Caracterização e Evolução do Tráfego Malicioso Observado em um Honeypot DNS

Thiago Heinrich

Trabalha com ataques de amplificação, explora diferentes protocolos que podem ser utilizados para estes fins.

Explora DNS na realização de ataques DdoS

Principalmente por DNS mal configurados

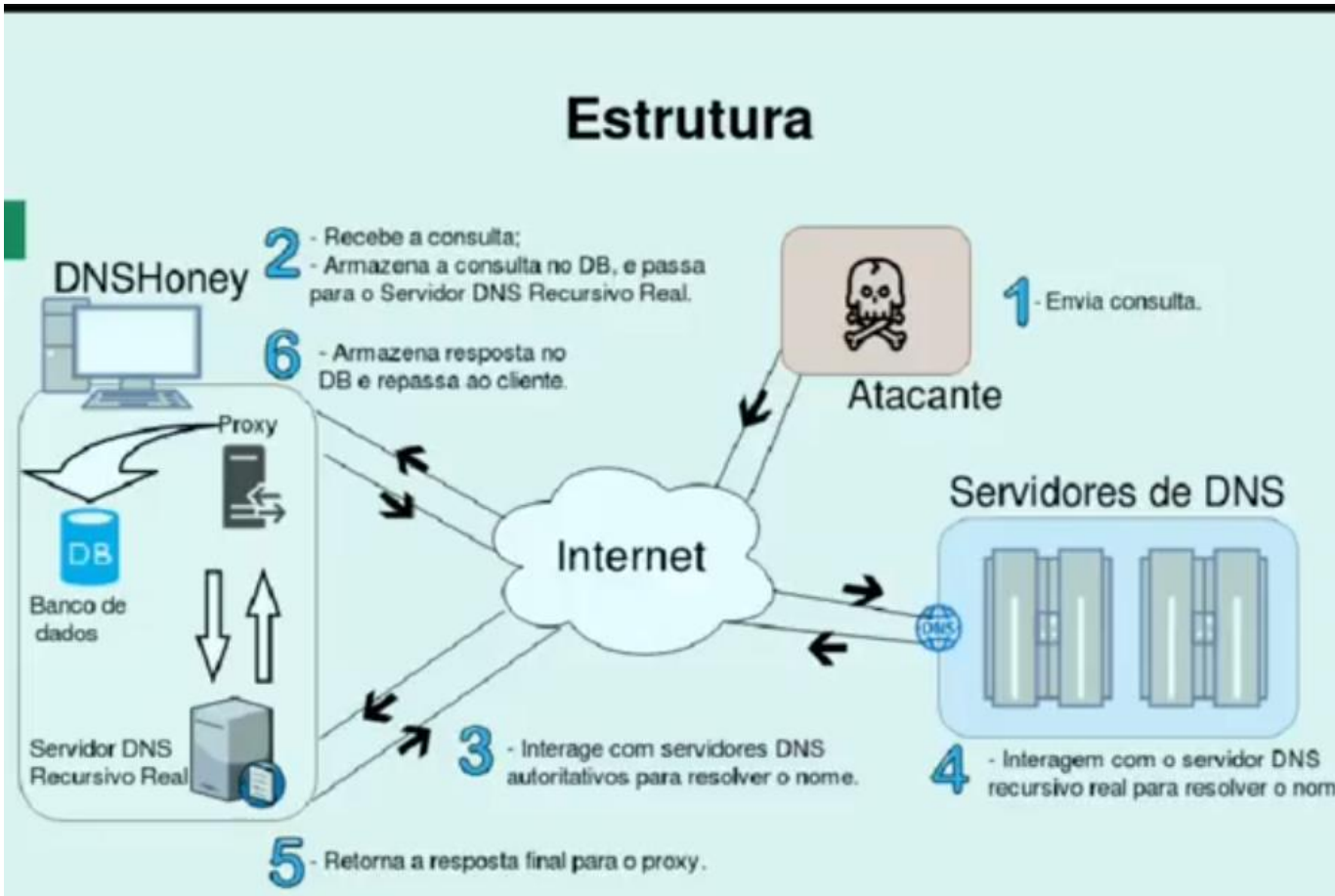
Análise através de um HoneyPot DNS, capturando tráfego. O atacante ta utilizando ele pra realizar os ataques (intermediário). Por esse motivo ele consegue identificar atitudes e comportamento e atvidades do atacante.

DdoS conjunto de protocolos.

Conjunto de máquinas infectadas ou botnets que vai realizar um conjunto de consultas no serviço de DNS Recursivo, Essas consultas vão ser resolvidas por um servidor autoritativo e serem encaminhadas para a vítima.

Ele sabe o conjunto de operação do atacante, mas, não sabe onde ele estava. O objetivo do trabalho foi fazer um honeypot para captura desse tráfego e análise.

Honeypot dele é uma máquina com porta 53 aberta, que é o que o DNS está ouvindo e buscando simular um serviço falho, responde 20% das consultas com serverfail.



Como ele é o proxy e não quer prejudicar ninguem, limita as consultas e resposta para cada vítima.

Ferramentas não verificam se o serviço parou de funcionar ou responder, porque pegam de uma lista pronta que não é atualizada frequentemente.

Existem ferramentas que varrem a internet e buscar open dns de por exemplos empresas que deixaram mal configurado, se identificam encaminham um aviso para a organização e para eles consertarem, ele tinha um conjunto de endereços que não iam gerar respostas.

Honeypot não era publicado, era somente encontrado por scanners.

No período de quase 600 dias teve o volume total de quase 60gb.

64 milhões de transações e 7% foram respondidas, 80% das consultas foram válidas para o honeypot.

Respondendo tão pouco, não gerou tanto impacto quanto poderia.

Processados 11.4gb de tráfego 18% consultas e 82% respostas. Princípio do DNS é gerar uma consulta pequena e gerar uma resposta maior

99.9% das consulta tinha 50bytes(normal) 44% das respostas geradas tinha até 50bytes, 45% das consultas respondidas tinha 2200bytes ou mais. Então tinha influencia em relação ao tamanho de amplificação.

Como o honeypot sabia o endereço das vítimas ele conseguia fazer alguns mapeamento, maior vítimas era nos estados unidos seguido da china e por fim brasil. Brasil está no topo por causa da localização do honey pot.

Domínios e RRs: 6,357 RRs Distintos, concentração de consultas em poucos RRs, 99% do tipo ANY

Domínios e RRs

-	RR	Fator de Amplificação	Porcentagem (%)
1	fema.gov ANY	92,6	27,0
2	nccih.nih.gov. ANY	45	13,0
3	wapa.gov. ANY	97,5	9,9
4	usgs.gov. ANY	5,6	9,1
5	1x1.cz. ANY	118,2	7,4
6	. ANY	50,8	6,0
7	NRC.GOV. ANY	51,3	4,0
8	nccih.nih.gov.pkt. ANY	45	2,9
9	leth.cc. ANY	90	2,4
10	diasp.org. ANY	1.3	1,9
-	**Média/Total**	**59.7**	**83.6**

4 pilares Any: Depurar domínios DNS(maior funcionalidade); Obter múltiplas informações com uma única consulta; Descobrir potenciais alvos de ataques ou produzir respostas grandes a partir de consultas pequenas, amplificando o tráfego

31% dos nomes aparentavam ser controlados e utilizados por uma ferramenta. 1 Grupo de numero reais = 8% RandomString.FixedName.com

Grupo2 não gerava resposta

14% das consultas era reverse dns lookup vindo de 99% de ips válidos

Algumas consultas de usuários finais “consulta em google.com e avqs.macaffee.com”(ou a máquina foi contaminada por algum tipo de bot ou malware)

Os que mais utilizaram eram composto pro caracter inválido e números _707_31_

Especificação dos ataques DoS, para caracterizar, algumas métricas foram utilizadas: Se em 60 segundos, receber 60 consultas consecultivas, vai considerar que está realizando algum tipo de ataque DdoS

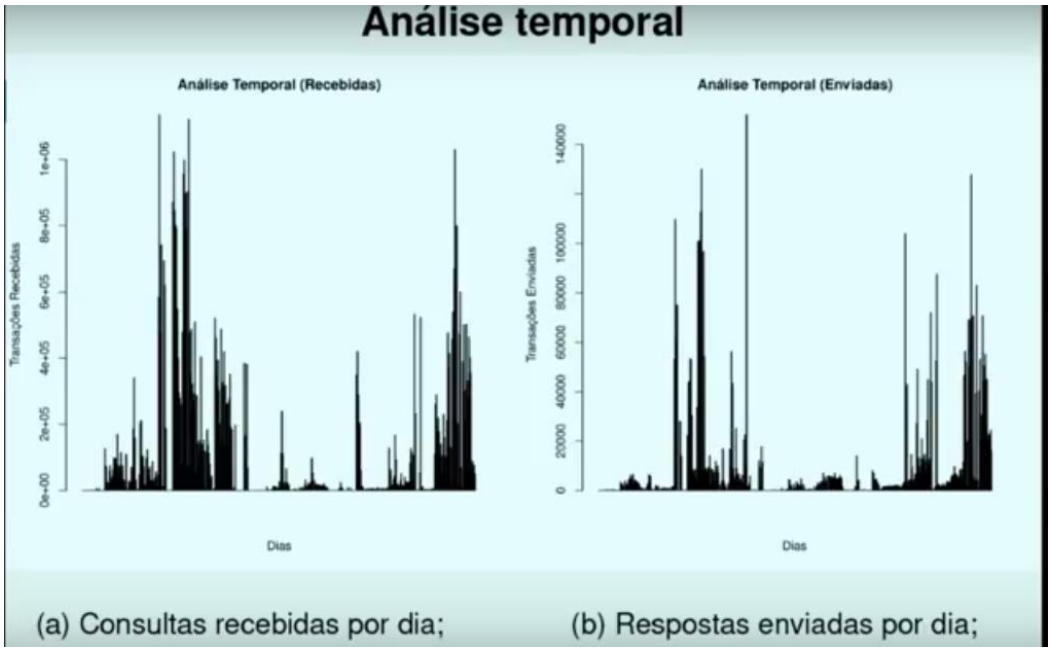
Média diária de tráfego recebido pelo honey pot: 109.444,7 requisições por dia

Duração dos ataques: 50% até 9minutos; 25% duraram até 18 minutos ou mais

- Um total de 26.375 IPs estavam envolvidos com ataques DoS ;
- 919 RRs foram utilizados nas consultas correspondentes a esses ataques ;

Métricas	Envolvido em DoS	Total	Porcentagem dos Envolvidos
Ips	26.375	280.457	9,4%
RRs	919	6.357	14,4%
Número de consultas	37.050.333	64.481.442	57,4%

57% participaram de ataques



Últimos 60 dias quase n recebeu nenhum, mas, em certos períodos observamos grandes picos.

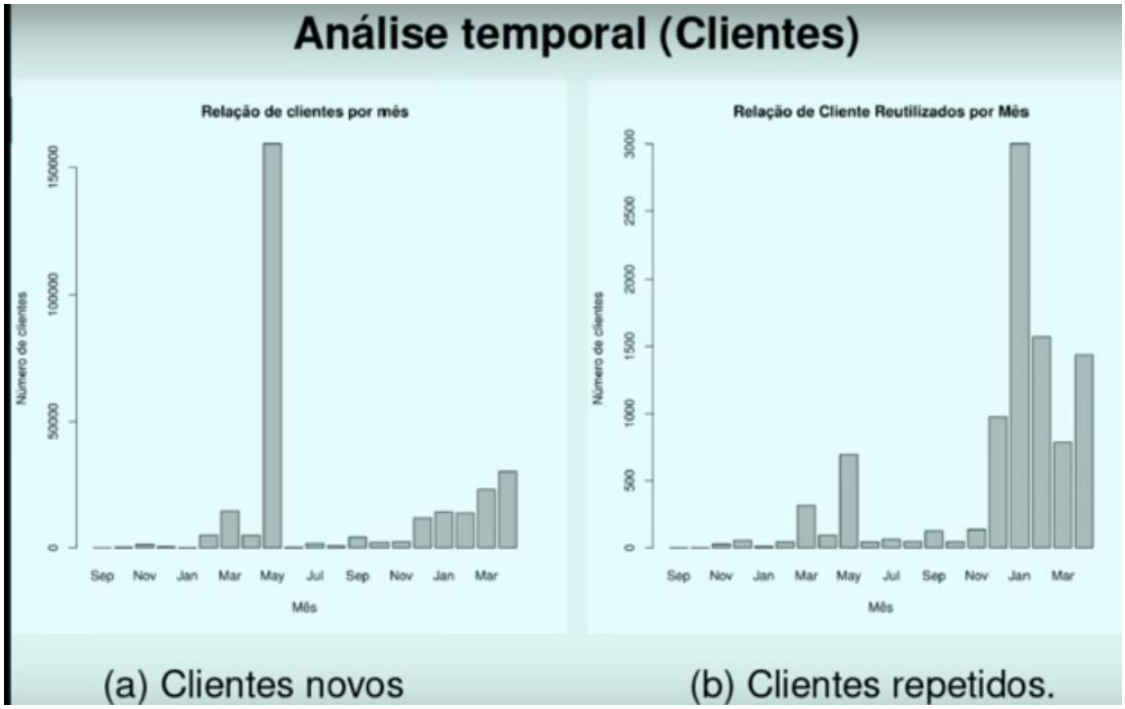
Especificação dos ataques DoS em 2018

- Média de requisições por dia 217.469,2 ;
- Duração dos ataques: 50% até 5 minutos; 25% duraram até 20 minutos; 5% até 35 minutos.

Requisições por ataque DoS

Média	Mediana	3 quartil	95 percentil	99 percentil	Máximo
4.094,3	1.411	2.940	14.518,5	52.636	203.474

Considerando o período, não houve uma queda considerável de uso



Período estranho em maio de 2017, explicado por uso do honey pot por usuários finais.
Considerando os últimos 5 meses, ele está sendo utilizado
Gráfico b representa clientes reutilizados.

Anomalias geradas como por exemplo varreduras feita pelo Nmap, consultas por nome equivocados e consultas por outros protocolos para amplificação como o Rcon

Conclusão: Ideia principal era saber o que acontecia quando um DNS Recursivo fosse exposto a internet.