at different points. Our analyses indicate that factors such as location and connectivity have significant impact on the observed traffic, but certain features, such as profiles of messages sent by different protocols, source addresses and test patterns from spammers repeat themselves around the world.*

Resumo. *Diversos esforços têm sido feitos para se criar uma visão abrangente do tráfego de spam. Entretanto, observações em pontos isolados da Internet estão sempre limitadas por fatores de localidade espacial. Este trabalho pretende acrescentar uma dimensão a essa análise ao contrastar amostras de tráfego de spam coletadas simultaneamente em diferentes pontos. Nossas análises indicam que fatores como localização e conectividade têm impacto sensível sobre o tráfego observado, porém certas características, como perfis das mensagens enviadas por diferentes protocolos, endereços de origem e padrões de teste dos spammers se repetem ao redor do mundo.*

1. Introdução

Ainda hoje, *spam* é um dos grandes problemas presentes na Internet. Além do caráter indesejado, *spams* são muitas vezes relacionados com o envio de *phishing*, além da propagação de *malwares*, como cavalos de tróia, vírus e *worms* [Newman et al. 2002], tornando-os ainda mais nocivos para a rede e seus usuários. Por tudo isso, estudos mostram que o abuso causado pelos *spams* acarretam vários bilhões de dólares de prejuízo às empresas e à sociedade em geral [Sipior et al. 2004].

O combate ao *spam* é caracterizado pela constante evolução das técnicas de detecção dessas mensagens, uma vez que as ferramentas utilizadas pelos *spammers* se mostram cada vez mais sofisticadas, reduzindo a eficácia dos filtros anti-*spam* e a rastreabilidade dos *spammers* [Goodman et al. 2007]. Um exemplo disso é o crescimento na

utilização de máquinas infectadas por *malwares*, como os bots, para o envio de *spam* e *phishing* [Xie et al. 2008], permitindo que o *spammer* permaneça no anonimato.

Mesmo com o desenvolvimento de técnicas de combate, é necessário um esforço contínuo para entender a forma de atuação dos *spammers* ao enviar mensagens indesejadas pela Internet, devido à sua natureza evolutiva. Essa evolução acontece tanto no modo como *spammers* disseminam suas mensagens pela rede, buscando maximizar o volume de mensagens enquanto mantêm sua identidade oculta, quanto na forma como compõem o conteúdo das mesmas [Pu 2006]. Logo, analisar o comportamento dos *spammers* ao longo do tempo permite identificar padrões e características que podem ajudar na evolução das ferramentas de combate ao *spam*. Por exemplo, o tráfego gerado por máquinas participantes de *botnets* tende a apresentar características similares. Sendo assim, o entendimento desses padrões pode ser útil para identificar *bots* e as redes de que fazem parte.

Para entender o comportamento dos *spammers* na rede, realizamos neste trabalho a caracterização do tráfego de *spam* utilizando dados coletados por *honeypots* de baixa interatividade localizados em redes intermediárias. A grande vantagem da análise aqui realizada está no fato dos dados serem coletados em diversos pontos distintos da Internet, fornecendo assim visões diferentes do problema e não apenas uma visão singular, proveniente de apenas uma fonte de dados, como visto em diversos trabalhos anteriores. Com isso, pretendemos adicionar uma dimensão às análises existentes, ao contrastar amostras de um grande volume de tráfego, oriundos de diversas localidades, reduzindo distorções comuns em coletas restritas a um único local.

Os resultados indicam que algumas características, como perfis das mensagens enviadas por diferentes protocolos, endereços de origem e padrões de teste dos spammers, se repetem nas diversas localidades observadas. Além disso, mostram que o comportamento das campanhas de *spam* que aparecem nos *honeypots* possuem grande influência no tráfego gerado. Por fim, os resultados evidenciam o comportamento dos *spammers* ao descobrirem um novo *honeypot* na rede, que começam a enviar mensagens utilizando o protocolo SOCKS indiscriminadamente, enquanto o início do envio de mensagens utilizando SMTP possui restrições.

2. Trabalhos Relacionados

Diversos trabalhos avaliaram as características apresentadas pelo tráfego de *spam* coletado nos servidores de correio de destino. Kim *et al.* caracterizaram o tráfego de *spam* a partir de dados da camada de aplicação coletados em servidores de correio eletrônico de destino [Kim e Choi 2008]. Gomes *et al.* analisaram uma carga de trabalho de mensagens de usuários de uma universidade brasileira e destacaram uma série de características capazes de diferenciar *spams* de mensagens legítimas [Gomes et al. 2007]. Esses trabalhos, entretanto, focaram apenas tráfego em um ponto específico da rede, os servidores de correio de destino, e consideraram a análise de elementos do conteúdo das mensagens.

Outros consideraram a origem do *spam* na rede como, por exemplo, Las-Casas *et al.*, que propõem uma ferramenta de detecção de *spammers* que analisa o tráfego de saída de um provedor [Las-Casas et al. 2011, Las-Casas et al. 2013]. Nossas observações sobre tráfego em pontos intermediários da rede permite que administradores entendam a natureza do tráfego que passa por suas redes, quando o controle direto sobre a origem do mesmo não é possível.

Com relação ao tráfego de *spam* gerado por *botnets*, relatórios recentes mostram que 88% do total de *spams* enviados são provenientes dessas redes [Symantec 2011]. John *et al.* mostram que apenas 6 *botnets* são responsáveis pela maior parte dos *spams* recebidos [John et al. 2009]. Já Stone-Gross *et al.* destacam o gerenciamento de campanhas de *spam* enviadas por *botnets*, do ponto de vista do *botmaster*. Observando o envio de *spam* do ponto de vista do espaço de endereços IP, eles concluiram que as atividades das *botnets* estão mais dispersas no espaço de endereços IP, o que dificulta a filtragem de *botnets* baseada em análise de endereços [Kokkodis e Faloutsos 2009]. Outros investigaram características de tráfego coletado da camada de rede que seriam comuns a *spammers* [Ramachandran e Feamster 2006], mas se basearam em uma visão local do tráfego.

Neste trabalho realizamos uma caracterização do tráfego de *spam* que, diferente de trabalhos anteriores, possui uma visão global, evitando assim possíveis distorções por se considerar um ponto único da rede. Acreditamos que este trabalho pode ser útil para a evolução dos trabalhos que consideram o combate ao *spam*, uma vez que nele é mostrado como o tráfego de *spam* se comporta em diferentes locais e quais padrões e características são importantes para a contínua identificação das mensagens indesejadas.

3. Metodologia

Os dados foram coletados através de um conjunto de oito *honeypots* de baixa interatividade instalados ao redor do mundo. Esses *honeypots* foram configurados de modo a simular computadores com *proxies* e *mail relays* abertos, que frequentemente são abusados para o envio de *spam* e para outras atividades maliciosas.

Dentre os oito *honeypots* utilizados, dois se encontram em redes brasileiras (BR-01 e BR-02), enquanto os restantes se localizam em diferentes *country codes*: AU-01 (Austrália), AT-01 (Áustria), EC-01 (Equador), NL-01 (Holanda), TW-01 (Taiwan) e UY-01 (Uruguai). Como mencionado anteriormente, a distribuição dos *honeypots* por diferentes pontos da rede mundial teve por objetivo permitir uma visão ampla do tráfego de *spam* ao redor da Internet para, com isso, reduzir distorções comuns em coletas restritas a uma única localidade.

A captura de mensagens foi feita pelos sistemas *spamsinkd* e *spamtestd*, desenvolvido por alguns dos autores, para capturar spams e mensagens de teste, respectivamente [CERT.br 2013]. Quando uma máquina se conecta à porta 25 de um dos *honeypots*, tem a impressão de interagir com um servidor SMTP operando como *open relay*, pronto para repassar mensagens. Máquinas que se conectam a portas tradicionais utilizadas por mecanismos de *proxy*, como as associadas aos protocolos HTTP e SOCKS, são levadas a crer que suas tentativas de conexão para outros servidores SMTP através de tais *proxies* são bem-sucedidas. Em ambos os casos, porém, nenhum *spam* é efetivamente entregue. Todas as transações são armazenadas com informações como data e hora, origem (endereço IP, prefixo de rede e AS), protocolo que foi abusado no *honeypot* e, finalmente, o conteúdo completo de cada mensagem que teria sido enviada.

Neste trabalho consideramos o período de 84 dias entre 09/05/2012 e 31/07/2012. Esse período foi escolhido por ser o maior intervalo recente em que a coleta ocorreu sem interrupções. Ao todo, durante aquele período, foram coletados quase 815 milhões de mensagens, enviadas por 53 mil endereços distintos. Mais detalhes sobre o tráfego coletado são apresentados na seção 4.

4. Resultados

Nesta seção mostramos os resultados mais interessantes encontrados na análise do tráfego de *spam*, além da discussão a respeito destes. Inicialmente apresentamos uma visão geral dos dados, seguido pela comparação e análise detalhada dos diferentes *honeypots*. Observações interessantes encontradas são mostradas posteriormente, além da discussão sobre o redescobrimento de um *honeypot* na rede e o comportamento do tráfego neste.

Tabela 1. Visão Geral

	SMTP(%)	SOCKS(%)	HTTP(%)	Total
Mensagens (milhões)	143,87 (17,7%)	557,73 (68,4%)	113,26 (13,9%)	814,87
Endereços IP	50.348 (93,9%)	3.146 (5,9%)	644 (1,2%)	53.608
Prefixos de rede	4.477 (86,0%)	921 (17,7%)	74 (1,4%)	5.207
Sistemas Autônomos (AS)	1.551 (93,7%)	268 (16,2%)	25 (1,5%)	1.655
***Country Codes* (CC)**	131 (97,0%)	63 (46,7%)	9 (6,7%)	135
Volume de tráfego (TB)	0,51 (15,0%)	2,91 (56,3%)	0,95 (28,0%)	3,39

A tabela 1 oferece uma visão geral dos dados coletados pelos oito *honeypots*. No período de 84 dias, quase 815 milhões de mensagens foram coletadas, oriundas de endereços associados a 135 *country codes* distintos, cerca de 55% dos *country codes* do mundo. Do total de mensagens, 68,44% foram enviadas utilizando o protocolo SOCKS, 17,65% usando SMTP e apenas 13,89% usando HTTP. É interessante notar que, das aproximadamente 113 milhões de mensagens utilizando o protocolo HTTP, mais de 82 milhões foram provenientes do *honeypot* TW-01 que, conforme será discutido posteriormente, possui características bastante distintas dos demais.

Tabela 2. Top 10 Country Codes

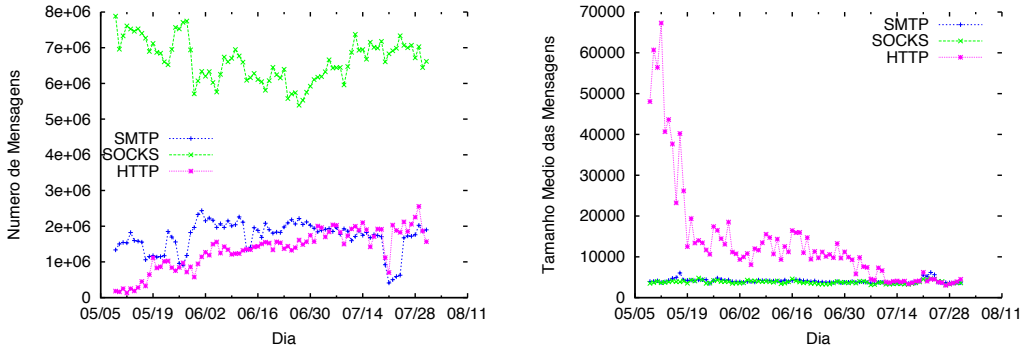
	Mensagens	Endereços IP	Prefixos's	AS's
US	479.118.779	1.533	769	278
PH	119.506.411	97	23	7
CN	47.049.075	18.508	915	51
BR	27.398.959	946	601	99
TW	21.898.881	28.183	130	21
JP	13.340.731	70	39	17
RU	9.097.963	493	387	246
KR	6.430.220	190	127	35
IN	6.271.617	265	209	40
HK	5.856.073	59	55	23

Apesar de mensagens terem sido observadas originando-se de 135 *country codes* distintos, alguns poucos CCs foram responsáveis pela grande maioria de todo o *spam* recebido. A tabela 2 mostra aqueles que originaram mais mensagens indesejadas ao longo do período. Como é possível verificar, os 10 *country codes* que mais enviaram mensagens são responsáveis por mais de 90% do total de *spam* recebido. Quase 60% das mensagens recebidas foi oriunda de endereços associados ao CC US. Estes resultados sugerem que o envio de *spams* está concentrado em alguns poucos *country codes*.

4.1. Comportamentos por protocolo

Através das porcentagens na tabela 1, já é possível observar alguns elementos interessantes do comportamento dos *spammers*: (i)a maior parte das mensagens é enviada através de *proxies* SOCKS, porém por um número relativamente pequeno de máquinas; (ii)apesar de responder por uma fração pequena do total de mensagens (pouco menos de 14%), o protocolo HTTP responde por aproximadamente 28% do tráfego; (iii)o número de endereços IP que usam cada protocolo e o número de mensagens enviadas por cada um variam bastante entre protocolos.

Uma análise temporal dos dados agregados por protocolo indicam comportamentos relativamente estáveis em termos de mensagens enviadas por cada protocolo, conforme pode ser visto na figura 1(a). O volume total enviado usando-se cada protocolo também segue um comportamento bastante semelhante (não apresentado por limitações de espaço). Já a figura 1(b) mostra que o tamanho médio das mensagens enviadas por SOCKS e SMTP permaneceu relativamente estável durante todos os dias, enquanto as mensagens enviadas por HTTP variaram significativamente ao longo do tempo, com algumas de suas mensagens bem maiores que as demais. Inspecionamos essas mensagens maiores e observamos que elas foram enviadas por apenas 5 endereços distintos e todos provenientes do *country code* CN, e foram recebidas por todos os *honeypots*, com exceção do BR-01 e TW-01[1]. Logo, o aparecimento destas pode estar relacionado a algumas campanhas específicas, originadas em CN.



(a) Mensagens por protocolo (b) Tamanho das mensagens por protocolo

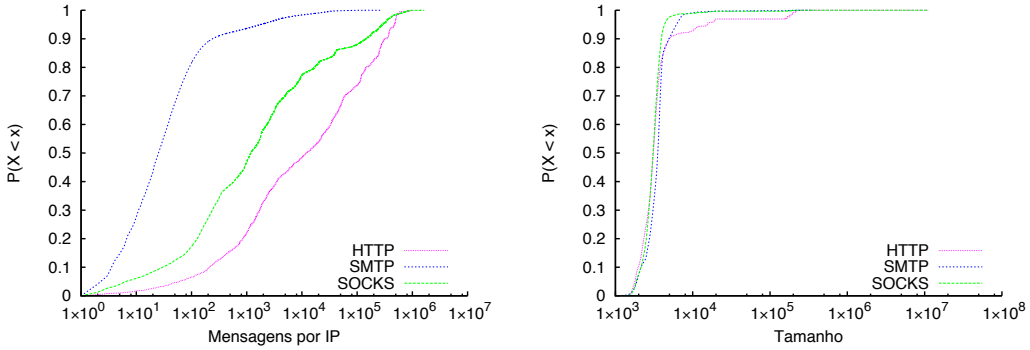
Figura 1. Dados agregados por protocolo ao longo do tempo

A figura 2 apresenta dados sobre a distribuição de mensagens por endereços de origem e por tamanho para cada protocolo, ressaltando as diferenças entre eles. A figura 2(a) mostra que os endereços que utilizam protocolos diferentes possuem comportamentos distintos com relação ao número de mensagens enviadas. Enquanto quase 90% dos endereços IP utilizando SMTP enviaram menos de 100 mensagens ao longo dos 84 dias, apenas 17% dos transmissores SOCKS e 8% dos HTTP enviam menos que isso. Por outro lado, uma fração desprezível dos transmissores SMTP enviou mais que cem mil mensagens, enquanto 11% dos SOCKS e 25% dos HTTP ultrapassaram esse valor.

Com relação ao tamanho das mensagens enviadas usando cada protocolo (fig. 2(b)), o perfil de 80% das mensagens enviadas por cada protocolo são bastante semelhantes, sendo as mensagens enviadas por SOCKS apenas ligeiramente maiores. Entretanto, apenas 2% das mensagens enviadas usando SMTP tinha mais de 5 KB, quanto eram 10% das mensagens enviadas por SOCKS e HTTP. Já no caso de HTTP, cerca de 3% das mensagens enviadas com aquele protocolo eram maiores que 200 KB.

Além disso, apenas uma fração pequena das máquinas utilizou mais de um protocolo para enviar *spam* durante o período (a soma dos números de endereços IP distintos que foram vistos usando cada protocolo é menos de 1% superior ao total de endereços distintos). Esses fatores nos permitem afirmar que as máquinas que utilizam cada tipo de

[1]Naquele período, BR-01 havia trocado de endereço recentemente e ainda não estava sendo abusado pelos *spammers* em geral; TW-01, como discutido posteriormente, tem um comportamento diferenciado com relação a tráfego oriundo de CN.



(a) Núm. de mensagens por end. origem (b) Tamanho das mensagens

Figura 2. Distribuições acumuladas para mensagens por protocolo

protocolo têm comportamentos diferentes, indicando origens (*spammers*) diferentes: (i) máquinas que usam *proxies* abertos (HTTP e SOCKS) enviam mensagens em grande volume, o que sugere o uso de uma infraestrutura especializada; (ii) máquinas que enviam *spam* usando SMTP tendem a enviar bem menos mensagens, mas seu conjunto ainda é responsável por uma parcela significativa do tráfego, o que sugere a formação de *botnets*.

4.2. Comparação entre os diversos locais de coleta

A visão geral dos dados fornece informações interessantes sobre comportamentos que se mantém entre os *honeypots*. Entretanto, analisar cada um dos *honeypots* individualmente nos permite identificar características não possíveis de serem observadas anteriormente, visualizando os dados como um todo. Dado que os *honeypots* estão em localizações distintas, as características dos dados coletados em cada ponto pode apresentar variações.

Distribuição dos endereços IP de origem entre os honeypots

A tabela 3 apresenta o número de endereços IP em comum entre cada par de *honeypots*. Analisando-a, percebemos que alguns *honeypots* possuem muitos endereços em comum, como AU-01 e UY-01: 91% dos endereços presentes em UY-01 também estão presentes no AU-01, correspondendo a 58% dos endereços ali observados (AU-01 foi contactado por mais máquinas). Outro exemplo é entre os *honeypots* AT-01 e BR-01, que possuem 15.417 endereços em comum, que representam 85% de AT-01. Este alto número de origens em comum entre os *honeypots* indica que *spammers* tendem a distribuir seu tráfego por uma grande variedade de pontos intermediários, independente de localidade. Com isso, algumas das características do tráfego presente em diferentes pontos tendem a ser similares, como observado anteriormente, uma vez que parte dos transmissores são comuns e, em consequência, as mensagens de *spam* observadas tendem a ser semelhantes entre eles.

Ainda com relação à tabela 3, podemos notar que o *honeypot* TW-01 é bastante distinto dos demais com relação aos endereços IP que abusaram dele. Além de registrar um número muito menor de endereços IP de origem (apenas 2.194), estes endereços não aparecem em altas proporções nos demais *honeypots*. O *honeypot* que apresenta maior número de endereços em comum com o TW-01 é o BR-02, com 66% dos 2.194 endereços do primeiro sendo observados no segundo também. Porém, em média, cerca de 51% dos endereços observados em TW-01 aparecem nos demais *honeypots*, valor baixo quando

comparado aos valores dos demais. Por conta dessa diferença, TW-01 será tratado separadamente mais à frente.

Tabela 3. Percentual de endereços IP em comum entre os *honeypots*

	AT-01	AU-01	BR-01	BR-02	EC-01	NL-01	TW-01	UY-01	Total
AT-01	-	86%	85%	77%	50%	71%	6%	58%	18.138
AU-01	56%	-	79%	78%	54%	68%	3%	52%	27.636
BR-01	41%	58%	-	74%	57%	49%	3%	35%	37.563
BR-02	41%	63%	82%	-	68%	58%	4%	37%	33.920
EC-01	27%	44%	62%	67%	-	37%	3%	25%	34.253
NL-01	57%	84%	83%	88%	56%	-	6%	53%	22.284
TW-01	49%	43%	46%	66%	51%	57%	-	49%	2.194
UY-01	66%	91%	83%	80%	53%	74%	7%	-	15.917

Distribuição dos *Country Codes* de origem

Como os *honeypots* se localizam em diferentes posições do globo, torna-se interessante observar a origem dos transmissores dos *spams* recebidos por cada um deles, para verificar se a localização influencia no recebimento de mensagens de diferentes origens. A tabela 4 mostra os 5 *country codes* que mais enviaram mensagens para cada um dos *honeypots*. Em todos os *honeypots*, os *country codes* que mais abusaram são basicamente os mesmos, alterando pouco entre eles e, como seria de se esperar, estão todos entre os mais frequentes no global (tab. 2).

Tabela 4. Percentual do total de mensagens por *country codes* em cada *honeypots*

AT-01	AU-01	BR-01	BR-02	EC-01	NL-01	TW-01	UY-01
US (72,88%)	CN (22,98%)	BR (13,79%)	US (51,20%)	CN (23,72%)	US (84,73%)	US (67,83%)	US (70,82%)
PH (15,64%)	BR (11,29%)	CN (12,06%)	PH (23,92%)	TW (16,18%)	PH (9,90%)	PH (25,08%)	PH (13,64%)
CN (2,50%)	US (8,04%)	US (9,38%)	CN (6,53%)	BR (14,45%)	JP (1,57%)	TW (2,94%)	CN (3,97%)
JP (1,19%)	RU (5,56%)	RU (6,12%)	BR (3,29%)	US (10,11%)	CN (1,25%)	JP (1,93%)	BR (1,71%)
BR (1,15%)	IN (3,34%)	TW (3,76%)	JP (2,96%)	IT (3,24%)	TW (0,55%)	TH (0,22%)	JP (0,90%)

Entretanto, a proporção de mensagens enviadas por cada *country code* se altera em cada um. Dos oito *honeypots*, em cinco deles mais de 50% das mensagens recebidas são provenientes de US. Já nos outros três *honeypots*, a origem dos *spams* se distribui entre os vários *country codes*. Além disso, naqueles três, o número de mensagens concentrado nos cinco principais CCs é significativamente inferior ao dos demais, indicando uma maior distribuição da origem dos *spammers* nesses casos. Outro ponto interessante é que, embora os dois *honeypots* brasileiros estejam próximos geograficamente, a distribuição dos *country codes* originários das mensagens recebidas por eles é muito distinta. No BR-02, US representa mais de 50% dos *spams*, enquanto no BR-01 representa apenas 9,38%. Já as mensagens provenientes do próprio Brasil equivalem a mais de 11% dos *spams* recebidos pelo BR-01, sendo o segundo *country code* a mais abusar aquela máquina. Por outro lado, no BR-02 o *country code* BR é apenas o quarto, com cerca de 3% do total de mensagens recebidas.

Essa diferença de perfil chama a atenção pelo fato dos *honeypots* BR-01 e EC-01 estarem instalados em redes de "pior qualidade", segundo relatos dos membros da equipe que acompanham essas máquinas ao longo do tempo. Apesar de todos os coletores terem uma limitação de banda de entrada de 1 Mbps, a capacidade máxima dos links de acesso às redes onde estão aquelas máquinas é mais baixa que a do restante, além de serem conexões que ao longo do tempo se mostraram mais instáveis, com maiores taxas de perda, etc. Isso sugere que a semelhança entre essas máquinas (e sua diferença para as demais) pode ser

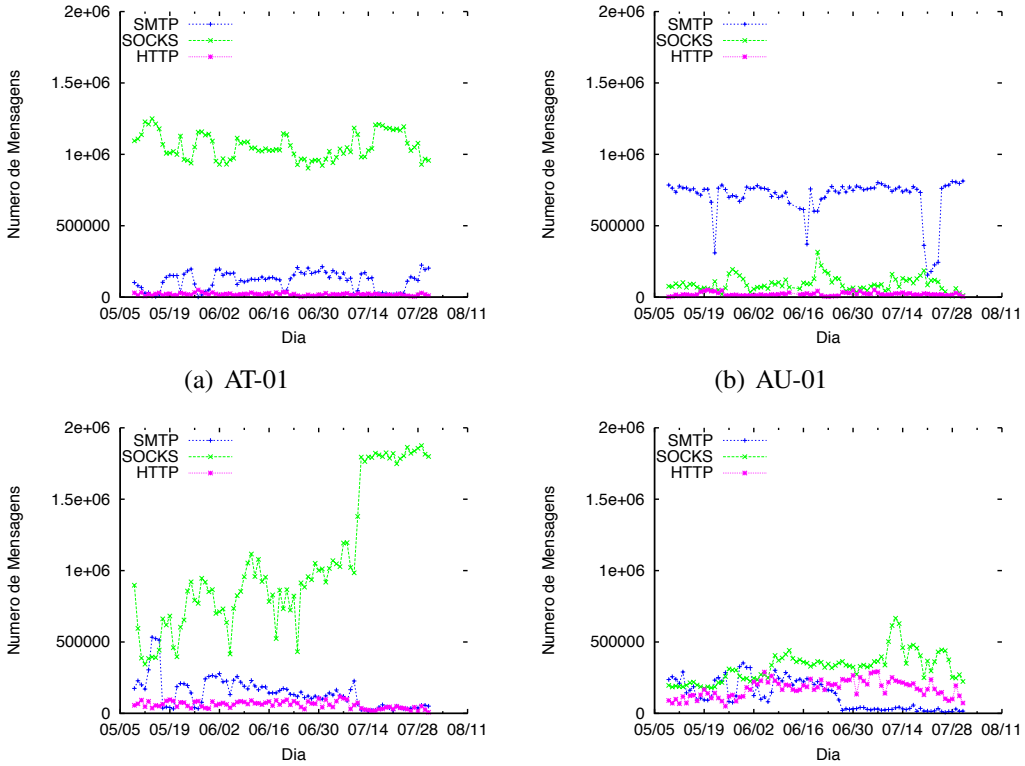
mais devida à sua conectividade que à sua posição na rede. Nesse sentido, TW-01 também se destaca, por ser o coletor na rede considerada de maior banda e qualidade.

Entretanto, fatores geográficos ainda podem desempenhar um papel na escolha dos *spammers*. Chama a atenção, por exemplo, o fato de que o único *honeypot* que não recebeu um grande volume de tráfego originado de CN (China) seja exatamente TW-01 (Taiwan). A razão para essa diferença não está clara e exigiria uma análise mais abrangente das condições (inclusive políticas) daquela região.

Tráfego de *spam* por protocolo

O tráfego apresentado por todos os *honeypots* apresenta variações ao longo do tempo. Entretanto, mesmo havendo variação, é possível perceber características gerais em cada *honeypot*, como mostrado nas figuras 3 e 4. Observando o AT-01, por exemplo, percebemos que o tráfego majoritário presente é causado por SOCKS, bem como no BR-02. Já o *honeypot* AU-01 possui maior parte do tráfego causado por SMTP, enquanto EC-01 possui um equilíbrio no tráfego gerado por cada protocolo, com uma queda no número de mensagens no final do período analisado. Considerando a discussão anterior, AT-01 e BR-02 estão em redes acadêmicas de boa qualidade, enquanto EC-01 está em uma rede mais limitada.

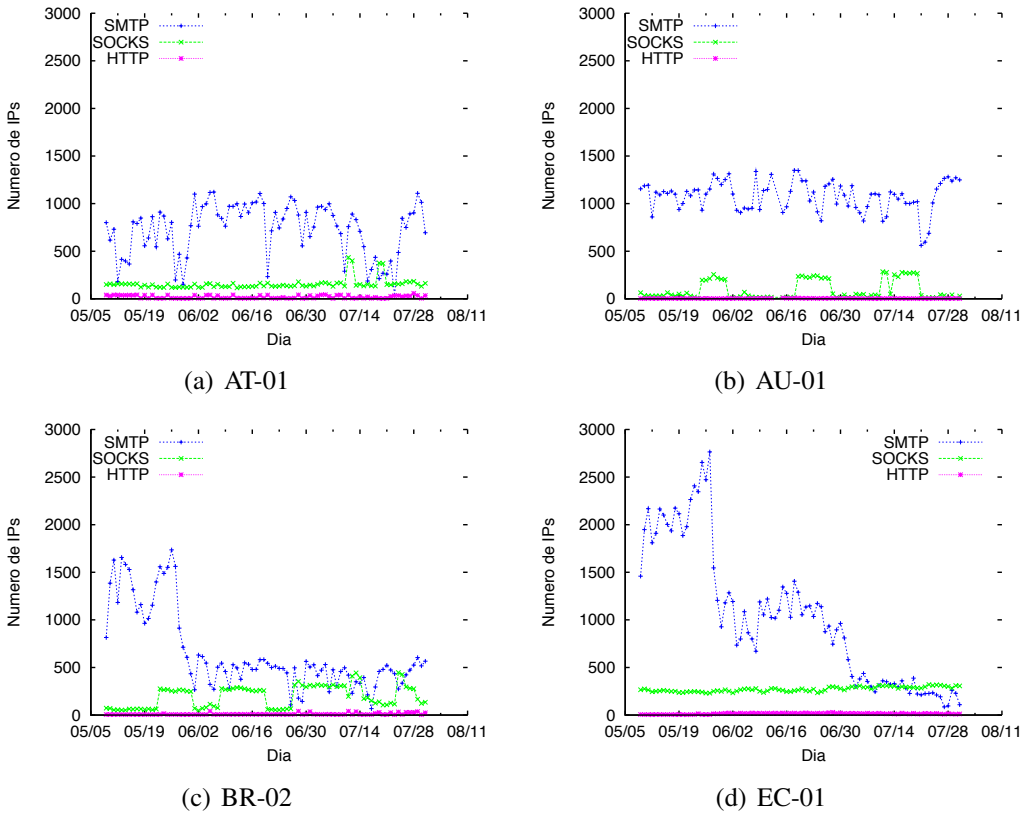
Com relação ao número de endereços de origem, todos eles apresentam número pequeno de transmissores utilizando SOCKS que, conforme observado anteriormente, enviam um número alto de mensagens. Além disso, possuem um número alto de transmissores explorando SMTP e um número quase irrisório de endereços de origem abusando a máquina através de HTTP.



(a) AT-01 (b) AU-01

(c) BR-02 (d) EC-01

Figura 3. Número de mensagens por protocolo



(a) AT-01 (b) AU-01

(c) BR-02 (d) EC-01

Figura 4. Número de endereços IP por protocolo

Mensagens de teste recebidas pelos *honeypots*

Uma característica interessante encontrada em todos os 8 *honeypots* é o padrão de mensagens de teste recebidas. Essas mensagens são geradas pelos *spammers* periodicamente e contêm em seu corpo a identificação da máquina que está aparentemente sendo utilizada para entregar o *spam* (nesse caso, um dos *honeypots*). Elas são identificadas no tráfego coletado e recebem tratamento especial, sendo as únicas mensagens que o *honeypot* realmente entrega, periodicamente, para garantir que o *spammer* ache que seu objetivo está sendo alcançado e continue a utilizar a nossa infraestrutura. Apesar de não serem apresentadas por questões de espaço, as curvas que representam o número de endereços IP que enviaram mensagens de teste são muito semelhantes entre todos os coletores, com correlações extremamente elevadas (muito próximas de 1,0, para a maioria dos casos). Além disso, o número de endereços de origem em comum é elevado, sendo maior que 90% em grande parte dos casos, comparando os *honeypots* par-a-par.

Foram encontrados 1.608 endereços IP enviando mensagens de teste em todos os *honeypots*. Desse total, 324 (20,2%) enviaram apenas mensagens de teste no período observado, enquanto os 79,9% restantes enviaram tanto mensagens de teste quanto *spams*. Outra característica desses endereços é que a maioria (77,5%) é proveniente de redes domésticas, de acordo com dados de *black lists* consultadas durante a coleta. Com base ainda nessas *black lists*, 32,5% são, garantidamente, máquinas infectadas por algum tipo de *malware*[2]. Além disso, 230 máquinas enviaram mensagens de teste para todos os

[2]www.spamhaus.org

honeypots e, dessas, 97% enviaram tanto mensagens de teste quando *spams* e 73,91% são máquinas infectadas. Esses fatores indicam que, normalmente os testadores são máquinas infectadas presentes em redes domésticas e que, além de testarem o funcionamento da máquina abusada, continuam enviando *spams* em paralelo a essas mensagens.

4.3. Análise baseada em campanhas

Em algumas das análises utilizamos o conceito de campanhas de *spam*. Uma campanha é um conjunto de mensagens que possuem um objetivo comum e uma mesma estratégia de disseminação [Guerra et al. 2008]. Neste trabalho utilizamos o algoritmo de agrupamento FPCluster para agrupar as mensagens com base em diversos de seus atributos e identificar as estratégias de ofuscação utilizadas. Esse algoritmo constrói uma árvore de padrões frequentes que é usada para extrair os padrões de agrupamento das mensagens [Totti et al. 2012, Guerra et al. 2008]. O mecanismo desenvolvido anteriormente foi estendido para realizar a identificação de campanhas existentes por vários dias, a partir do agrupamento de campanhas com mesmos atributos encontradas em dias consecutivos. Ao se realizar esse agrupamento, 448.123 campanhas de um dia foram agrupadas em 155.696 campanhas de maior duração.

A tabela 5 apresenta o percentual de campanhas em comum entre cada par de *honeypots* em relação ao total de campanhas do *honeypot* da linha. Os *honeypots* AT-01 e NL-01 possuem 23.367 campanhas em comum, o que representa 81,33% do total das campanhas do AT-01. TW-01 possui um número pequeno de campanhas em comum com os demais *honeypots*, e, em consequência, possui características muito distintas das demais máquinas. Essas indicações nos levam a crer que *honeypots* com muitas campanhas em comum possuem muitas similaridades, o que não acontece nos casos em que o número de campanhas em comum é baixa.

Tabela 5. Percentual de campanhas em comum entre os *honeypots*

	AT-01	AU-01	BR-01	BR-02	EC-01	NL-01	TW-01	UY-01	Total
AT-01	-	5,04%	9,06%	28,59%	0,82%	81,33%	1,95%	4,31%	28.731
AU-01	31,05%	-	52,43%	30,92%	21,30%	14,65%	7,98%	22,00%	4.663
BR-01	50,28%	47,25%	-	22,76%	15,48%	38,84%	5,80%	14,45%	5.175
BR-02	33,06%	5,80%	4,74%	-	6,02%	69,84%	2,50%	2,65%	24.844
EC-01	5,97%	25,23%	20,35%	37,98%	-	8,23%	6,22%	6,05%	3.936
NL-01	40,95%	1,20%	3,52%	30,40%	0,57%	-	1,71%	1,69%	57.068
TW-01	0,74%	0,49%	0,39%	0,82%	0,32%	1,28%	-	15,69%	76.215
UY-01	6,46%	5,36%	3,90%	3,44%	1,24%	5,05%	62,42%	-	19.159

Mais um fator interessante com relação ao impacto da rede em que o *honeypot* se encontra, é que aqueles localizados nas redes com maior qualidade possuem maior número de campanhas, enquanto os dois identificados anteriormente como estando em redes de baixa qualidade (BR-01 e EC-01) possuem um número muito menor de campanhas distintas. As campanha observadas em alguns momentos têm impacto direto sobre o perfil de tráfego observado, à medida que campanhas se iniciam ou terminam.

Aumento do número de endereços IP utilizando SOCKS

Nos gráficos referentes aos transmissores encontrados nos *honeypots* AT-01 e BR-02, (figs. 4(a) e 4(c)), são perceptíveis períodos em que há um aumento no número de endereços IP que enviam mensagens utilizando SOCKS. Nesses períodos é visível um degrau na curva, que sobe no início do intervalo e volta ao seu valor mais baixo após alguns dias. Observando as curvas para o número de mensagens observadas (figs. 3(a)

e 3(c)), podemos observar variações no tráfego SOCKS no mesmo período.

Para tentar explicar este comportamento, focamos aqui no primeiro aumento ocorrido no *honeypot* BR-02, por volta do dia 23/05. Identificamos as principais campanhas do período e os endereços das máquinas que dela participavam. O resultado pode ser visto na tabela 6. Inicialmente, aquelas campanhas são praticamente inexistentes, com um número muito pequeno de transmissores; no dia em que ocorre o aumento do tráfego elas passam a se originar de um grande número de endereços. Há claramente uma relação com o surgimento dessas novas campanhas, a participação de novos transmissores e o aumento do tráfego SOCKS.

Tabela 6. Número de endereços IP das 5 maiores campanhas do dia 23/05 ao dia 31/05

	22/05	23/05	...	31/05	01/06
Campanha 1	2	182	...	175	8
Campanha 2	2	170	...	174	9
Campanha 3	-	137	...	128	-
Campanha 4	-	137	...	130	-
Campanha 5	-	137	...	127	-

Queda do número de transmissores utilizando SMTP

Como pode ser visto nas figuras 4(c), e 4(d), durante o período de 26/05 e 01/06, houve uma queda visível no número de endereços IP que enviaram mensagens utilizando o protocolo SMTP em alguns *honeypots*. Para entender o motivo da queda, observamos as principais campanhas envolvidas neste período. A tabela 7 contém as maiores campanhas no dia 26/05, dia em que se iniciou a queda, e nos dias seguintes. Como podemos observar, essas campanhas foram perdendo força, algumas chegando até a serem encerradas. Isso sugere que a queda se deveu ao término dessas campanhas.

Tabela 7. Número de endereços IP das 5 maiores campanhas do dia 26/05

	26/05	27/05	28/05	29/05	30/05	31/05	01/06
Campanha 1	469	476	29	31	20	9	4
Campanha 2	256	180	0	0	0	0	0
Campanha 3	237	217	123	63	1	28	6
Campanha 4	236	11	0	0	0	0	0
Campanha 5	220	144	0	0	0	0	0

Outras análises semelhantes foram realizadas para outros pontos onde observamos mudanças bruscas no perfil do tráfego. Através dessas análises, concluimos que eventos externos, como o início ou término de uma campanha, têm forte impacto sobre os detalhes do perfil de tráfego observado, devendo ser considerado em análises de tráfego desse tipo.

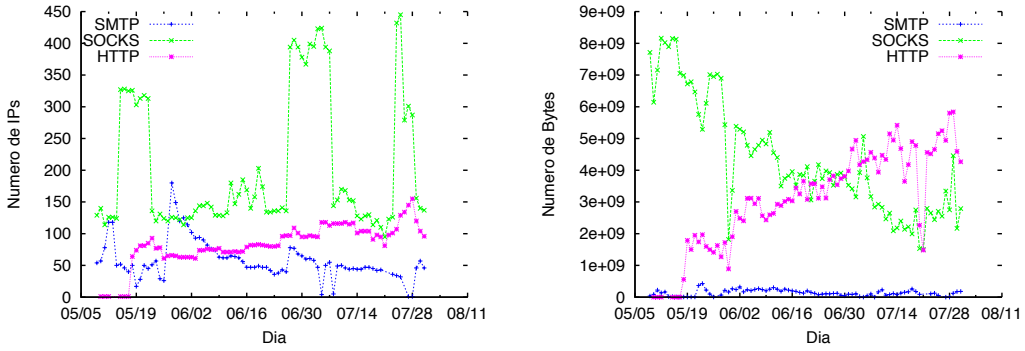
4.4. O *honeypot* TW-01

Conforme mencionado anteriormente, o perfil que mais difere dos demais foi o do *honeypot* TW-01. Apesar de apresentar um número muito pequeno de transmissores (2.194), o número de mensagens é muito alto, com mais de 207 milhões de mensagens, sendo maior que o de todos os demais *honeypots* individualmente.

Outro aspecto que diferencia TW-01 dos demais é o tráfego HTTP. Enquanto os outros 7 *honeypots* enviaram poucas mensagens utilizando esse protocolo ao longo do período, no TW-01 houve mais de 82 milhões de *spams* enviados dessa forma. Esse número representa quase 73% do total de mensagens utilizando HTTP recebidas por todos os *honeypots*. Todas essas mensagens recebidas pelo TW-01 foram enviadas a partir de

apenas 345 endereços IP.

Ainda com relação ao número de *spams* recebidos, o tráfego SMTP foi muito pequeno, representando apenas 1,4% do total. Já o tráfego SOCKS é bastante significativo, sendo utilizado por mais de 1.500 endereços IP e totalizando mais de 122 milhões de mensagens. Outro fator interessante desse *honeypot* está no número de campanhas presente em seu tráfego. Durante o período de 84 dias, mais de 76 mil campanhas distintas foram observadas no TW-01, o que representa quase 49% do total de campanhas presentes em todos os *honeypots*.



(a) Endereços IP por protocolo (b) Bytes por protocolo

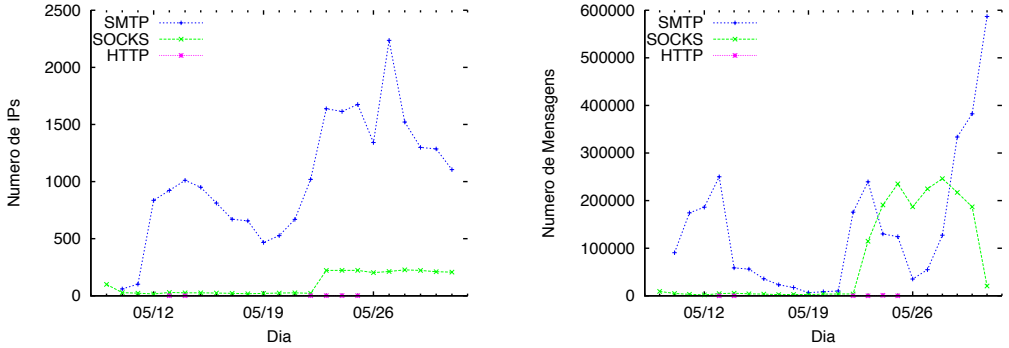
Figura 5. Características do *honeypot* TW-01

Como mencionado anteriormente, TW-01 está localizado em uma rede de alta velocidade e de qualidade superior à de todos os demais coletores. Esse perfil de rede parece beneficiar *spammers* que usam transmissão "por atacado", talvez porque esses transmissores tendem a permanecer ativos por mais tempo e se beneficiam da estabilização do algoritmo de controle de congestionamento de TCP. Dessa forma, eles teriam uma condição privilegiada para aproveitar a banda disponível, dificultando o acesso a máquinas de menos capacidade que enviam apenas poucas mensagens periodicamente. Provavelmente pelo mesmo motivo, aumentos significativos no número de transmissores usando SOCKS observados durante período em três momentos não tiveram grande impacto sobre o tráfego observado, pois os novos transmissores se viam em desvantagem ao concorrer pela banda disponível com os transmissores pesados já existentes.

4.5. Início do ataque a uma máquina vulnerável na rede

Por fatores externos ao projeto, o endereço IP de um dos *honeypots* foi alterado no início do nosso período de coleta. Apesar dessa máquina já estar em atividade há um longo período, a troca de seu endereço acabou simulando o aparecimento de uma nova máquina na rede. Com isso, foi possível analisar o processo do descobrimento de *proxies* e *mail relays* em uma máquina vulnerável por um *spammer*. Os gráficos da figura 6 mostram o comportamento do tráfego recebido por aquele *honeypot* logo após o seu ressurgimento na rede, usando o novo endereço pela primeira vez.

Logo no primeiro dia após o surgimento da máquina, cerca de 100 endereços IP já começaram a abusar da mesma, enviando cerca de 9 mil mensagens. Todos esses transmissores abusaram da máquina através do protocolo SOCKS. Uma possível explicação para o seu surgimento é que *spammers* que utilizam SOCKS vasculham a rede à procura de *proxies* abertos e quando encontram já começam a enviar *spams* através dos mesmos. Já os transmissores que utilizam SMTP apareceram somente no segundo dia após o apa-



(a) Endereços IP por protocolo (b) Mensagens por protocolo

Figura 6. Tráfego após surgimento do *honeypot* BR-01

recimento do *honeypot*, coincidindo com o aparecimento da primeira mensagem de teste enviada por um *spammers*. Esse fato leva a crer que os *spammers* que utilizam SMTP se valem mais de mensagens de teste para confirmar se a máquina a ser abusada realmente entrega as mensagens.

Após o primeiro dia, o número de transmissores enviando *spams* com SOCKS se estabiliza, com apenas alguns picos, em que o número de endereços aumenta consideravelmente (fato discutido na seção 4.3), assim como o número de mensagens enviadas por eles. Com relação aos endereços utilizando SMTP, a partir do segundo dia o número de mensagens de teste aumenta, coincidindo com o aumento do número de transmissores e do número de mensagens enviadas. A maioria dos transmissores que passaram a usar a máquina por SMTP nunca chegaram a fazer uma varredura da máquina antes do primeiro envio, nem usaram mensagens de teste, o que sugere que foram informados da existência do *honeypot* por algum canal externo (provavelmente através dos canais de comando e controle de uma *botnet*).

5. Conclusões e Trabalhos Futuros

O combate ao *spam* é uma tarefa contínua, onde se busca sempre entender melhor a evolução dos *spammers* e suas técnicas de disseminação de mensagens. Este trabalho buscou estender o entendimento sobre padrões de comportamento usado por esses transmissores com o objetivo de enviar seu tráfego mantendo-se ocultos atrás de máquinas intermediárias. Para isso, utilizamos uma análise do tráfego de *spam* no nível da rede.

Diferentemente de outros trabalhos anteriores na área, utilizamos um conjunto de máquinas geograficamente dispersas pelo mundo, a fim de coletar tráfego de *spam* em diferentes pontos da Internet. Isso nos permitiu observar que diversas características do tráfego, como tamanho das mensagens, endereços de origem e o uso de mensagens de teste, se repetem em diferentes locais. Por outro lado, certos detalhes como volume de tráfego instantâneo observado e a distribuição do tráfego entre protocolos e origens pode ser mais afetado por características da conectividade das máquinas atacadas e pelo padrão de ocorrência de campanhas que por fatores de localização. Acreditamos que essas observações serão úteis para outros pesquisadores que busquem mais informações sobre a origem do *spam*, a fim de viabilizar novas pesquisas na área.

Como trabalhos futuros, pretendemos avançar nas análises com a observação do

conteúdo específico das mensagens, para melhor entender a relação com localidades específicas, bem como realizar uma análise mais profunda dos padrões de tráfego de rede para confirmar as observações sobre o impacto da qualidade da conexão da rede atacada ao restante da Internet.

Agradecimentos

Esta pesquisa foi parcialmente financiada pelo Instituto Nacional de Ciência e Tecnologia para a Web - InWeb (MCT/CNPq 573871/2008-6), NIC.br, CNPq, Capes e FAPEMIG.

Referências

CERT.br (2013). SpamPots Project. *http://honeytarg.cert.br/spampots*.

Gomes, L. H., Cazita, C., Almeida, J. M., Almeida, V., e Jr., W. M. (2007). Workload Models of Spam and Legitimate E-mails. *Performance Evaluation*, 64(7-8):690–714.

Goodman, J., Cormack, G. V., e Heckerman, D. (2007). Spam and the ongoing battle for the inbox. *Communications ACM*, 50:24–33.

Guerra, P. H. C., Guedes, D., Meira Jr., W., Hoepers, C., e Steding-Jessen, K. (2008). Caracterização de estratégias de disseminação de spams. Em *SBRC 2008*, Rio de Janeiro, Brasil.

John, J., Moshchuk, A., Gribble, S. D., e Krishnamurthy, A. (2009). Studying Spamming Botnets Using Botlab. Em *6th USENIX Symp. on Networked Systems Design and Implementation*, Boston, EUA.

Kim, J. e Choi, H. (2008). Spam Traffic Characterization. Em *Int'l Technical Conference on Circuits/Systems, Computers and Communications*, Shimonoseki City, Japão.

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

Las-Casas, P. H., Guedes, D., Almeida, J. M., Ziviani, A., e Marques-Neto, H. T. (2013). Spades: Detecting spammers at the source network. *Computer Networks*, 57(2):526 – 539. Botnet Activity: Analysis, Detection and Shutdown.

Las-Casas, P. H. B., Guedes, D., Almeida, J. M., Ziviani, A., e Marques-Neto, H. T. (2011). Detecção de Spammers na Rede de Origem. Em *SBRC 2011*, Campo Grande, Brasil.

Newman, M. E. J., Forrest, S., e Balthrop, J. (2002). Email Networks and the Spread of Computer Viruses. *Physical Review E*, 66(3):035101.

Pu, C. (2006). Observed trends in spam construction techniques: A case study of spam evolution. Em *In Third Conference on Email and Anti-Spam (CEAS)*.

Ramachandran, A. e Feamster, N. (2006). Understanding the Network-Level Behavior of Spammers. *SIGCOMM Computer Communication Review*, 36(4):291–302.

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

Symantec (2011). Internet Security Threat Report, Volume 17. *http://www.symantec.com/threatreport*.

Totti, L. C., Moreira, R. E. A., Fazzion, E., Fonseca, O., Meira Jr., W., Guedes, D., Hoepers, C., Steding-Jessen, K., e Chaves, M. H. P. (2012). Impacto da Evolução Temporal na Detecção de Spammers na Rede de Origem. Em *SBRC 2012*, Ouro Preto, Brasil.

Xie, Y., Yu, F., Achan, K., Panigrahy, R., Hulten, G., e Osipkov, I. (2008). Spamming botnets: signatures and characteristics. *SIGCOMM Computer Communication Review*, 38(4):171–182.