Caracterização e Evolução do Tráfego Malicioso Observado em um Honeypot DNS

Tiago Heinrich e Rafael Obelheiro

Programa de Pós-Graduação em Computação Aplicada (PPGCA)
Campus Joinville

UDESC
UNIVERSIDADE DO ESTADO DE SANTA CATARINA

Contexto

- Ataques de amplificação;

- O Domain Name System (DNS) desempenha um papel central no funcionamento da Internet;

- Servidores DNS mal configurados para saturar vítimas com tráfego;

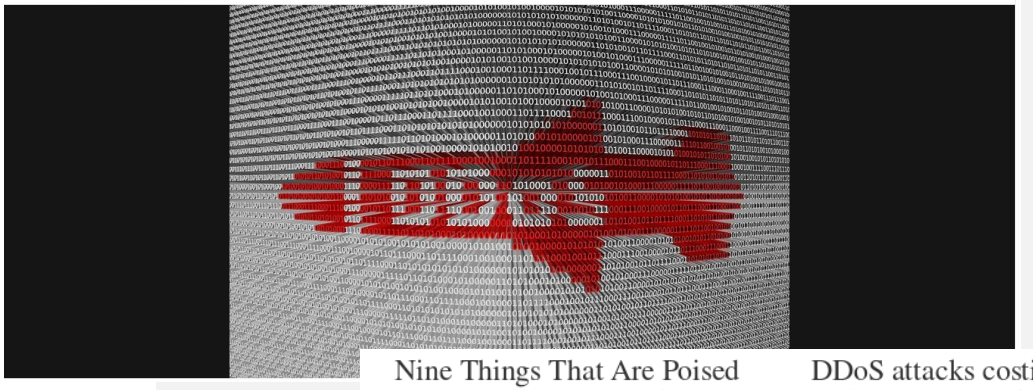
- Honeypot DNS.

Atualidade

Record-setting Australian DDoS attack is a reminder to get your IoT security in order

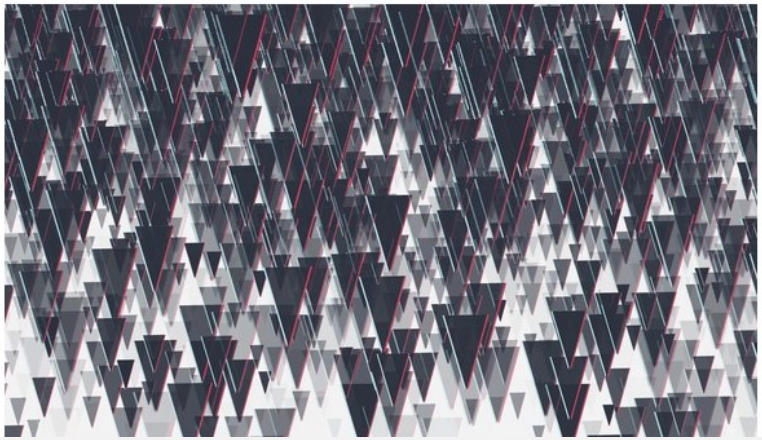
As IoT devices proliferate, security spend is becoming a corporate compliance issue

David Braue (CSO Online) on 09 April, 2018 12:13



LILY HAY NEWMAN SECURITY 03.01.18 11:01 AM

GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED



Nine Things That Are Poised To Impact Cybersecurity

April 19, 2018 - admin - 0 Comment

From the Equifax breach this past September to the recent hack of MyFitnessPal data through Under Armour, the number of high-profile cyberattacks has continued to climb in recent months. Every company, regardless of size, must be prepared for the possibility that they'll be the next victim. One important step every business should take to protect their sensitive customer data is invest…

Read More

DDoS attacks costing UK firms £35,000 per attack

April 18, 2018 - admin - 0 Comment

New research highlights the financial and reputational cost of DDoS attacks. New research has revealed that DDoS attacks can cost enterprises £35,000 per attack though lost revenue is only the fourth most damaging consequence of falling victim to this kind of cyber attack. Corero Network Security surveyed over 300 security professionals across a range of industries such as financial services,…

Read More

APAC is becoming a hotspot for DDoS attacks

April 18, 2018 - admin - 0 Comment

The region's largest and most-connected economies are most vulnerable to distributed denial-of-service attacks, according to CenturyLink. Some of Asia's

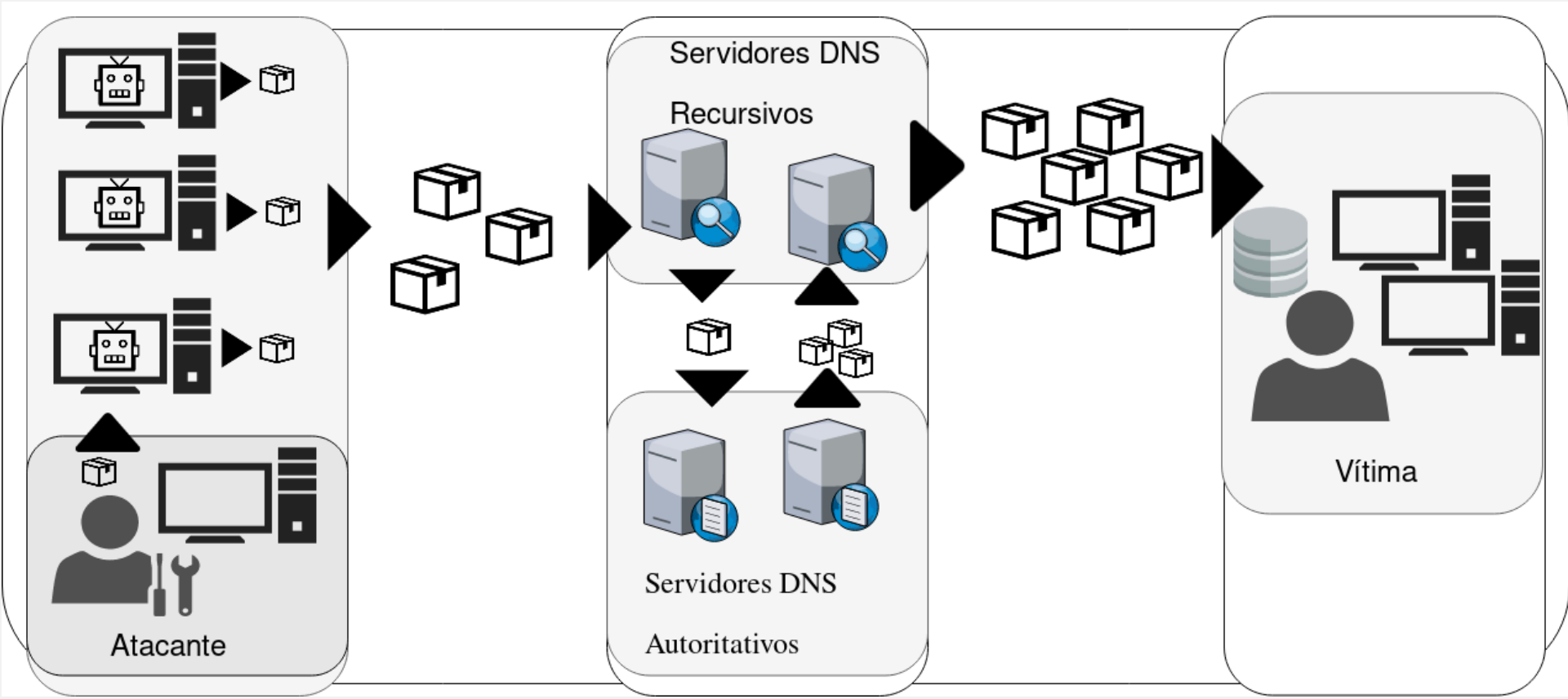
Here's how much money a business should expect to lose if they're hit with a DDoS attack

April 17, 2018 - admin - 0 Comment

More than two-thirds of organizations experience

UDESC

Distributed Reflection Denial of Service (DRDoS)

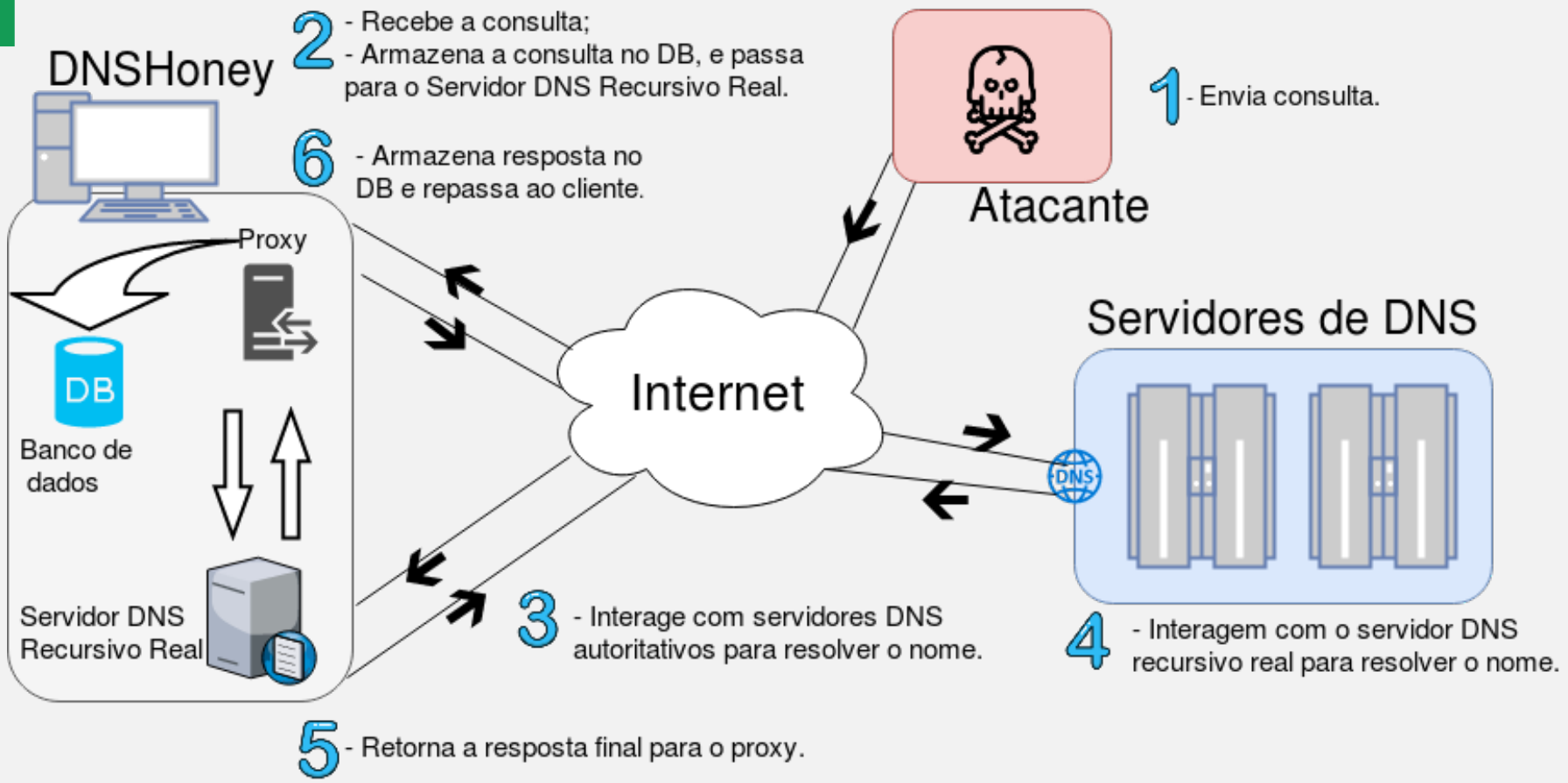


Objetivo

- Utilizar um Honeypot:
  - Coleta de informações;
    - Honeypots são recursos computacionais com o objetivo de serem sondados, atacados ou comprometidos.
  - Realizar interações com os atacantes.

  - Configurações:
    - Porta 53;
    - ServFail em 20%.

Estrutura


DNSHoney
2 - Recebe a consulta;
- Armazena a consulta no DB, e passa para o Servidor DNS Recursivo Real.
6 - Armazena resposta no DB e repassa ao cliente.
Proxy
DB
Banco de dados
Servidor DNS Recursivo Real
Atacante
1 - Envia consulta.
Internet
Servidores de DNS
DNS
3 - Interage com servidores DNS autoritativos para resolver o nome.
4 - Interagem com o servidor DNS recursivo real para resolver o nome.
5 - Retorna a resposta final para o proxy.

Coleta

- Estava localizado na rede da Universidade;
- O número de consultas diárias por endereço IP foi fixado em 30;
- Ocorrência de varreduras.

-	Início	Fim	Total (dias)	Total(horas)
Honeypot	17/09/2016	27/04/2018	588	14.112

Estatísticas de Tráfego

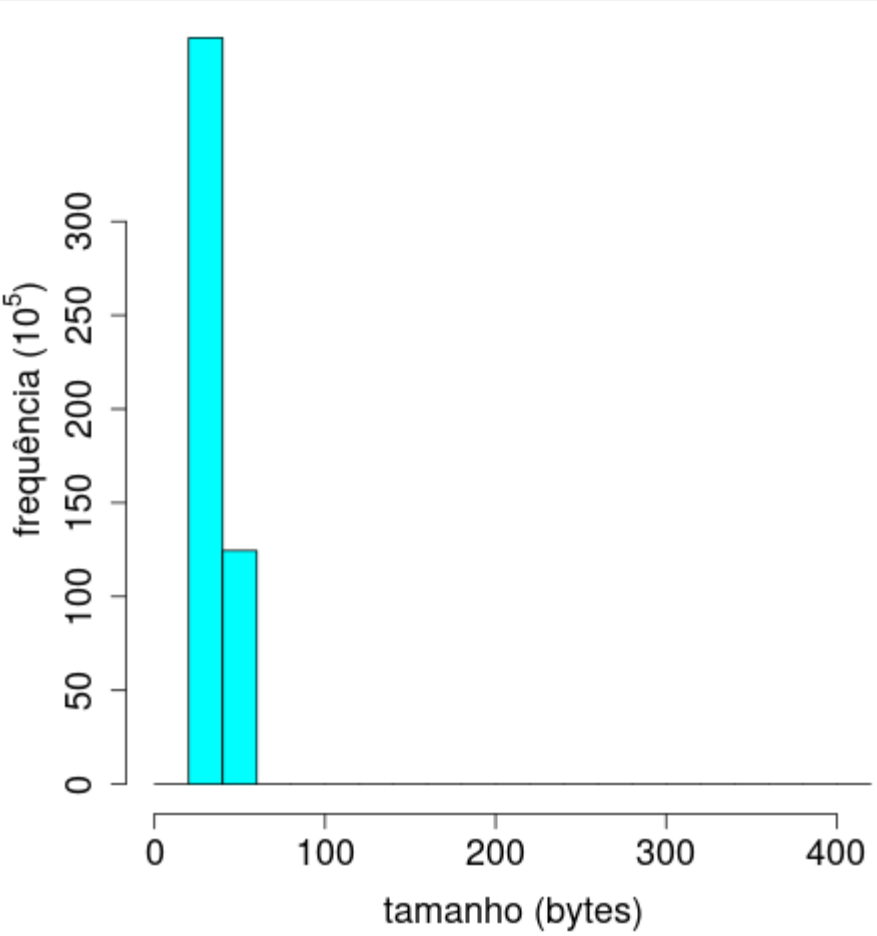
- Volume do banco de dados (59G) ;
- Interrupção da coleta;
- Total de 64 milhões transações;
- Respondidas 7.0% de todas as consultas recebidas;
  - 79.2% consultas válidas para as quais o honeypot enviou uma resposta para o cliente.
- Não respondidas 92.9%;
  - 94.9% ignoradas.

Volume de dados em bytes

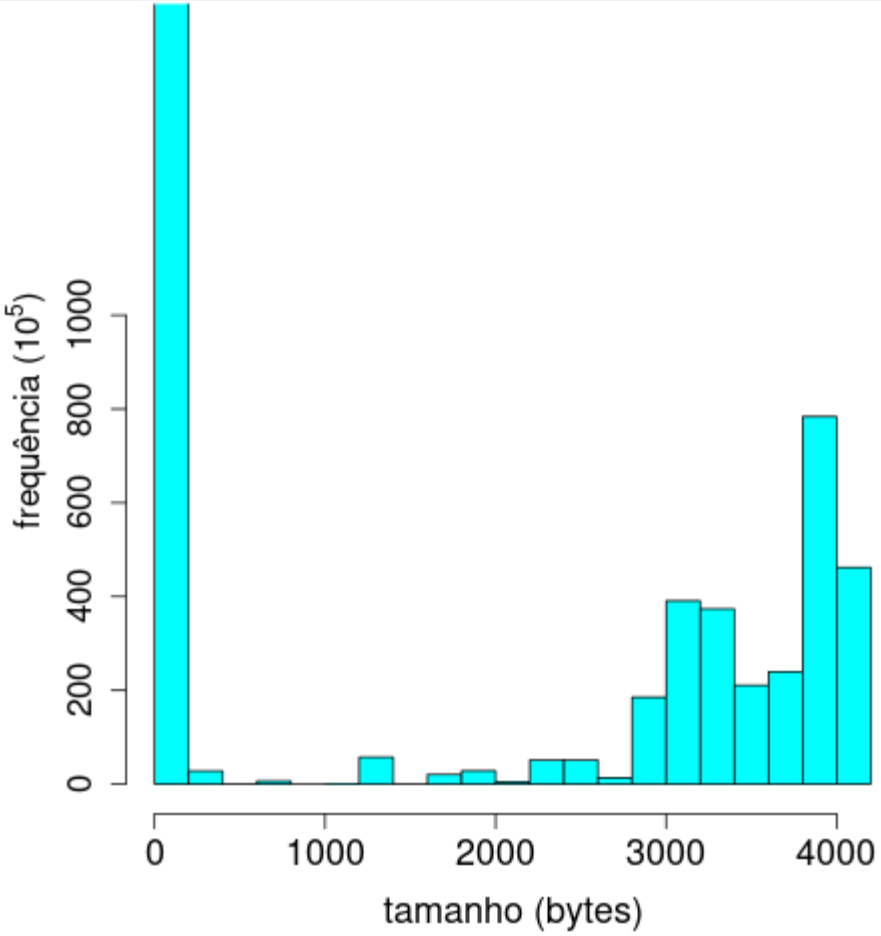
- Processados 11.4 GB de tráfego;
  - 1.8 GB (18%) de consultas;
  - 9.6 GB (82%) de respostas.

Transações	Quantidade	Porcentagem
Respondidas	4.533.586	7,0
– Válidas	3.594.433	79,2
– ServFail	939.153	20,7
Não respondidas	59.819.878	92,9
– Ignoradas	56.827.432	94,9
– Erros	2.992.446	5,0
Total	64.353.464	100,0
– EDNS(0)	61.713.962	95,8

Distribuição dos tamanhos de Consultas/Respostas



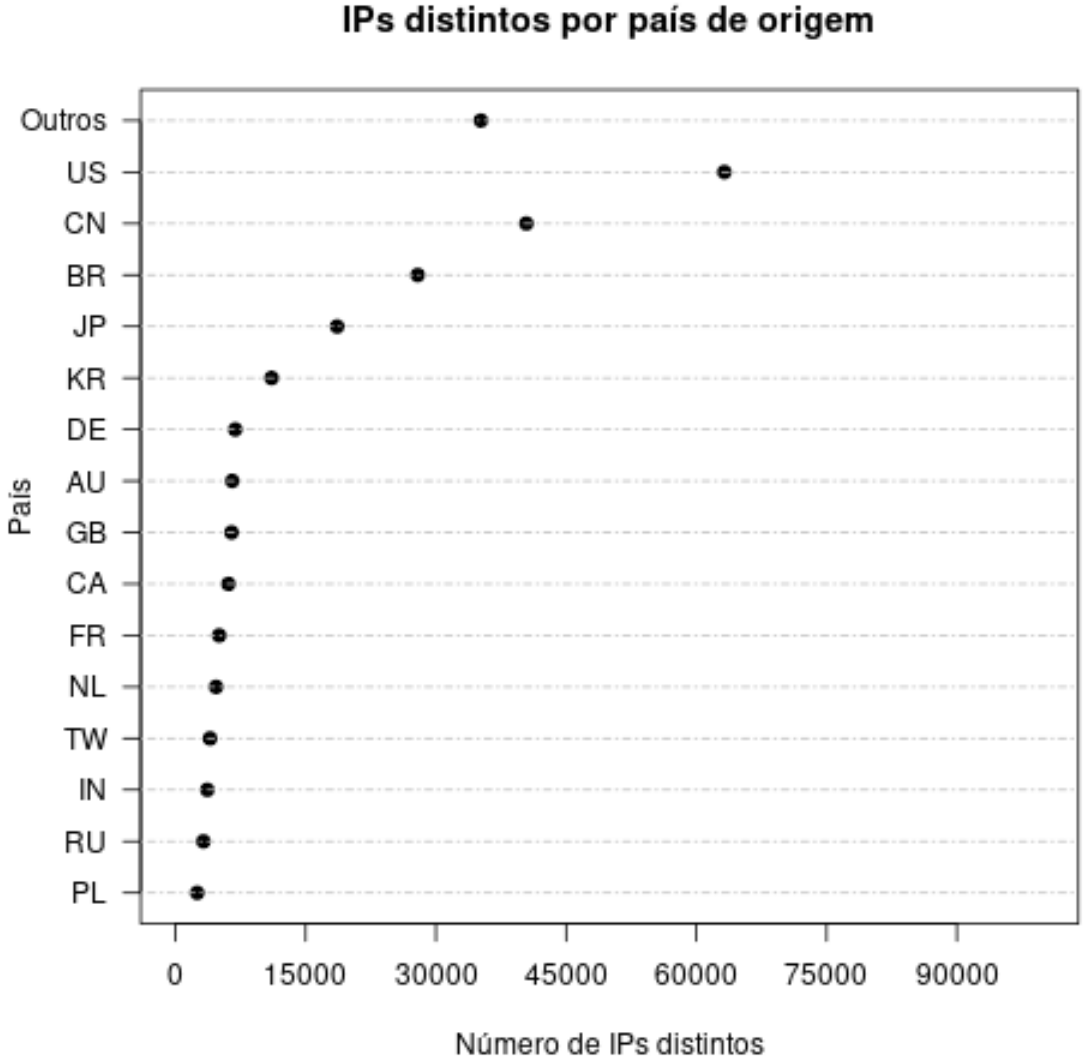
(a) Consultas;



(b) Respostas;

UDESC

Dados de Geolocalização



Domínios e RRs

- Total de 6.357 RRs distintos ;
- Concentração de consultas em poucos RRs;
- A ampla maioria das consultas observadas pelo honeypot é por RRs com tipo ANY;
  - 99% no total (ANY).
- ANY:
  - Depurar domíinios DNS;
  - Obter múltiplas informações com uma única consulta;
  - Descobrir potenciais alvos de ataques, ou;
  - Produzir respostas grandes a partir de consultas pequenas, amplificando o tráfego.

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**

Conjunto de nomes controlados

- 31% dos nomes que foram consultados no honeypot;

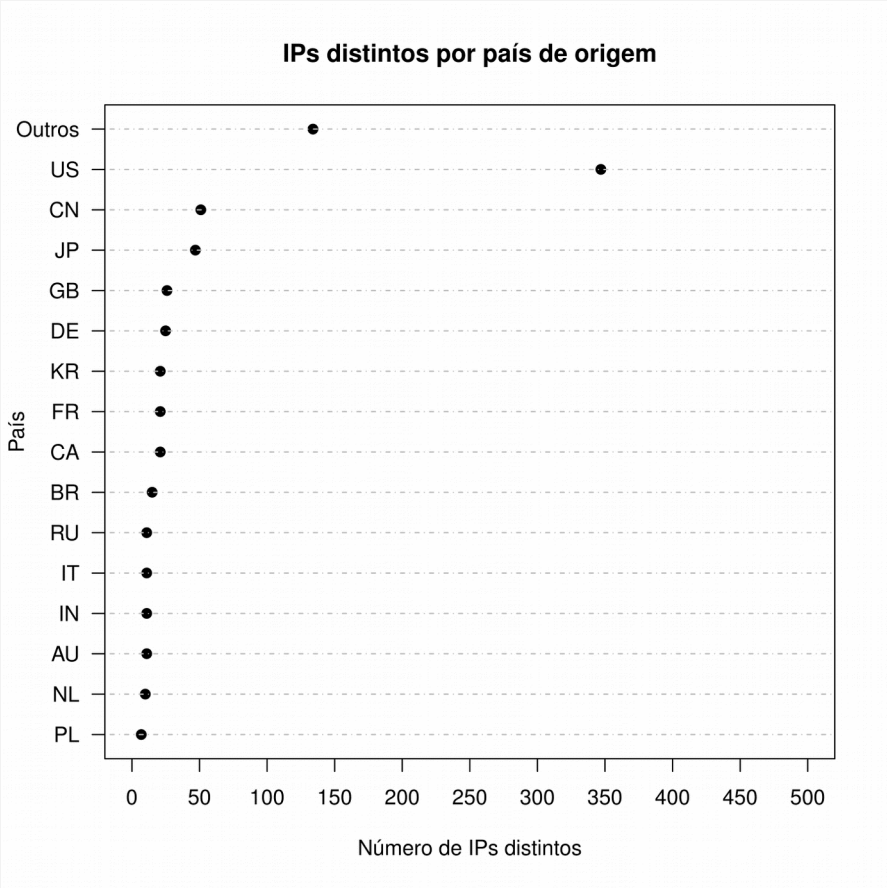
- Foram identificados um total de 9 domínios, que aparentavam estar sendo utilizados por *softwares* específicos, estes apresentam uma variação no nome consultado;

- **Grupo 1:**
  - Nomes reais (8% dos nomes utilizados);
  - ***RandomString.FixedName.com.*** ;
  - Conjunto de nomes não apresenta um período fixo de retorno.

- **Grupo 2:**
  - Associados com nenhum nome existente (domínio inexistente);
  - Mal configuração do *software* ;

Reverse DNS lookup

- Este compõe 14% de todas as consultas realizadas:
  - IPs reservados (0.02%); 127.0.0.1, 192.168.*.* e 10.*.*.*
  - IPs Válidos (99%);
  - DNS-SD (0.02%). b. db. dr. lb. r.



(a) Geolocalização IPs válidos;

Domínios projetados para amplificação

- Diversos domínios contendo RRs que não possuem nenhum significado;
- Único propósito aparente é gerar respostas grandes (próximas a 4~KB) ;
- Exemplo:
  - Nomes com mais de 250 registros A pertencentes a uma mesma sub-rede;
  - Nomes com mais de 30 registros TXT cujo conteúdo é a letra “x” repetida 99 vezes combinada com um sufixo numérico;
- Mesmos registros SOA, NS, MX e A associados ao nome;

Domínios projetados para amplificação

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11143
;; flags: qr rd ra; QUERY: 1, ANSWER: 40, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;hehehey.ru.                            IN          ANY

;; ANSWER SECTION:
hehehey.ru. 600 IN  TXT  "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx9"
hehehey.ru.  600 IN  TXT "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx10"

;; MSG SIZE rcvd: 3850
```

Consultas de usuários finais

- Consultas por nomes tipicamente associados a usuários finais;
  - *google.com*, *facebook.com*, *amazon.com*
- Nomes usados por ferramenta:
  - *avqs.mcafee.com* e *.baidu.com.*
- Fator de amplificação é baixo (<10);
- Incremento no número de endereços IP distinto;
- Descoberta de serviços de rede:
  - DNS-SD, DNS-Based Service Discovery.

Desaparecimento e redução no tamanho de domínios

- Mudanças no conteúdo dos domínios consultados que levaram à redução no fator de amplificação;

- Poucas consultas após o desaparecimento dos RRs.

Conjunto de nomes inválidos

- Foram identificados três grupos de nomes inválido;

- **Grupo 1:**
  - Única consulta;
  - Nome que só possuía caracteres inválidos;
  - Sem relação com algum outro nome.

- **Grupo 2:**
  - Conjunto de nomes que contém caracteres inválidos;
  - Total de 68 nomes;
    _707_31_

- **Grupo 3:**
  - IDN DNS;
  - Somente um nome.

Especificação dos ataques DoS

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.

- Média de 109.444,7 requisições por dia;
- Duração dos ataques: 50% até 9 minutos; 25% duraram até 18 minutos ou mais.

Requisições por ataque DoS

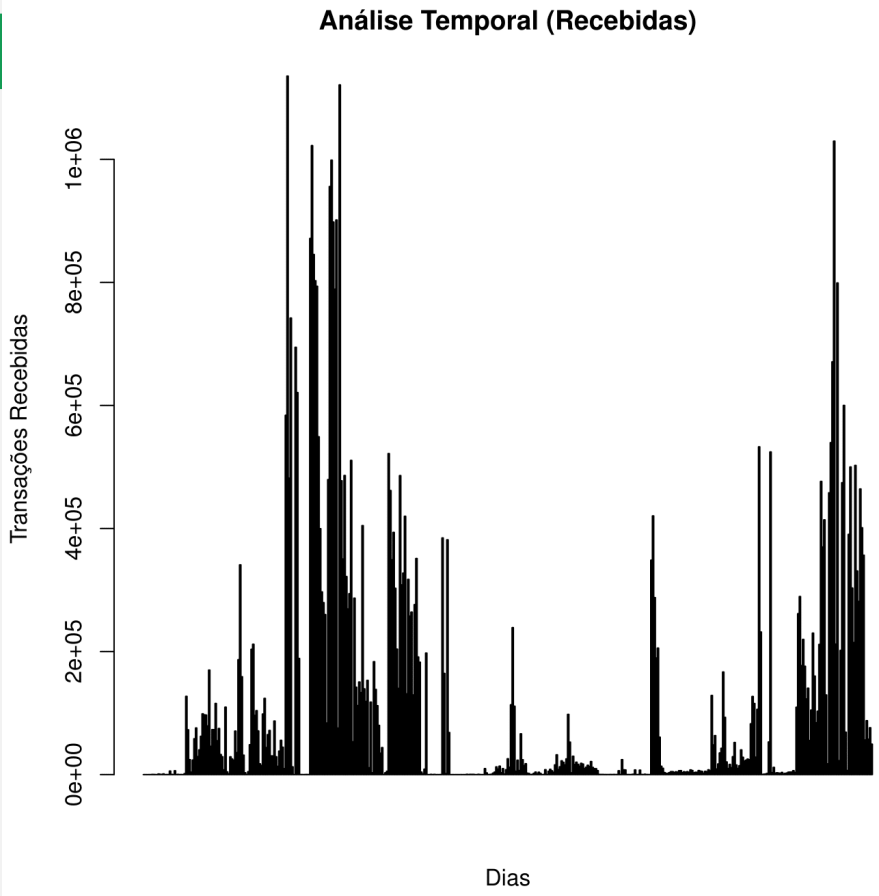
Média	Mediana	3 quartil	95 percentil	99 percentil	Máximo
6.342,7	2.323	5.115,5	27.705,4	73.721,9	227.328

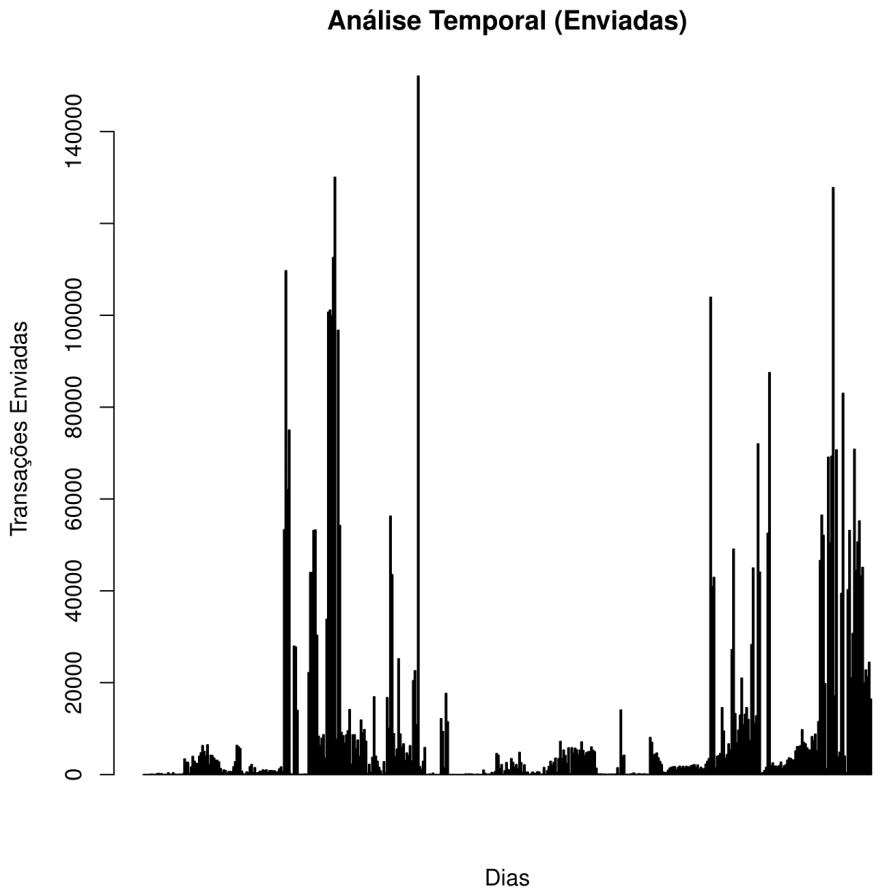
Ataques DoS

- 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%

Análise temporal

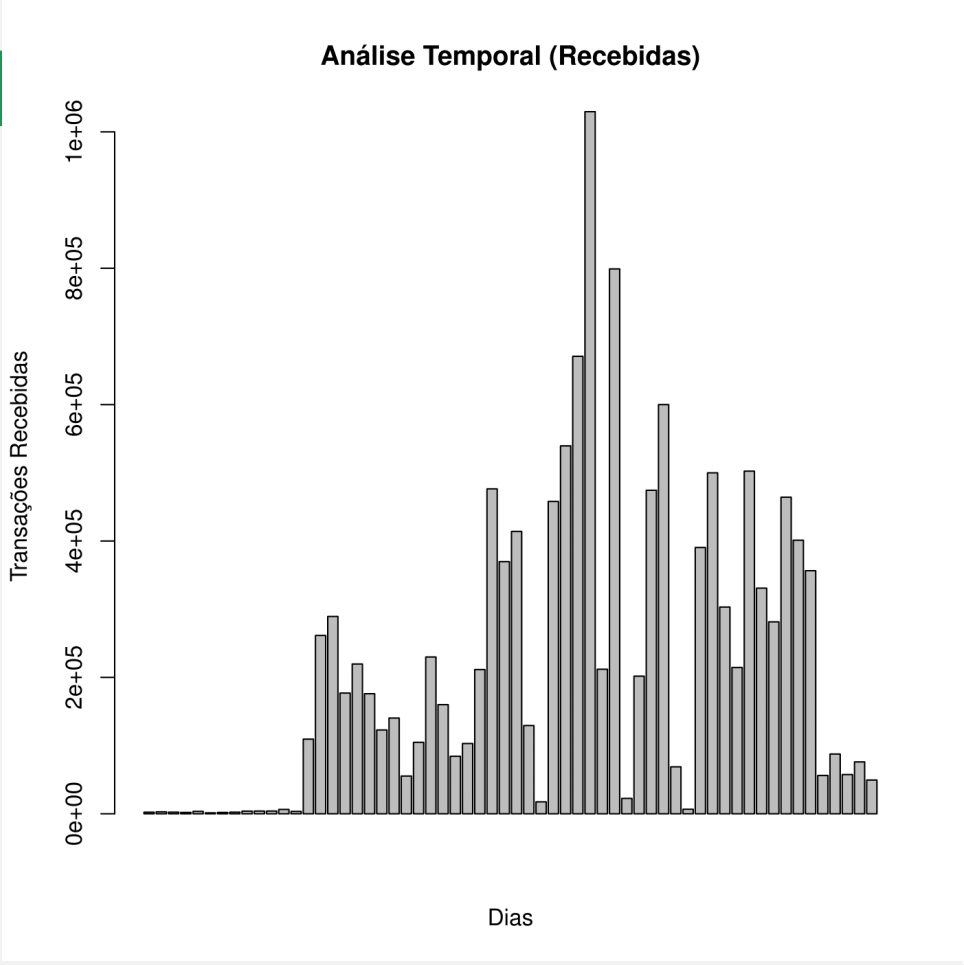




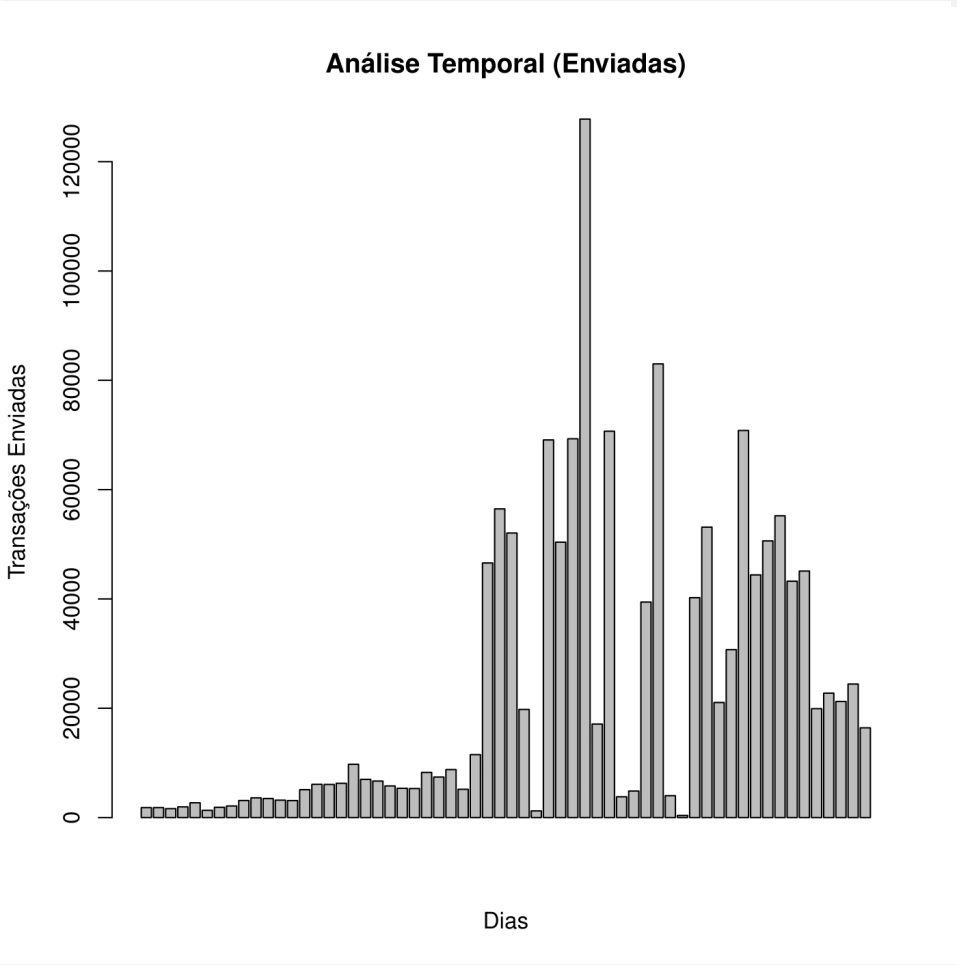
(a) Consultas recebidas por dia;

(b) Respostas enviadas por dia;

Análise temporal 2018



(a) Consultas recebidas por dia;



(b) Respostas enviadas por dia;

UDESC

Especificação dos ataques DoS em 2018

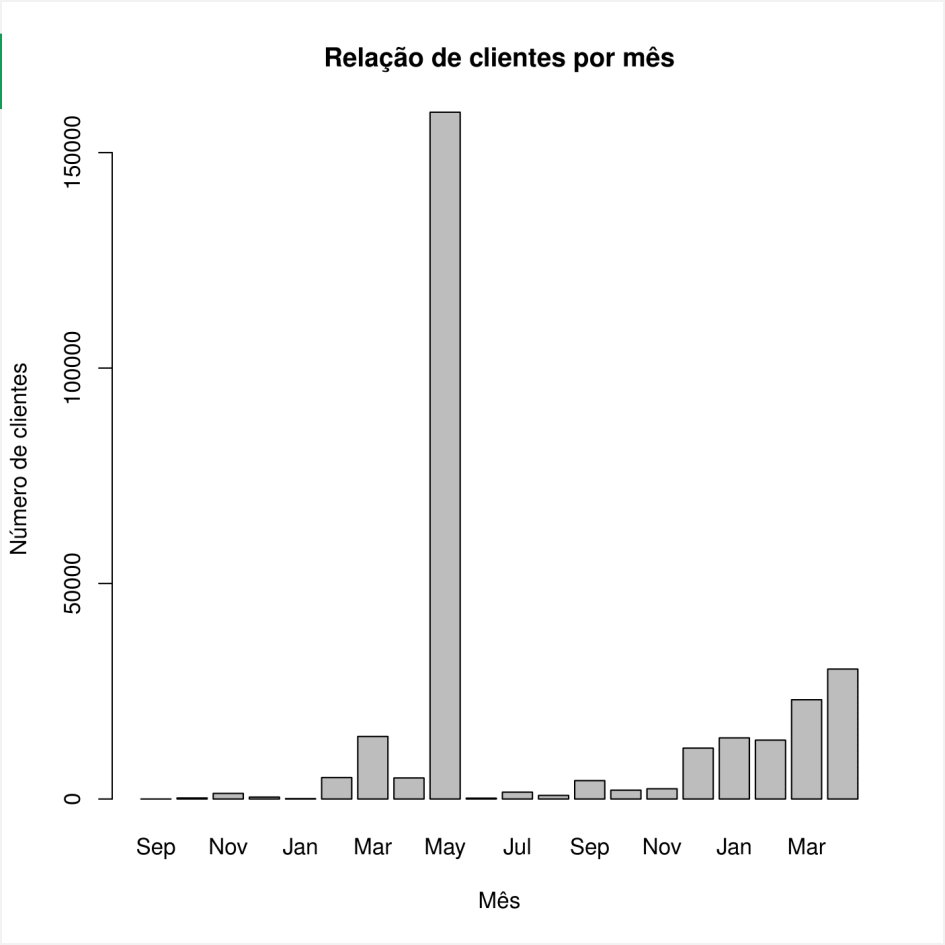
- Média de requisições por dia 217.469,2 ;

- Duração dos ataques: 50% até 5 minutos; 25% duraram até 20 minutos; 5% até 35 minutos.

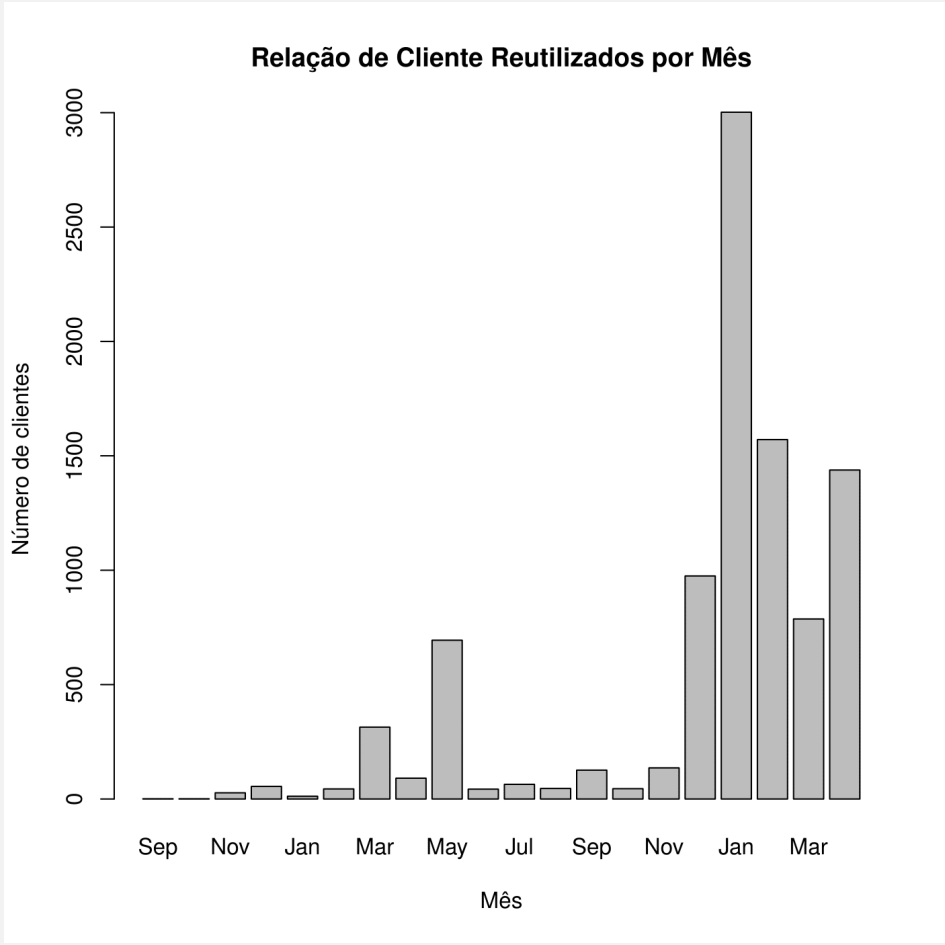
Requisições por ataque DoS

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

Análise temporal (Clientes)



(a) Clientes novos



(b) Clientes repetidos.

Anomalias de Tráfego

- Varreduras UDP e SIP;
  - Nmap e SIP.
- Consultas por nomes equivocados;
- Consultas de sistemas utilizados para ataques de amplificação;
  - RCON.

Conclusão

- Origem a pesquisa: O que acontece com um servidor DNS recursivo exposto a Internet?

- Conclusões:
  - Vira refletor em ataques DRDoS!
  - Esses ataques vem aumentando em duração e intensidade;
  - No geral o tráfego DNS também vem aumentando de intensidade.

- Evidências de uso do honeypot como servidor DNS recursivo regular por parte de usuários finais ou em nome destes;

- Perda de requisições.

Continuidade do trabalho

- Nova infraestrutura para o Honeypot
  - Solucionar problemas com Database
  - Nomes controlados
- Novos protocolos
  - Chargen
  - NTP
  - Memcached
  - ...
- Infraestrutura distribuída

Agradecimentos

- A Felipe Longo, pelo desenvolvimento da versão inicial do honeypot
- À FAPESC, pelo apoio financeiro às atividades do GRADIS
- A Coordenadoria de Informática da UDESC Joinville

UDESC

Obrigado

UDESC – Universidade do Estado de Santa Catarina

tiagoheinrich1995@gmail.com
rafael.obelheiro@udesc.br

Referência

LONGO, F. S. Honeypot para Servidores DNS Recursivos : Adaptação, Coleta e Análise de Resultados. Monografia (Trabalho de conclusão de curso) — Bacharelado em Ciência da Computação, Universidade do Estado de Santa Catarina, Joinville, dezembro de 2015.

BROWNLEE, N. ; CLAFFY, k. ; NEMETH, E. DNS Measurements at a Root Server. In : IEEE Global Telecommunications Conference (GLOBECOM). San Antonio, TX : IEEE Global Telecommunications Conference (GLOBECOM), 2001.

CASTRO, S. et al. Understanding and preparing for DNS evolution. In : Traffic Monitoring and Analysis Workshop (TMA). Zurich, Switzerland : TMA 2010, 2010. p. 1–6

GAO, H. et al. An empirical reexamination of global DNS behavior. SIGCOMM Comput. Commun. Rev., ACM, New York, NY, USA, v. 43, n. 4, p. 267–278, ago. 2013. ISSN 0146-4833. Disponível em : <http://doi.acm.org/10.1145/2534169.2486018>

ZDRNJA, B. ; BROWNLEE, N. ; WESSELS, D. Passive monitoring of DNS anomalies. In : Proceedings of the 4th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin, Heidelberg : Springer-Verlag, 2007. (DIMVA '07), p. 129–139. ISBN 978-3-540-73613-4.

ZHAO, G. et al. Detecting APT malware infections based on malicious DNS and traffic analysis. IEEE Access, v. 3, p. 1132–1142, 2015.

Este trabalho é licenciado sob uma licença Creative Commons "Atribuição-Não Comercial-Compartilha Igual 4.0 Internacional"