Uma Análise do custo de tráfego de Spam para operadores de rede

- Riberto A. de Matos.
- Marcos T. Silva.
- Leandro Celini.

O que é SPAM?

*T*ermo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas.

Mensagens de spam são utilizadas para propagação de Malware, ataques de Phishing e venda ilegal de produtos. O spam gera custos para usuários, vítimas de Phishing, e para operadores de rede, que pagam pela transferência do tráfego.

2013

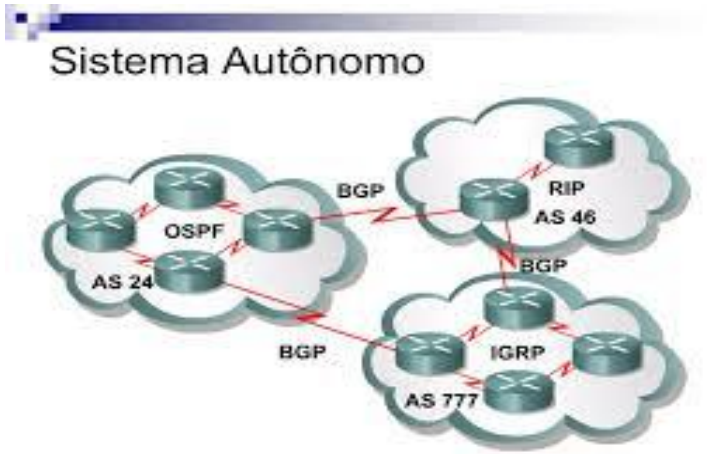
[Symantec 2014]

Desafios

- Identificar quais redes são oneradas pelo spam
- Obter amostra representativa do tráfego na internet
- Conhecer relações comerciais entre ASes e tráfego de spam

Sistema Autônomo (AS)

Uma entidade registrada junto as autoridades da Internet.



Honeypots

- As mensagens de spam que utilizamos em nossa análise foram coletadas de cinco honeypots instalados em diferentes países, dois no Brasil, um na Holanda, um nos Estados Unidos e um no Uruguai, em redes de diferentes características.
- Honeypots são máquinas que simulam servidores vulneráveis para atrair spammers.
- Os honeypots são configurados para simular proxies HTTP e SOCKS bem como relays SMTP abertos.
- Quando um spammer se conecta ao servidor SMTP de um Honeypots, ele é levado a crer que está interagindo com um servidor SMTP operando como um relay aberto.
- Quando uma máquina se conecta a um honeypot através dos protocolos HTTP ou SOCKS, é levada a crer que é capaz de estabelecer conexões com outros servidores SMTP na rede. Estes serviços são frequentemente utilizados para o envio de spam. Além disso, como esses protocolos são orientados a conexão, é improvável a ocorrência de IP spoofing (ataque que consiste em mascarar (**spoof**) pacotes **IP** utilizando endereços de remetentes falsificados.), que só seria possível se feito ao longo da rota de retorno dos pacotes e durante toda a duração da conexão.

Inferência das rotas trafegadas pelo spam

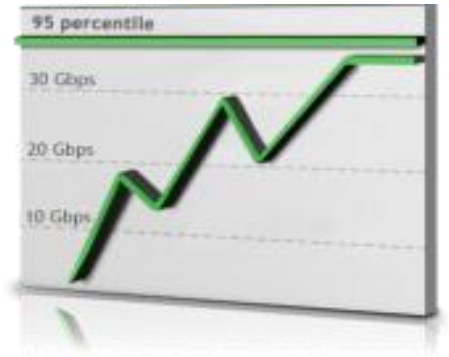
- Para inferir as rotas percorridas pelas mensagens de spam, primeiro coletamos medições utilizando traceroute e depois mapeamos os endereços IP nos traceroutes em sistemas autônomos (Ases) registrada junto as autoridades da internet
- Usamos as plataformas **RIPE Atlas** (que e uma das plataformas de medição dos parâmetros de rede na Internet de maior implementação no mundo todo) e **PlanetLab** (é uma rede de pesquisa mundial que permite o desenvolvimento de novos serviços de rede) para medir as rotas que seriam trafegadas pelas mensagens de spam dos honeypots até seus destinos, caso as mensagens tivessem sido entregues. Estas plataformas possuem monitores em milhares de redes ao redor do globo, inclusive nas redes dos honeypots.

Medindo as Rotas

- Para medir as rotas trafegadas pelas mensagens de spam dos spammers até os honeypots, seria necessário ter acesso a dispositivos próximos aos spammers. Essa abordagem não é prática pois as mensagens de spam são enviadas de 722 ASes distintos, 58,12% deles não cobertos por nós PlanetLab ou RIPE Atlas.

Mapeando endereços IP

- Como nosso estudo é baseado nas relações entre ASes, precisamos mapear endereços IP obtidos nas medições com traceroute em seus respectivos ASes.
- Utilizamos as bases de mapeamento de endereço IP em número de ASes do iPlane.



Analise de custos

- As rotas usadas para avaliação de custos, foi entre honeypot e as maquinas que enviam spam e entre honeypot e os domínios de destino.
- Grande parte dos contratos entre ASes o custo pela banda é proporcional ao 95° percentil da banda consumida em intervalos de cinco minutos.
- Algumas ASes tem seus prefixos anunciados para os provedores são separados, para distribuir e diminuir o 95° percentil do trafego.

Analise de custos

Tabela 3. ASes que mais pagam/recebem no BR-02 do *spammer* ao *honeypot*

MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
AS *Honeypot* BR-02, BR	66,5	Level 3, US (3356)	97,0
HiNetUSA, TW (9680)	44,1	HiNetUSA, TW (9680)	44,1
HiNet, TW (3462)	44,1	PacNet, HK (10026)	16,2
InfoSphere NTT PC, JP (2514)	14,0	TeliaSonera, SE (1299)	14,2
Internet INT Japan, JP (2497)	11,9	SprintLink (1239)	10,4

Analise de custos

Tabela 4. ASes que mais pagam/recebem no BR-02 do *honeypot* ao servidor de destino

MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
AS *Honeypot* BR-02, BR	1.898,7	Level 3, US (3356)	3.247,3
Yahoo-Switzerland, CH (42173)	1.346,4	Qwest, US (209)	538,1
KDDi Corp, JP (2516)	538,4	NTT-Comm, US (2914)	4,0
OCN NTT, JP (4713)	4,2	LVLT-3549, US (3549)	2,8
Microsoft Corp, US (8075)	2,7	TiNet-Backbone, DE (3257)	1,4

Analise de custos

A TW Cable recebe 4 vezes mais do que paga.

Tabela 5. ASes que mais pagam e recebem, por *honeypot*, pelo tráfego do *spammer* ao *honeypot*

ID	MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
	AS *Honeypot* BR-01	90,5	Embratel,BR (4230)	90,6
	Embratel, BR (4230)	48,0	Verizon, US (701)	39,7
BR-01	HiNetUSA, TW (9680)	24,0	HiNetUSA, TW (9680)	24,0
	HiNet, TW (3462)	24,0	SprintLink, US (1239)	17,5
	ROSTelecom, RU (12389)	10,2	TiNet-Backbone, DE (3257)	11,9
	AS *Honeypot* NL-01	86,7	TiNet-Backbone, DE (3257)	69,9
	HiNet, TW (3462)	30,4	HiNetUSA, TW (9680)	30,4
NL-01	HiNetUSA, TW (9680)	30,3	KPN Eurorings, NL (286)	20,7
	InfoSphere, JP (2514)	22,8	PacNet, HK (10026)	20,4
	OCN NTT, JP (4713)	5,6	TeliaNet, SE (1299)	16,3
	AS *Honeypot* US-03	58,4	XO Comm, US (2828)	32,1
	HiNet, TW (3462)	22,5	TWCable-Backbone, US (7843)	26,3
US-03	HiNetUSA, TW (9680)	19,7	Level 3, US (3356)	25,7
	CW CABLE AND WIRELESS WW, GB (1273)	5,4	HiNetUSA, TW (9680)	22,5
	TWCable-Backbone, US (7843)	5,3	TeliaNet, SE (1299)	13,7
	AS *Honeypot* UY-01	77,2	SprintLink, US (1239)	111,2
	HiNetUSA, TW (9680)	23,0	HiNetUSA, TW (9680)	23,0
UY-01	HiNet, TW (3462)	23,0	NTT-Comm, US (2914)	15,0
	InfoSphere, JP (2514)	12,3	TWGATE-AP, TW (9505)	9,4
	TWGATE-AP, TW (9505)	9,4	ROSTelecom, RU (12389)	9,0

Analise de custos

Apesar de algumas Ases estarem nas que mais pagam pelo trafego de Spam, a quantidade que elas recebem é sempre maior.

Tabela 6. ASes que mais pagam e recebem, por *honeypot*, por tráfego do *honeypot* aos servidores de destino

ID	MAIS PAGAM (ASN)	VOLUME (GB)	MAIS RECEBEM (ASN)	VOLUME (GB)
BR-01	AS *Honeypot* BR-01	2.230,9	Embratel, BR (4230)	2.230,9
	MailRu, RU (47764)	475,0	RETN Limited, UA (9002)	475,0
	Embratel, BR (4230)	61,4	Verizon, US (701)	104,9
	HiNetUSA, TW (9680)	47,3	HiNetUSA, US (9680)	47,3
	HiNet, TW (3462)	47,3	BTN, US (3491)	8,8
NL-01	AS *Honeypot* NL-01	3.866,8	POPPE, US (4525)	177,8
	Yahoo-JP-AS-AP, JP (24572)	177,8	GigaInfra, JP (17676)	177,8
	GigaInfra, JP (17676)	177,8	ROSTelecom, RU (12389)	156,2
	RTComm, RU (8342)	166,1	Verizon, US (702)	14,5
	Sovam, RU (3216)	14,5	IpTransit, US (46786)	12,6
US-03	AS *Honeypot* US-03	146,0	XO-AS15, US (2828)	136,1
	TransTelecom, RU (20485)	56,4	Level 3, US (3356)	125,6
	HiNet, TW (3462)	49,5	HiNetUSA, TW (9680)	49,5
	HiNetUSA, TW (9680)	49,5	Verizon, US (701)	48,9
	MailRu, RU (47764)	47,5	TransTelecom, RU (20485)	47,5
UY-01	AS *Honeypot* UY-01	1.478,2	SprintLink, US (1239)	1.486,5
	SeedNet, TW (4780)	9,0	Level 3, US (3356)	9,3
	BTN-ASN, US (3491)	8,5	BTN-ASN, US (3491)	8,5
	HiNet, TW (3462)	3,4	HiNetUSA, TW (9680)	3,3
	HiNetUSA, TW (9680)	3,3	ChinaNet, CN (4134)	2,6

Conclusão

- Algumas redes são sistematicamente oneradas pelo tráfego de Spam, mas que podem cooperar para reduzir o tráfego filtrando mensagens de spam na origem.
- Com monitoramento podemos alertar a ASes que estão tendo seus custos aumentados e alerta-los.
- Ocorre uma amplificação do trafego de mensagens Spam ao atingir servidores SMTP, nesse caso o volume pago pelo honeypot na saída pode aumentar mais de 3000%.
- O uso de filtro Spam que impeçam mensagens de atingir um servidor SMTP podem reduzir o trafego de rede, o impacto é bem maior que os filtros nos servidores de destino que não impedem todo esse gasto de recursos.

FIM