Experiências com um Honeypot DNS: Caracterização e Evolução do Tráfego Malicioso

Tiago Heinrich, Felipe de Souza Longo, *Rafael R. Obelheiro*

Programa de Pós-Graduação em Computação Aplicada
Universidade do Estado de Santa Catarina – Joinville

SBSeg 2017

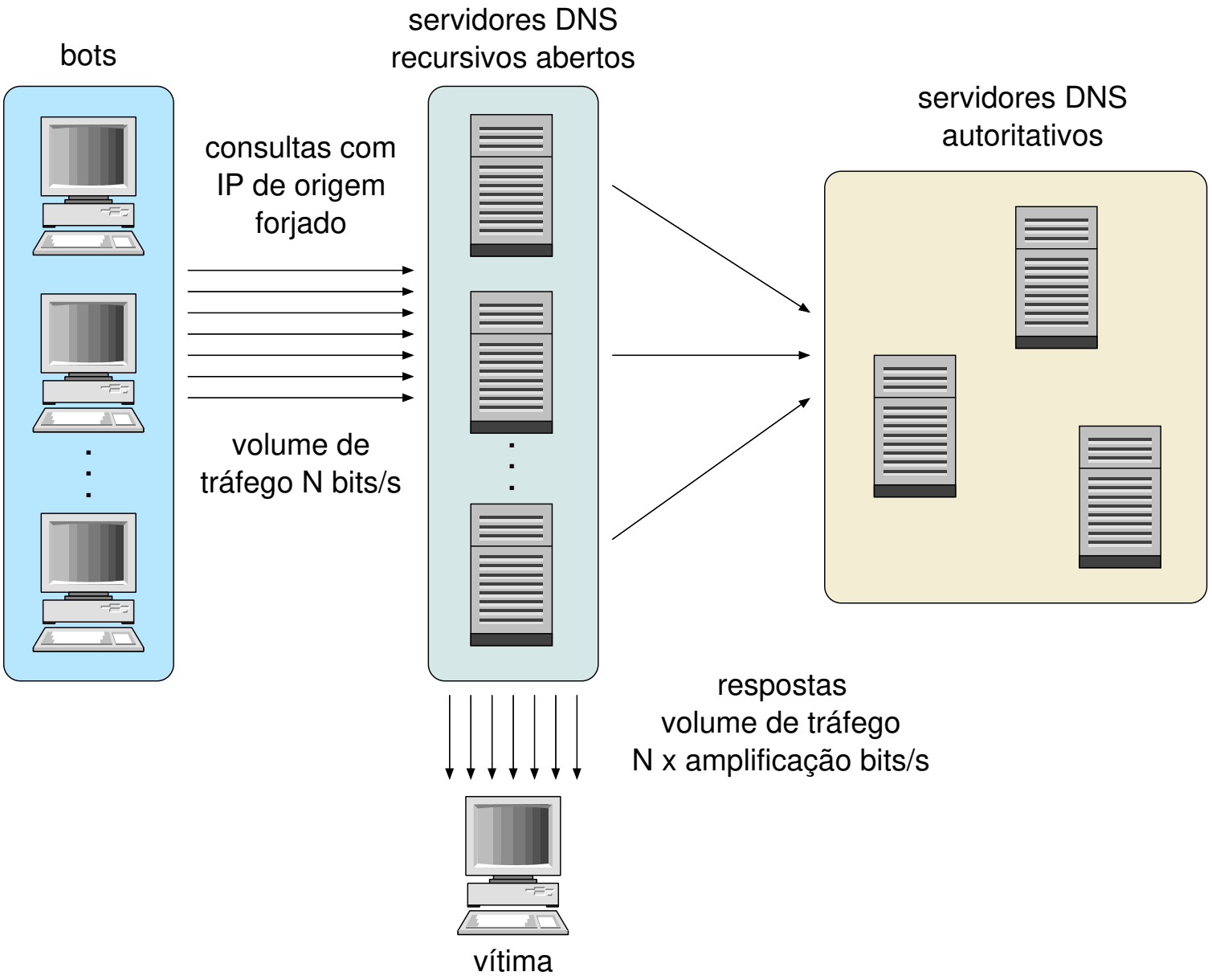
Brasília, 7 de novembro de 2017

Roteiro

Introdução

- O DNS desempenha um papel vital na Internet, tendo como principal funcionalidade traduzir nomes em endereços IP
- O DNS pode ser **alvo** de ataques
  - DoS contra usuários
  - falsificação de consultas/respostas/dados nos servidores
    - ★ redirecionamento de tráfego
  - vazamento de dados
    - ★ histórico de consultas de usuários
    - ★ identificação de alvos para ataques
- O DNS também pode ser **instrumento** de ataques
  - DDoS
  - canais cobertos
    - ★ C&C malware
    - ★ exfiltração de dados

Negação de serviço distribuída por reflexão (DRDoS)



Incidência de ataques DRDoS usando o DNS

- Em 2016, o DNS foi usado em 47% dos ataques DRDoS, gerando em média 3.083 Mbps por ataque; ataques aumentaram de 10.500 para 18.500 por semana[1]
- No 1º trimestre de 2017, 57% dos ataques DDoS observados eram baseados em reflexão, e o DNS foi um dos protocolos mais usados[2]

[1] Arbor Networks, *Worldwide infrastructure security report, vol. XII*

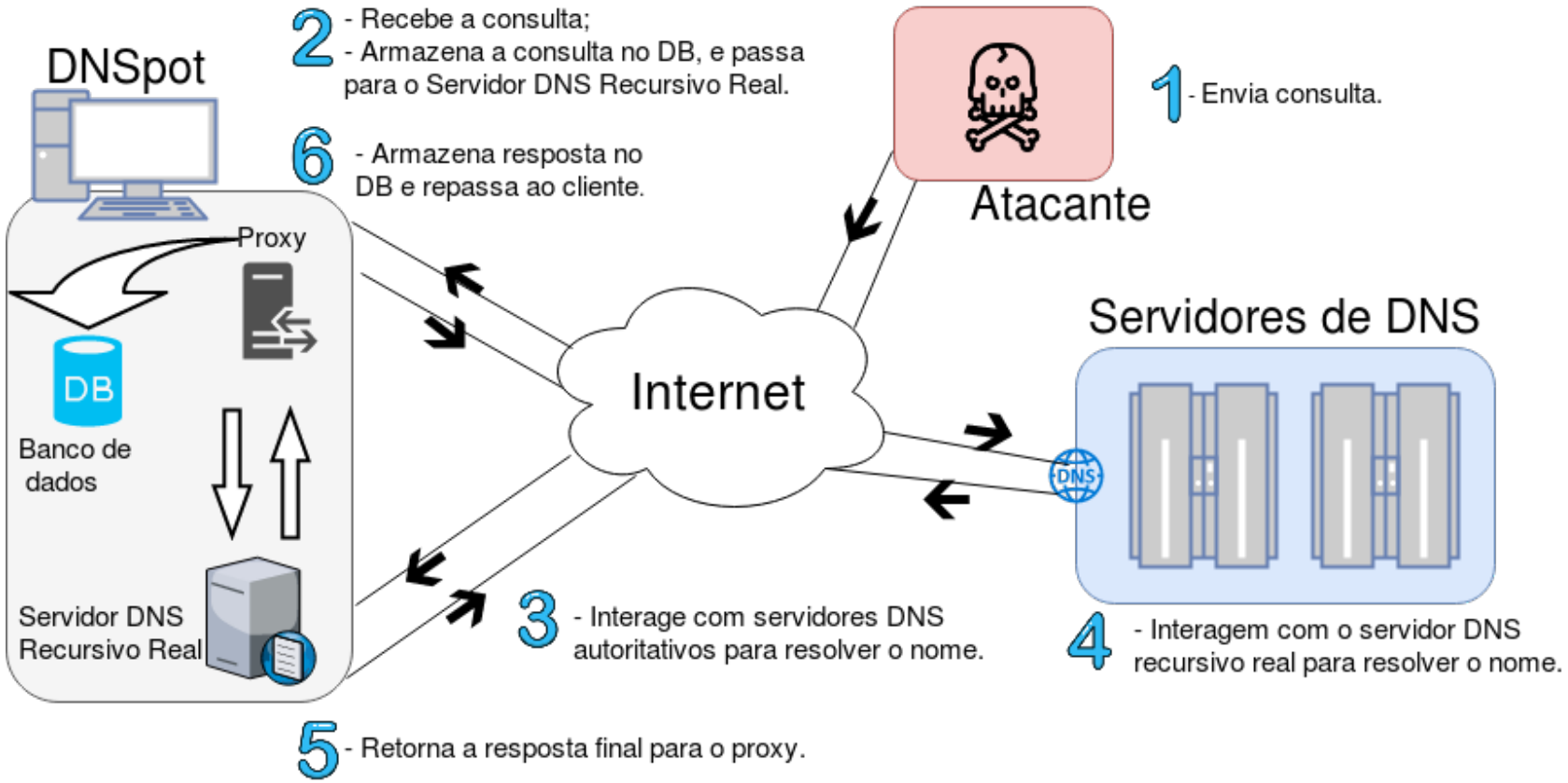
[2] Akamai, *Q1 2017 state of the Internet/security report*

Objetivo e contribuições

- **Objetivo**: investigar os ataques que podem ser efetuados contra um servidor DNS recursivo aberto
  - honeypot específico para DNS
- **Contribuições**
  - arquitetura de honeypot que permite interação controlada com um servidor DNS recursivo aberto
  - análise do tráfego coletado pelo honeypot em dois períodos
    - ★ 2015: 49 dias
    - ★ 2016–2017: 250 dias

Arquitetura do DNSpot

- Honeypot projetado especificamente para monitorar e analisar o tráfego DNS



Mecanismos de contenção

- Limite diário de consultas por IP de origem: reduz o tráfego enviado pelo DNSpot quando usado como refletor
  - consultas excedentes são processadas e armazenadas no BD, mas não respondidas
  - limite fixado em 30 nos nossos experimentos
- Mensagens falsas de erro: retorna mensagem de falha inespecífica do servidor (ServFail) com uma determinada probabilidade
  - ideia é aparentar inconfiabilidade, para não despertar suspeitas caso o honeypot falhe ou seja desligado
  - probabilidade fixada em 20% nos nossos experimentos
- Blacklists de nomes/sufixos: suprime respostas a varreduras por servidores recursivos abertos
  - p.ex., `openresolverproject.org`, `dnsresearch.cymru.com`

Implementação e coleta de dados

- DNSpot foi implementado em Python, usando Unbound para o servidor recursivo real e SQLite para o BD
- Datasets

Dataset	Início	Fim	Total (dias)
DS1	09/09/2015 07:57	28/10/2015 22:29	49,6
DS2	17/09/2016 08:00	25/05/2017 20:47	250,5

- Indisponibilidade estimada em 0,5–1% dos 300,1 dias

Estatísticas de consultas

Transações	DS1 Quantidade	%	DS2 Quantidade	%	Total Quantidade	%
Respondidas	488.289	**12,1**	1.600.386	**4,9**	2.088.675	**5,7**
– Válidas	391.050	*80,1*	1.280.425	*80,0*	1.671.475	*80,0*
– *ServFail* falso	97.249	*19,9*	319.961	*20,0*	417.210	*20,0*
Não respondidas	3.547.306	87,9	30.758.542	95,1	34.305.848	94,3
– Ignoradas	3.544.876	*99,9*	30.243.241	*98,3*	33.788.117	***98,5***
– Erros	2.370	*0,1*	515.301	*1,7*	517.671	*1,5*
Total	4.035.605	100,0	32.358.928	100,0	**36.394.533**	100,0

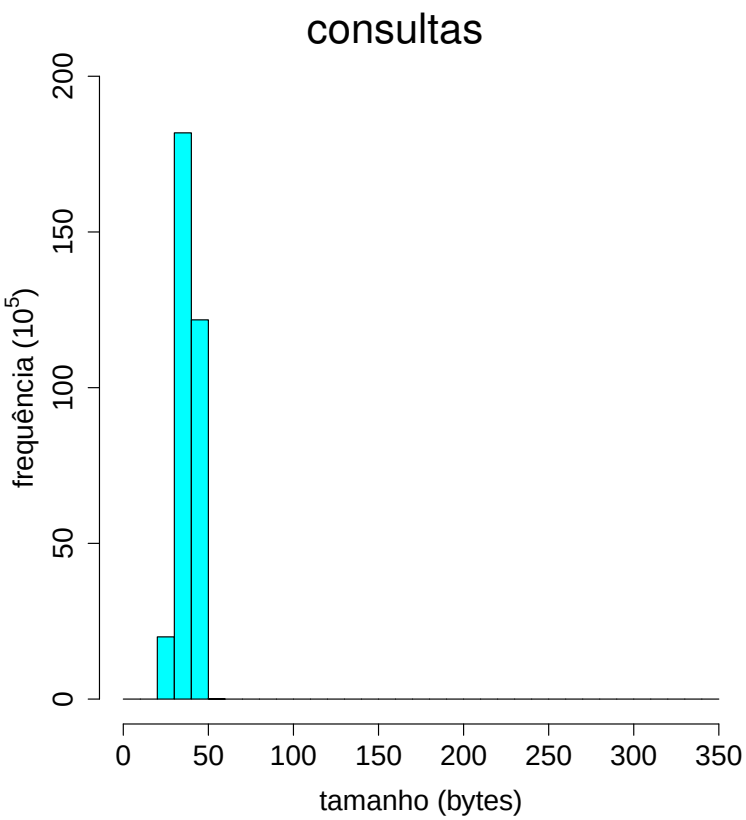
- Total de 36,4M consultas processadas
- Fração de consultas respondidas caiu em DS2
  - mais erros, maior intensidade e duração de ataques DoS
- Taxa média de processamento de requisições aumentou de 81k/dia (0,96 tps) para 130k/dia (1,50 tps)

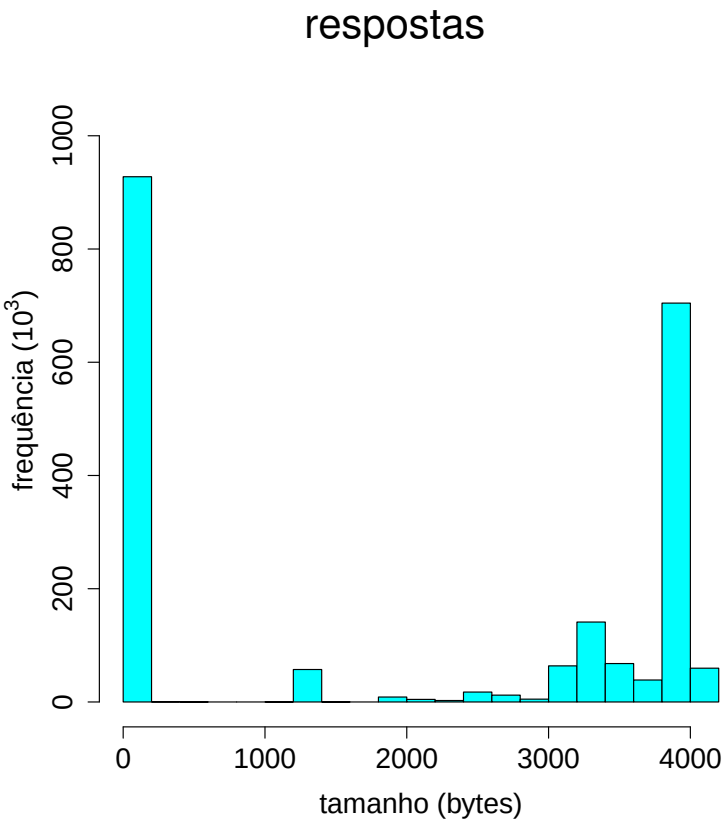
Volume de tráfego processado e esperado

Tipo	DS1		DS2		Total	
	MB	%	MB	%	MB	%
Tráfego processado	1.560,1	100,0	5.241,5	100,0	**6.801,6**	100,0
– Consultas	165,1	***10,6***	1.196,4	***22,8***	1.361,5	*20,0*
– Respostas	1.395,0	*89,4*	4.045,1	*77,2*	5.440,1	*80,0*
Tráfego esperado	14.775,6	–	34.775,9	–	49.551,5	–
Respostas	14.610,4	–	33.579,5	–	48.189,9	–
Redução de tráfego de resposta	13.215,4	90,5	29.534,4	84,9	42.749,8	**88,7**

- Total de 6,8 GB processados
- Restrição do número diário de consultas por endereço IP reduziu o tráfego de resposta em 88,7% (11,3% do pretendido)
  - aumento na proporção de consultas levou a uma redução menor em DS2
- Predominância de consultas ANY: 99,2% em DS1 e 94% em DS2 (94,6% no total)
  - especificações do DNS estão sendo alteradas para suprimir ANY

Tamanhos de consultas e respostas em DS2





- Consultas: 99,999% até 50 bytes
- Respostas: 43,9% até 100 bytes, 54,9% mais de 3.000 bytes
- Em DS1, um único RR (`hehehey.ru ANY`) apareceu em 97% das consultas (39 bytes) e 90,4% das respostas (3.850 bytes)

Top 5 países de origem

Posição	DS1 País	DS1 IPs distintos	DS1 %	DS2 País	DS2 IPs distintos	DS2 %
1	China	1.287	30,0	China	28.705	15,6
2	Estados Unidos	1.164	27,2	Estados Unidos	15.613	8,5
3	Rússia	759	17,7	Brasil	9.838	5,3
4	Alemanha	297	6,9	Coreia do Sul	6.815	3,7
5	Canadá	94	2,2	Japão	6.398	3,5
	outros	686	**16,0**	outros	117.195	**63,5**
Total	***73 países***	4.287	100,0	***161 países***	184.564	100,0

- Endereços podem representar origem de consultas ou vítimas de ataques DRDoS, que usam IP spoofing
- Diversidade aumentou tanto no número de países representados quanto na concentração de requisições
  - proporção do Top 5 caiu de 84% para 36,5%

Ataques DoS

- Para analisar ataques DoS, é necessário definir o que constitui um ataque desse tipo
  - não existe consenso na literatura

Definição

Um ataque DoS é formado por um conjunto com no mínimo 5 consultas com o mesmo IP de origem e com espaçamento máximo de 60 segundos entre consultas consecutivas, e pelas respostas a essas consultas

- Estabelecida empiricamente, considera que o DNSpot esteja sendo usado como um de vários refletores em um ataque DRDoS
- Não diferencia ataques DRDoS de ataques DoS contra o DNSpot, mas esses são pouco prováveis

Estatísticas de ataques DoS

	DS1		DS2	
N° de ataques	7.940		23.788	
Ataques/dia (média)	160,1		95,0	
Métricas	Total	Envolvidos em DoS	Total	Envolvidos em DoS
IPs	4.287	3.499 (81,6%)	184.564	23.745 (12,9%)
RRs	136	87 (64,0%)	4.982	840 (16,8%)
N° de requisições	4.035.605	4.032.778 (99,9%)	32.358.928	30.661.228 (94,7%)

- Redução na frequência de ataques e nas proporções de endereços IP, RRs e requisições envolvidos
  - explicada pela concentração de requisições (97%) em um único RR em DS1 e por um aumento nas consultas que não se encaixam na definição no final de DS2
  - proporção de requisições teve queda menos acentuada

Fator de amplificação de ataques DoS

- Fator de amplificação: razão entre o tamanho das respostas e o tamanho das consultas correspondentes

Fator de amplificação	DS1	DS2
Médio	96,3	74,1
Máximo	110,7	103,6

- Fator máximo foi comparável, mas o fator médio foi menor
  - 6,5% das consultas em DS2 tiveram fator de amplificação < 10
    - ★ nomes equivocados
    - ★ medidas de contenção do tamanho de respostas, como filtragem de ANY
- Maiores fatores foram observados para consultas ANY cujas respostas contêm diversos registros DNSSEC
  - corrobora outras referências

Duração e intensidade dos ataques DoS

- Duração dos ataques aumentou
  - DS1: 95% dos ataques duraram menos de 9 min
  - DS2: 50% dos ataques duraram até 8 min, e 25% duraram 19+ min
- Número de requisições por ataque também aumentou
  - mediana 17× maior, demais medidas aumentaram 12×

Dataset	média	mediana	3° quartil	95° percentil	máximo
DS1	507,9	132,0	402,0	2.100,2	25.363
DS2	6.029,7	2.264,0	5.024,0	25.594,4	203.474

Particularidades observadas (1)

- **Varreduras UDP e SIP**: requisições malformadas que foram classificadas como varreduras UDP típicas de Nmap e, o mais surpreendente, varreduras SIP (porta padrão 5060/UDP)
- **Domínios projetados para amplificação**: diversos domínios contendo RRs que não possuem nenhum significado ou utilidade para uma consulta normal DNS, servindo apenas para gerar respostas próximas a 4 KB úteis para ataques DRDoS
  - nomes com 250+ registros A na mesma sub-rede
  - nomes com 30+ registros TXT com 99 `x` (`xx...xx1`, `xx...xx2`, `...`)
    - ★ domínios diferentes mas mesmos registros SOA, NS, MX, A
- **Desaparecimento e redução de domínios**
  - 4º domínio mais popular em DS1 expirou durante a coleta, fazendo respostas caírem de 3875 para 96 bytes, mas continuou sendo usado
  - em DS2, 17 domínios desapareceram durante a coleta, mas as consultas não persistiram
    - ★ atualização de ferramentas de ataque?

Particularidades observadas (2)

- **Consultas por nomes equivocados**: número significativo de consultas por domínios obviamente inexistentes (`.3858`, `.pkt`), ou com tipos aparentemente trocados (TXT inexistente vs ANY com 4 KB)
- **Consultas de usuários finais** (DS2)
  - nomes de sites populares: `google.com`, `facebook.com`, `amazon.com`
  - nomes usados por ferramentas anti-malware: `avqs.mcafee.com`
  - nomes usados para descoberta de serviços (DNS-SD) com endereços de redes privadas (192.168.*.*)
  - fator de amplificação < 10, aumento no número de IPs distintos
    - ★ usuários finais usando o DNSpot como resolvedor regular? varreduras?

Discussão dos resultados

- Ataques DRDoS constituem o principal abuso
  - escolha adequada do nome consultado pode obter um fator de amplificação > 100, bem maior que os fatores típicos reportados (entre 28 e 54)[1]
  - limitação diária de consultas por IP restringiu o tráfego gerado pelo DNSpot a 11,3% do volume pretendido
- Volume significativo de requisições para um servidor não anunciado publicamente
  - 1,4 requisições por segundo, tráfego médio potencial de 165 MB/dia
  - primeiras requisições recebidas segundos após a ativação do honeypot, primeiro ataque DRDoS em < 28 h
- Análise da evolução entre as duas coletas revela diminuição na frequência dos ataques, mas um aumento relevante na sua duração e intensidade

[1] CERT.br, *Recomendações para melhorar o cenário de ataques distribuídos de negação de serviço (DDoS)*, 2016.

Conclusão

Pergunta que deu origem à pesquisa

O que acontece com um servidor DNS recursivo exposto à Internet?

Conclusão

Pergunta que deu origem à pesquisa

O que acontece com um servidor DNS recursivo exposto à Internet?

Conclusões

1. Vira refletor em ataques DRDoS!
2. Esses ataques vêm aumentando em duração e intensidade
3. No geral o tráfego DNS também vem aumentando de intensidade

- Perspectivas futuras
  - manter a coleta de dados, conjugando análises de curto e longo prazo
  - usar uma rede de honeypots distribuídos para monitoramento e detecção de ataques ao DNS

Experiências com um Honeypot DNS: Caracterização e Evolução do Tráfego Malicioso

Tiago Heinrich, Felipe de Souza Longo, *Rafael R. Obelheiro*

Programa de Pós-Graduação em Computação Aplicada
Universidade do Estado de Santa Catarina – Joinville

SBSeg 2017

Brasília, 7 de novembro de 2017

Distribuições empíricas da duração de ataques DoS