Caracterização de Payloads Usados em Ataques Distribuídos de Negação de Serviço por Reflexão (DRDoS)

Rafael Tenfen
Orientador Rafael Obelheiro
Qualificação
Joinville, SC
23/02/2022

UDESC
UNIVERSIDADE
DO ESTADO DE
SANTA CATARINA

Agenda

- DoS
  - DDoS
  - DRDoS
    - Protocolos
- Honeypots
  - MP-H
- Trabalhos Relacionados
- Proposta
  - Infraestrutura
  - Análise Longitudinal
  - Comparação de honeypots
  - Cronograma
- Referências

DoS - Denial of Service

- Negação de Serviço: Consiste em provocar a indisponibilidade de um recurso computacional, como um serviço um servidor ou uma rede conectada a internet.

- Ataques de negação de serviço: Um atacante com motivação financeira, política ou puramente destrutiva interrompe o serviço de uma vítima adicionando uma carga excessivamente alta de tráfego ao(s) serviço(s) da vítima.

- Ataques de negação de serviço existem basicamente a partir de quando a internet foi lançada.

- Em 1974 o primeiro ataque registrado foi realizado explorando uma vulnerabilidade em um mainframe conhecido como *Programmed Logic for Automatic Teaching Operations* (PLATO) (DENNIS, 2010).

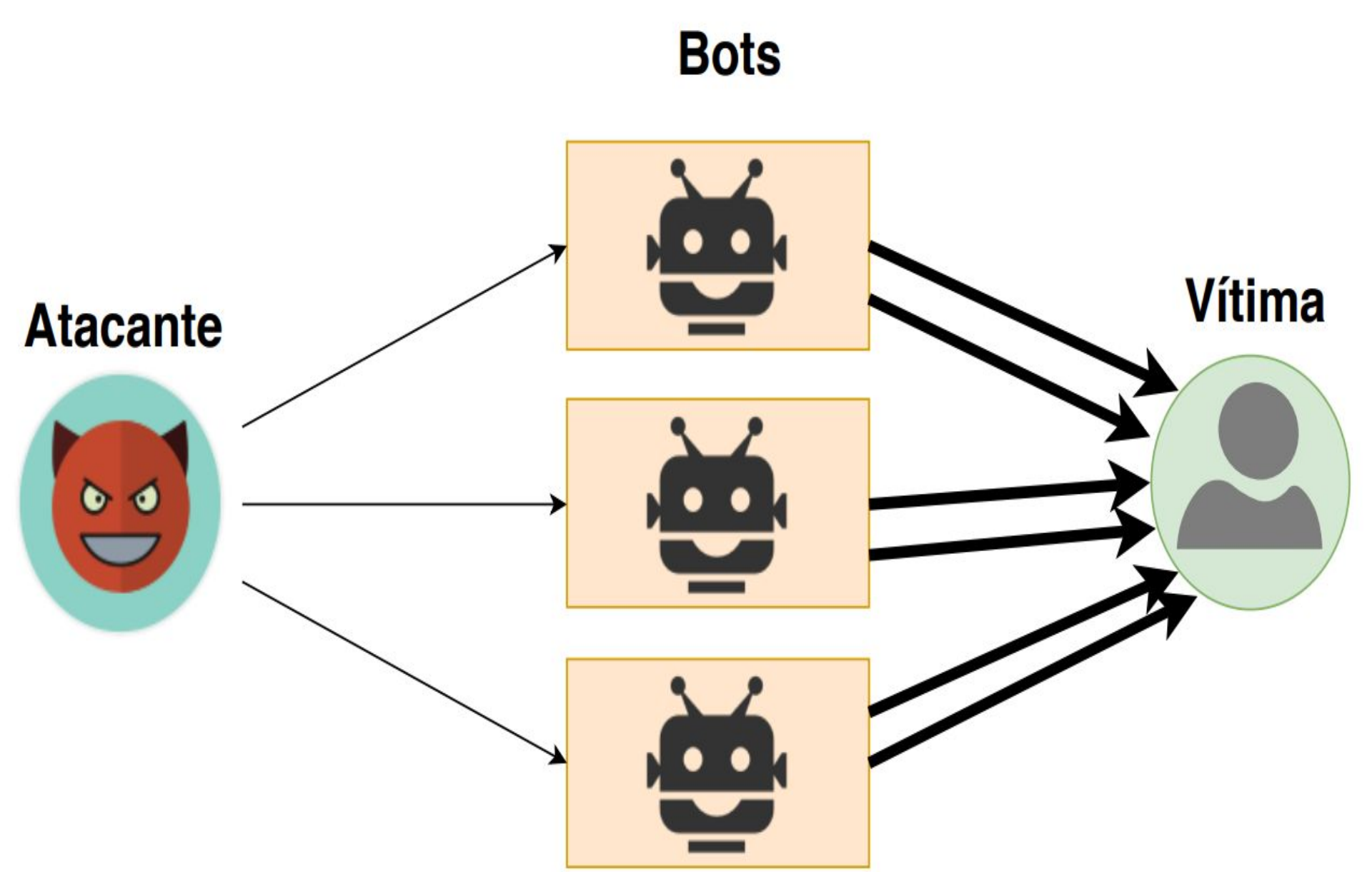
DDoS - Distributed Denial of Service

- Negação de Serviço Distribuído: Consiste em utilizar vários computadores em uma ação em conjunto para provocar a indisponibilidade de um recurso computacional.

- Ataques de negação de serviço distribuído: Quando um ataque DoS é realizado pela rede de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de (Distributed Denial of Service, DDoS).

- Botnets: São redes infectadas por malware e computadores remotamente designados para participar dos ataques.

- Em 1997 a primeira demonstração pública de ataque DDoS foi realizada por Khan C. Smith, durante o evento (DEF CON) grandes corporações acabaram sendo atacadas e assim interrompendo o acesso à Internet na Las Vegas Strip por mais de uma hora.



Esquema de um ataque DDoS [Heinrich 2019].

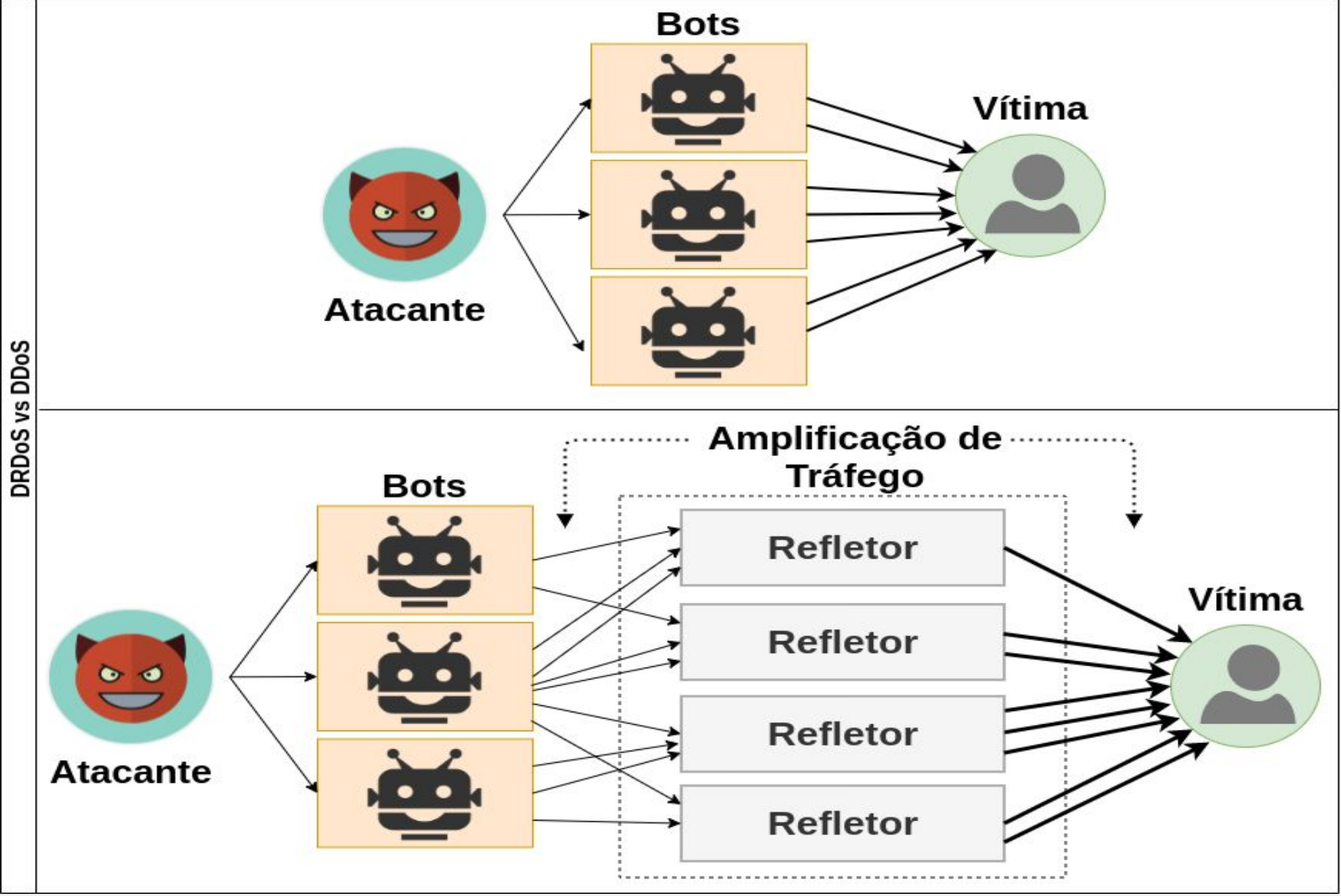
DRDoS - Distributed Reflection Denial of Service

- Negação de Serviço Distribuído por Reflexão: Consiste em utilizar vários computadores em uma ação em conjunto para provocar a indisponibilidade de um serviço através do uso de refletores.

- Ataques de negação de serviço distribuído por reflexão: Em um ataque DRDoS, o tráfego recebido pelos refletores tem como origem (forjada) o endereço IP da vítima, fazendo com que o tráfego de resposta seja enviado para esta, e não para os bots. Um atacante tem como objetivo esgotar a largura de banda da vítima.

- Refletores: Os atacantes podem incrementar seus ataques estruturando-os para utilizarem refletores. Para um atacante, um refletor é qualquer nó na rede que envia dados para um IP em resposta a uma requisição recebida anteriormente.

- Em 1998 também foi realizado o primeiro ataque de reflexão conhecido como Smurf attacks que explora o Internet Control Message Protocol.



Ataques Distribuídos de Negação de Serviço vs Ataques Distribuídos de Negação de Serviço por Reflexão. Adaptado de [Heinrich 2019].

Protocolos

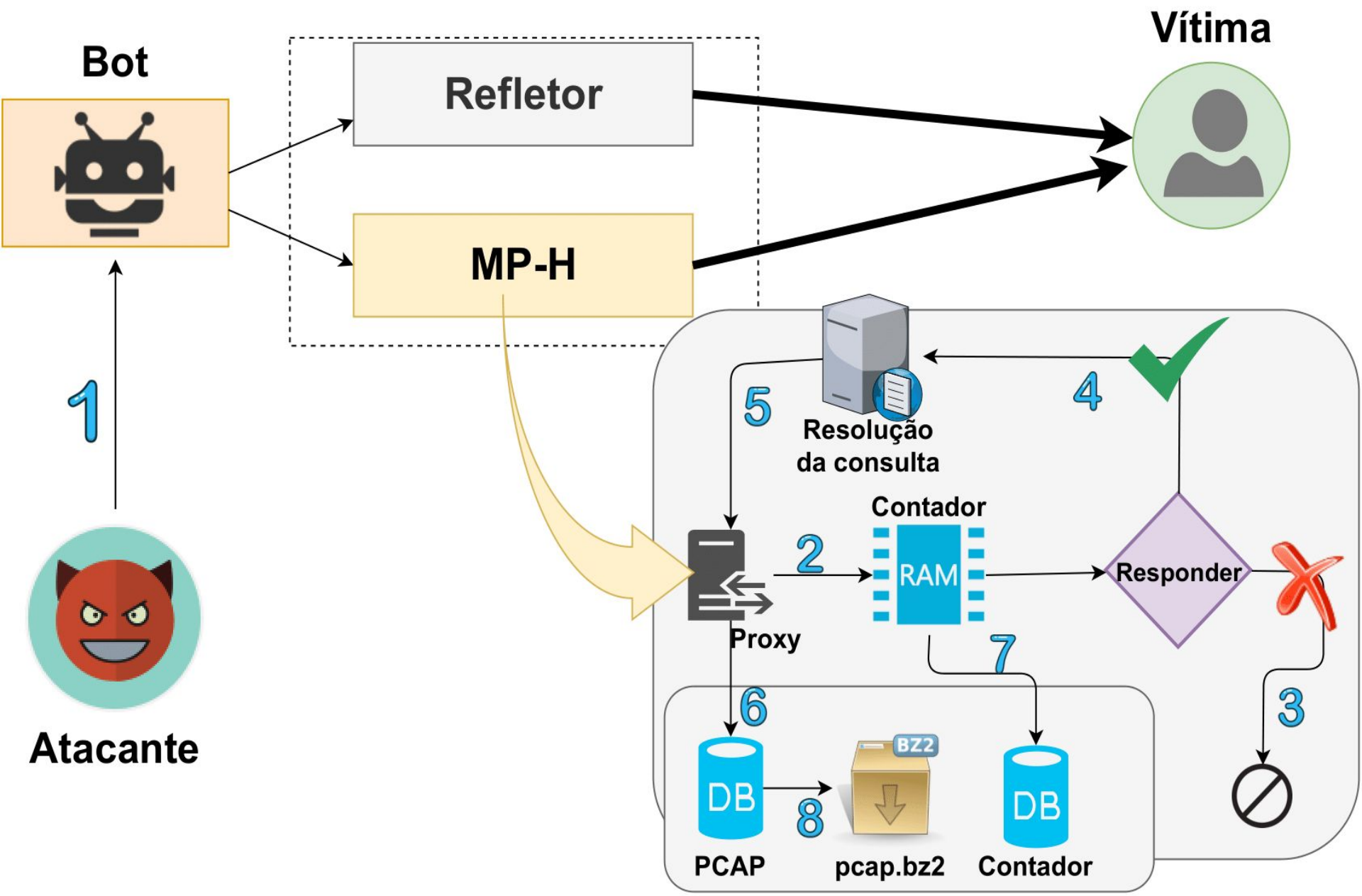
Protocolo/Serviço	Referência	Fator de amplificação
Steam	(CERT, 2014)	5.5
SNMP	(BITAG, 2012)	6.3
SSDP	(Majkowski, 2017)	30.8
DNS	(HOEPERS, 2016)	28 - 54
LDAP	(CERT, 2014)	46 - 55
CLDAP	(Choi and Kwak, 2017)	33 - 70
HTTP	(Beckett and Sezer, 2017)	79 - 100
QOTD	(CERT, 2014)	140.3
Chargen	(Rossow, 2014)	358.8
NTP	(CZYZ et al., 2014)	556.9
Memcached	(Newman and Bai, 2018)	10000 - 51000

Tabela com os principais protocolos utilizados em refletores como amplificadores em ataques DRDoS com o seu fator de amplificação.

UDESC

Honeypots

- Honeypot: É um recurso computacional que possui o objetivo de ser sondado, atacado ou até mesmo comprometido.
- Host: Geralmente um honeypot é um host que possui um endereço público na Internet, o qual não é anunciado.
- Interatividade: Quanto mais funcionalidades um honeypot implementa e quanto mais possibilidades de interação ele oferece.
- Payloads: Informações recolhidas pelos honeypots para serem analisadas posteriormente.
- Objetivo: Recolher as informações sobre os ataques que o utilizam como refletor/amplificador no ataque.



Fluxo de processo de requisições do MP-H [Heinrich 2019].

UDESC

Trabalhos Relacionados

Referência	Protocolos	Número de Honeypots	Período de coleta
[Rossow 2014]	NTP, SNMP, SSDP, NetBios, CharGen, QOTD, P2P, BitTorrent, Quake 3, Steam, DNS, Kad, ZAv2, Sality e Gameover	556.9	12 dias
[Krämer et al. 2015]	NTP, DNS, Chargen, SSDP, MS-SQL, NetBIOS, QOTD, SIP e SNMP	21	121 dias
[Noroozian et al. 2016]	NTP, DNS, Chargen, SSDP, QOTD e SNMP	8	730 dias
[Thomas et al. 2017]	QOTD, Chargen, DNS, NTP, SSDP, MS-SQL, Portmap e mDNS	65	1010 dias
[Jonker et al. 2017]	NTP, DNS, CharGen, SSDP e RIPv1	24	731 dias
[Heinrich et al. 2021]	Chargen, DNS, NTP, Memcached, QOTD, SSDP, CoAP, CLDAP e Steam	1	731 dias

Resumo dos trabalhos relacionados que apresentam os protocolos atendidos pelo honeypot, a quantidade de honeypots implantados e o período de coleta de dados

UDESC

Proposta

- Estender o trabalho apresentado por [Heinrich et al. 2021]: Foco em análise de payloads.
- Preencher lacunas encontradas na literatura:
  - Realizar uma análise longitudinal da evolução dos payloads, considerando os diferentes protocolos implementados pelo MP-H;
  - Comparar os payloads recebidos pelas diferentes instâncias.

Infraestrutura

- Dois honeypots na rede da UDESC:
  - Um honeypot ativo desde setembro de 2017;
  - Um honeypot ativo desde agosto de 2021;
  - Protocolos: Chargen, DNS, Memcached, NTP, QOTD, SSDP e Steam.
- Um honeypot na rede da UFPR:
  - Um honeypot ativo desde setembro de 2021;
  - Protocolos: Chargen, DNS, Memcached, NTP, QOTD, SSDP e Steam.

Comparação e correlação dos payloads

- Uma das lacunas encontradas na literatura é a comparação e correlação dos payloads entre dois ou mais honeypots, que pode se resumir nas seguintes questões:
  - Payloads são similares?
  - Payloads são diferentes entre si?
  - Dentre as 3 instâncias de honeypots (2 UDESC e 1 UFPR) algum dos ataques realizados utilizou mais de uma instância durante ao mesmo ataque?
  - Os ataques realizados com um mesmo protocolo, utilizam o mesmo mecanismo?

Análise longitudinal da evolução dos payloads

- A outra lacuna encontrada na literatura é a análise longitudinal da evolução dos payloads de ataques de negação de serviço ao longo do tempo. Esse trabalho pretende realizar as seguintes análises/questões:
  - Mudanças em protocolos específicos como o DNS com a utilização da query **ANY**;
  - Após o anúncio de depreciação da query **ANY** os ataques que utilizavam o protocolo DNS alteraram o modo de utilizar o protocolo.
  - Ao longo do tempo, um mesmo protocolo que não teve muitas alterações em sua implementação, é utilizado pelos atacantes da mesma forma?

Cronograma

Etapa	Data de início	Data de finalização
Analisar conteúdo recolhido pelos honeypots	28/02	13/03
Análise dos payloads	14/03	27/03
Análise longitudinal	28/03	24/04
Comparação entre honeypots	25/04	29/05
Desenvolvimento de artigo	30/05	26/06
Escrever a dissertação	27/06	31/08

Tabela com as etapas necessárias para concluir o mestrado com as datas de início e fim de cada etapa.

UDESC

Referências

- Heinrich, T. (2019). Caracterização de ataques DRDoS usando honeypot. Master's thesis,Dissertação de mestrado em Computação Aplicada, Universidade do Estado de SantaCatarina - UDESC, Joinville (SC).

- Heinrich, T., Obelheiro, R. R., and Maziero, C. A. (2021). New kids on the DRDoS block Characterizing multiprotocol and carpet bombing attacks. In International Conference on Passive and Active Network Measurement, pages 269–283. Springer.

- Jonker, M., King, A., Krupp, J., Rossow, C., Sperotto, A., and Dainotti, A. (2017). Millions of targets under attack: a macroscopic characterization of the DoS ecosystem. In Proceedings of the 2017 Internet Measurement Conference, pages 100–113.

- Paxson, V. (2001). An analysis of using reflectors for distributed denial-of-service attacks. ACM SIGCOMM Computer Communication Review, 31(3):38–47.

- Rossow, C. (2014). Amplification hell: Revisiting network protocols for DDoS abuse. In NDSS.

Obrigado

UDESC – Universidade do Estado de Santa Catarina

rafaeltenfen.rt@gmail.com

Caracterização de Payloads Usados em Ataques Distribuídos de Negação de Serviço por Reflexão (DRDoS)

Rafael Tenfen
Orientador Rafael Obelheiro
Qualificação
Joinville, SC
23/02/2022

UDESC
UNIVERSIDADE
DO ESTADO DE
SANTA CATARINA