Detecção de Refletores em Ataques DDoS Volumétricos

Universidade de Brasília
Yan Victor dos Santos - 14/0033599

Visão Geral

- Introdução
- Características
- Motivação do Ataque (Problema)
- Arquitetura de Mitigação
- Detecção de Refletores
- Conclusão
- Trabalhos Futuros
- Referências

Introdução

Introdução

1. Incentivadas pelo **lucro** e **eficiência**, empresas investem em diversos **serviços** na **Internet**
2. Solidifica o conceito de arquitetura **cliente-servidor**
3. Abre portas para **diversos** tipos de Ataques
4. Dentre os Ataques, temos o ataque **DDoS** (Distributed Denial of Service)
5. Este trabalho tem por **objetivo** detectar a existência de **refletores** em ataques DDoS Volumétricos

Características

DoS (Denial of Service)

1. Em termos leigos, é a **tentativa** de fazer um **servidor** ter **dificuldades** ou até mesmo ser **impedido** de fornecer serviços

2. Existem **diversas** maneiras de fazer um ataque **DoS**

3. **Dentre** as **diversas** formas, temos o ataque **DDoS** (Distributed Denial of Service)

DDoS (Distributed Denial of Service)

1. Ataque bastante comum
2. **Mestre controla** diversas **máquinas infectadas** (BotNet) para **atacar** a **vítima** em algum momento de interesse
3. **Grande número** de máquinas acedem **recursos** de um mesmo servidor e **esgota o *slot***, fazendo com que ele **não consiga** mais **atender** pedidos

O **objetivo** do ataque (**volumétrico**) é **inundar** a rede do servidor, sobrecarregando a largura de banda local

4. Localizar o atacante fica mais difícil

DDoS - Esquema

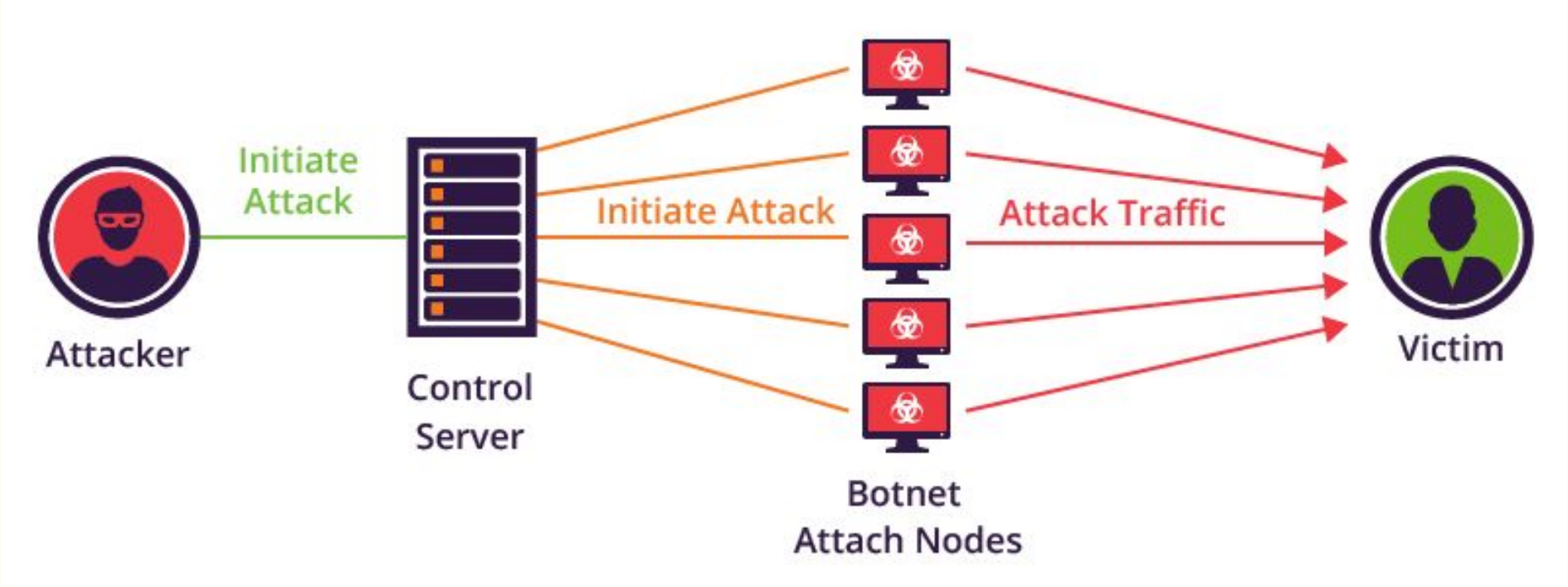


*Image from: incapsula.com. Text: “How to identify a mirai style DDoS attack”

Ataque DDoS com **Refletores**

1. **Aproveita-se** da **vulnerabilidade** de servidores que utilizam protocolos tais como: **DNS** (Domain Name System) e NTP (Network Time Protocol), principalmente em protocolo **UDP**

2. **Troca** o **IP** de origem para o da vítima, **envia** *queries* para servidores (**refletores**), que em seguida **respondem** legitimamente para a **vítima**, causando negação de serviço

3. **Maximiza** o ataque (Amplificação)

4. É um dos vetores **mais utilizados** para ataques DDoS

DDoS com Refletores - Esquema

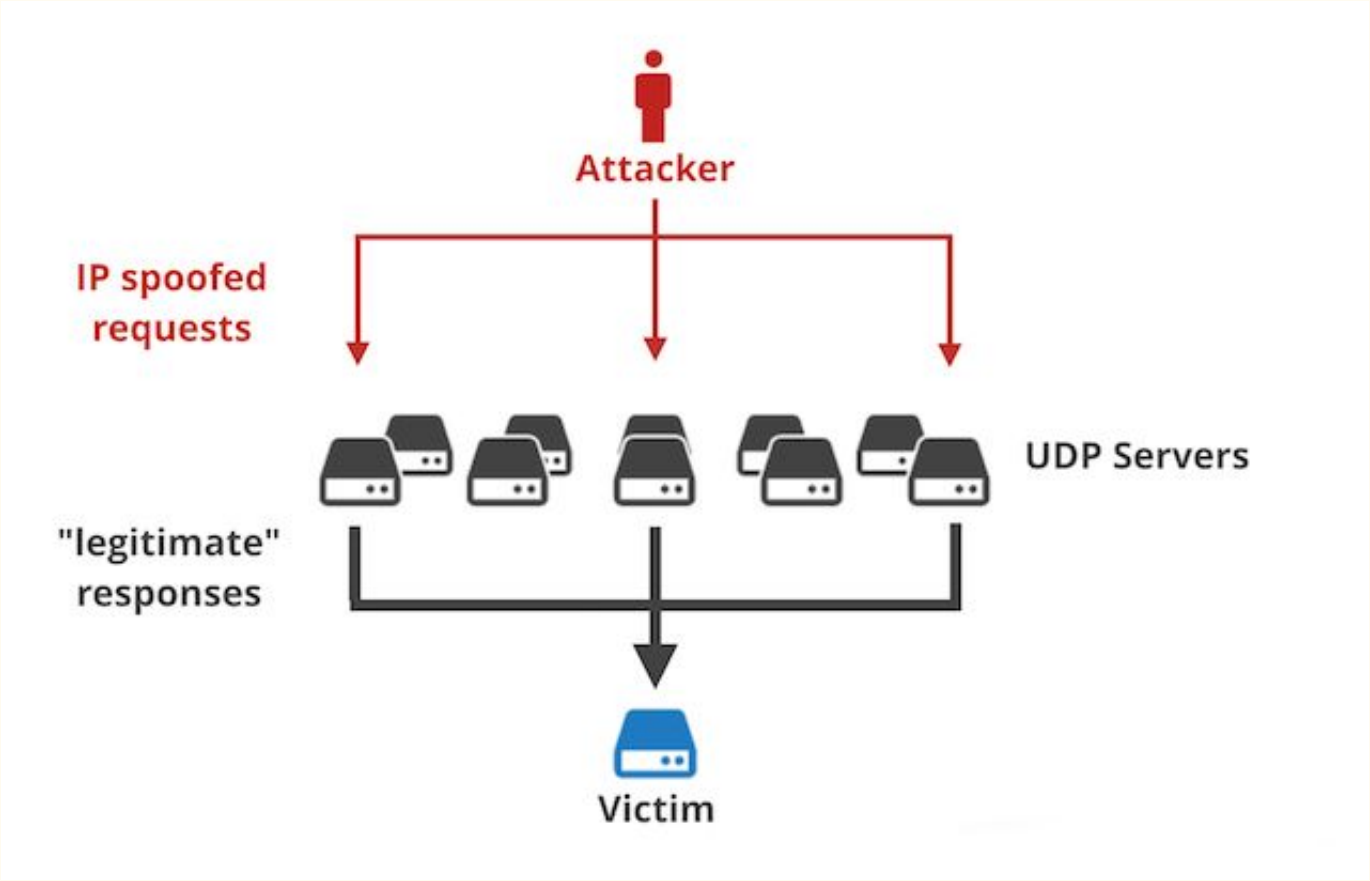


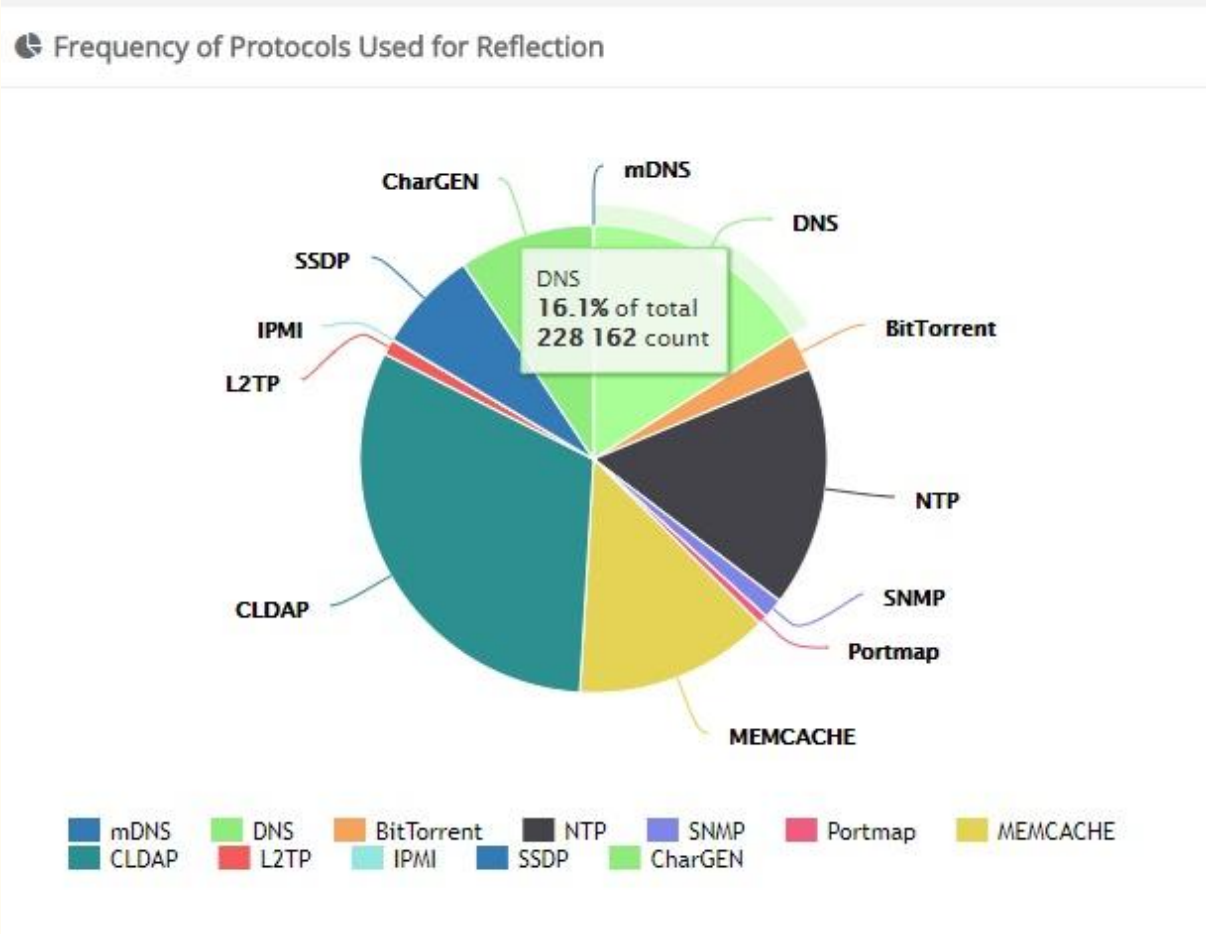
*Image from: Cloudflare

Motivação do Ataque (Problema)

Motivação do Ataque - Refletores

1. **Poucos recursos** podem gerar **grandes impactos**
2. Origem **não** ataca **diretamente** (camuflagem)
3. A **resposta** pode ser bem **maior que** a **requisição.**
   Exemplo: ANY pede ao servidor todos os registros para o nome *host* específico que você pediu
4. A resposta é **rápida** (UDP)

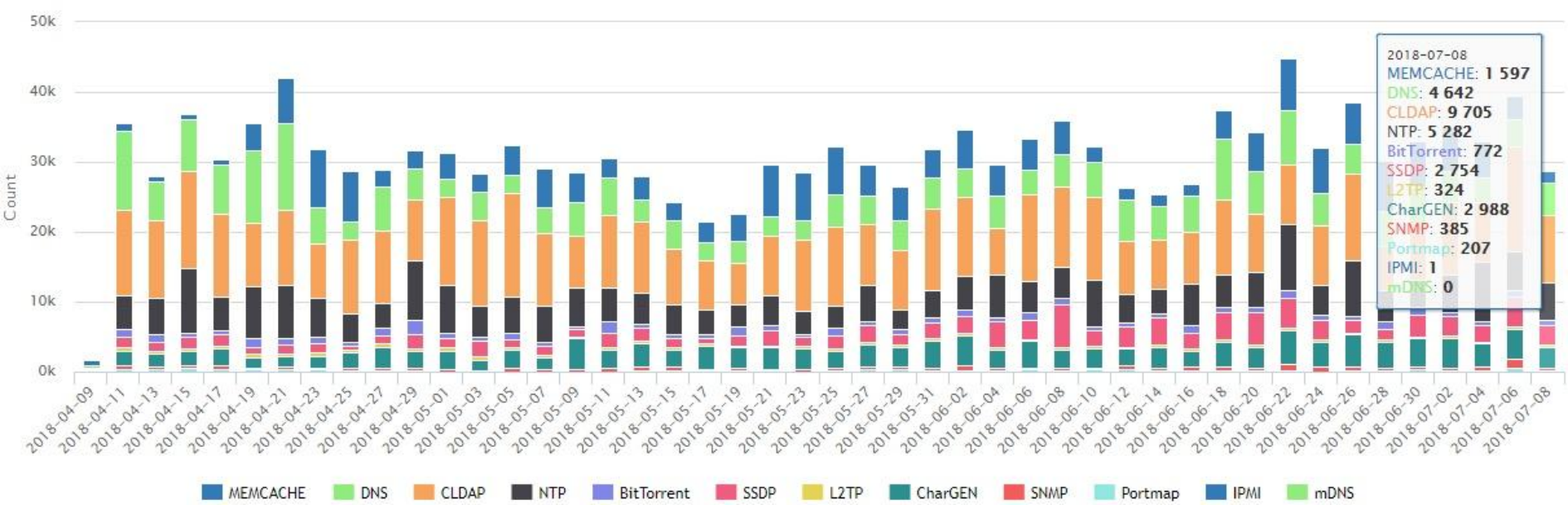
DDoS com Refletores - Frequência de Protocolos



Insight - DDoS Mon
Últimos 3 meses

*Fonte: [2]

DDoS com Refletores - Protocolos usados



*Fonte: [2]

Insight - DDoS Mon
Últimos 3 meses

Motivação do Ataque - DDoS Mon [2]

“Os ataques de inundação e reflexão da UDP continuam a liderar nos últimos dias.”

“Representam quase 70% do total de ataques em nossa observação.”

“As inundações UDP mais comuns atenuadas foram os ataques de reflexão do Sistema de Nomes de Domínio (**DNS**), seguidos pelos ataques de reflexão do Network Time Protocol (NTP) e do Simple Service Discovery Protocol (SSDP).”

DDoS com Refletores - DNS Packets ~ Exemplo

	Time (h:m:...	MAC source addr	MAC dest. addr	Frame	Protocol	Addr. IP src	Addr. IP dest	Port src	Port dest
1	21:14:27:456	00:02:B3:5B:AC:5B	00:02:B3:3C:32:68	IP	UDP->DNS	192.168.0.10	139.130.4.4	1027	53
2	21:14:28:447	00:02:B3:3C:32:68	00:02:B3:5B:AC:5B	IP	UDP->DNS	139.130.4.4	192.168.0.10	53	1027

O tempo que demorou para receber e responder à esta consulta DNS foi de apenas 0,991 segundos!

- *Rapidez na resposta*
- *Sem Handshake de 3 vias*
- *O PKG de resposta é mais complexo e maior que o PKG de requisição*

*Fonte: [3]

Motivação do Ataque - Cloudflare

“A especificação do UDP mostra ser um dos melhores para amplificação! Há absolutamente zero verificações, e os dados são entregues ao cliente com **velocidade máxima**! Além disso, o **pedido pode ser minúsculo e a resposta enorme**”, observaram os pesquisadores da Cloudflare. [1]

O que podemos fazer??! …

PODEMOS CONTRIBUIR

1. **Instanciar o problema**
2. **O que podemos resolver dentro das variações de DDoS?**
3. **Detectar Refletores**
4. **Proposta de uma solução para a detecção**

Arquitetura de Mitigação

Arquitetura de Mitigação

1. Ocorre do servidor (vítima) ser isolado da rede externa
2. Módulo de proteção que analisa o tráfego
3. Especializado em detectar determinado tipo de ataque
4. A resposta ao ataque depende do que foi direcionado para o problema

DDoS com Refletores

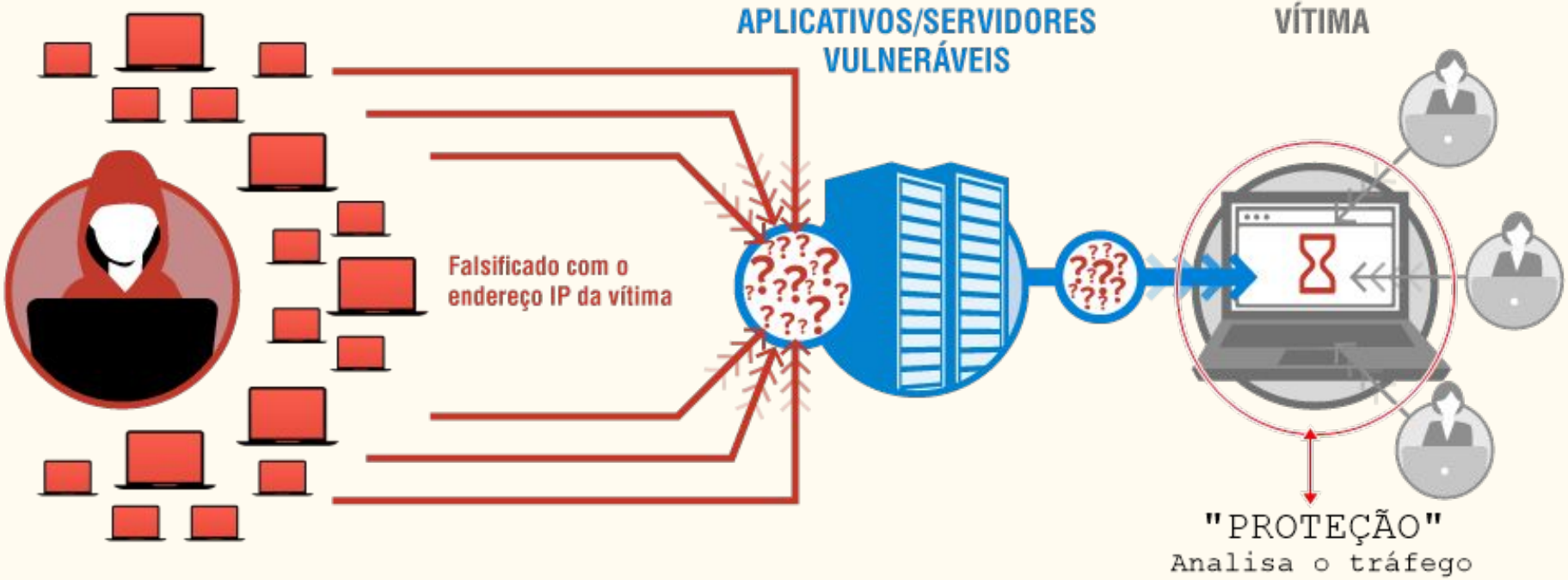


*Image from: [4]

Detecção de Refletores

Detecção de Refletores - DNS

Passo 1:

Detectar DDoS

Passo 2:

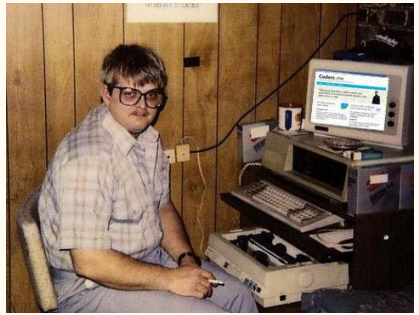
Detectar Refletores

Detecção de Refletores - DNS

Passo 1:

Detectar DDoS 

Por enquanto, vamos ***assumir*** *que o* ***problema*** *já foi* ***mitigado!***



Detecção de Refletores - DNS

Passo 1:

Detectar DDoS 

Passo 2:

Detectar Refletores

Detecção de Refletores - DNS

Passo 2:

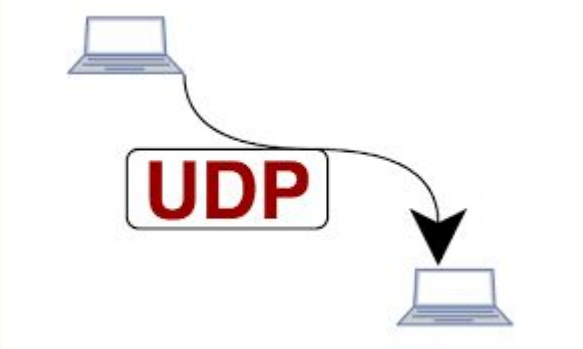
Detectar Refletores

*Este é o **foco** do trabalho!*

Passo 2: Detectar Refletores - PROTOCOLOS

Obs.: O “FOCO” é apenas uma instanciação temporária do problema para construção genérica

1. Escutar tráfego UDP, ICMP entrando e saindo. [FOCO: UDP]
2. No caso UDP, Identificar o protocolo (Porta). Verificar SNMP, NTP, DNS, etc. [FOCO: DNS]



Passo 2: Detectar Refletores - UDP ~ DNS[53]

SAINDO (Thread)	CHEGANDO (Thread)
Verifica se é REQUISIÇÃO (**OK**)	Verifica se é RESPONSE (**OK**)
OK: guarda na **TABELA DE ESTADOS**	**OK**: Verifica REQ pendente na **T.d.E.**
	Sim -> Repassa. **Não** -> **Eita**

Eita: implica em guardar o IP address de origem e dropar o pacote em seguida.

*A busca na Tabela de Estados deve ser eficiente

Passo 2: Detectar Refletores - Saindo OK

1. Guarda dados da requisição na Tabela de Estados para ser usada quando receber RESPONSE, incrementa contador
2. Espera por RESPONSE

...

Passo 2: Detectar Refletores - Chegando: EITA

1. Sempre que a RESPONSE correspondente chegar, o contador referente à requisição é decrementado
2. Muitos pacotes de Response sem existir requisições feitas anteriormente pelo servidor (Contador negativo)
3. Neste caso, há muitas chances de estar sofrendo um ataque por reflexão
4. O que fazer: anotar o IP na *BlackList* e dropar pacotes

DDoS com Refletores - EITA

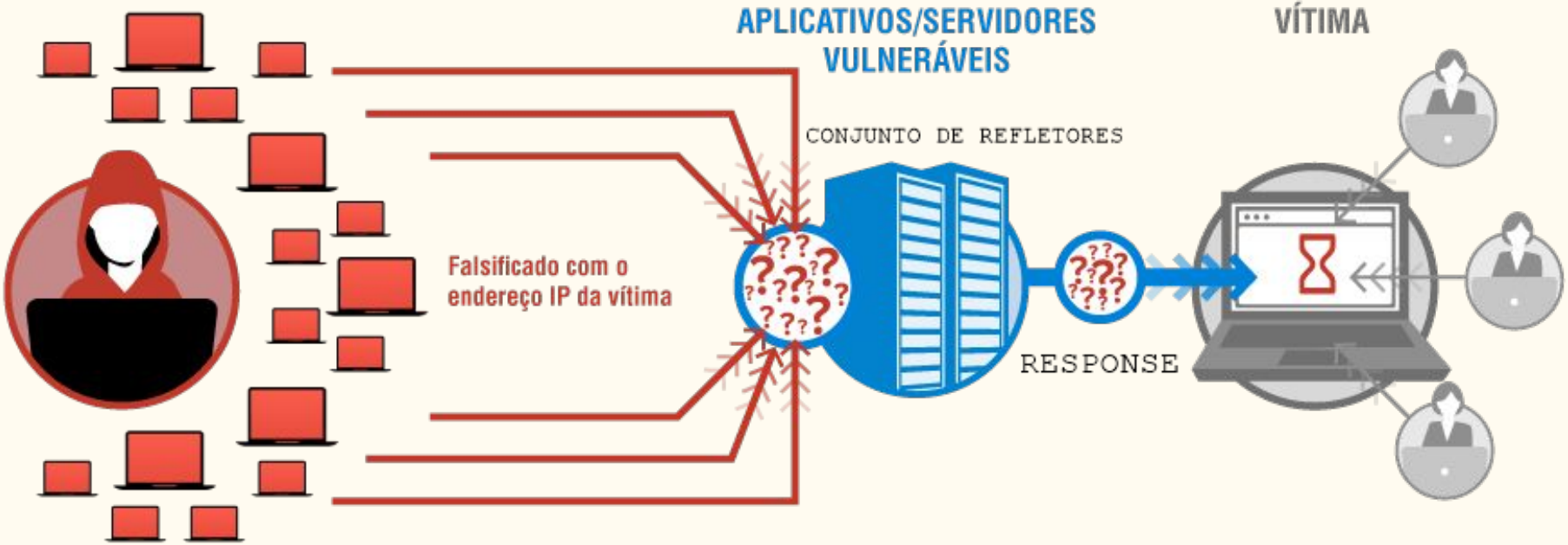


*Image from: [4]

DDoS com Refletores - Ferramenta

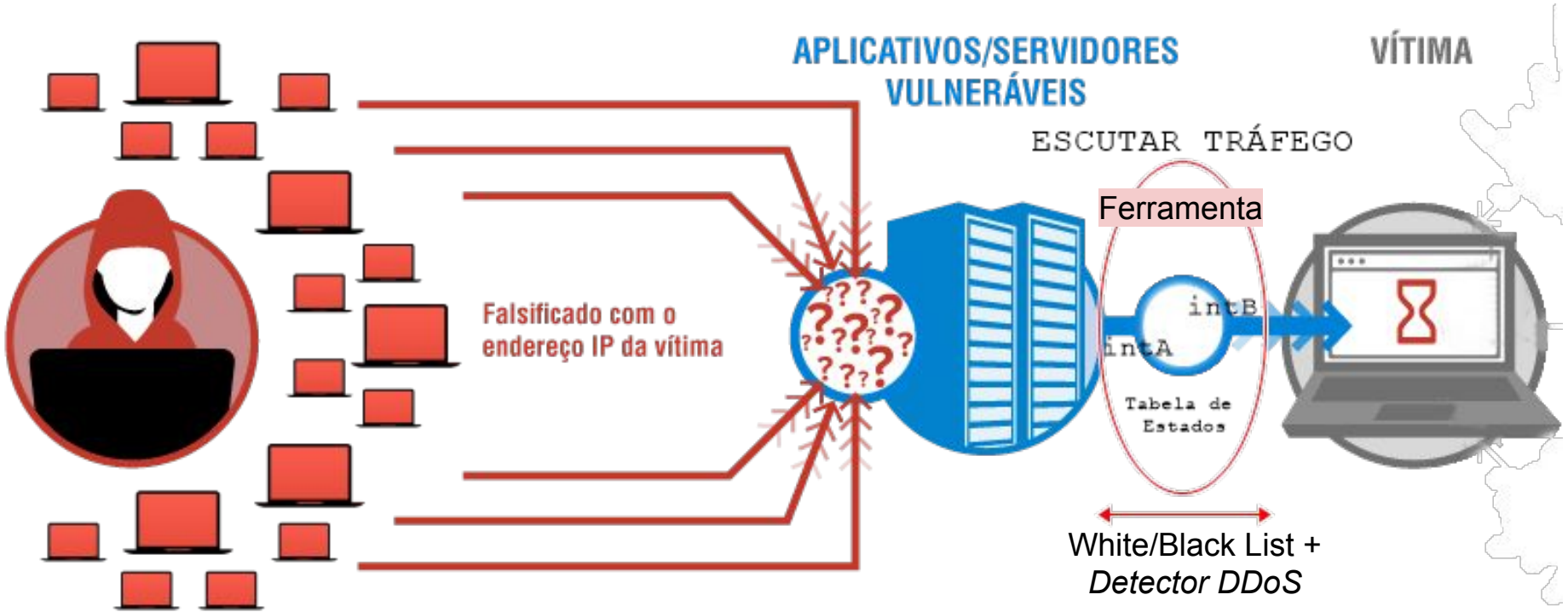


*Image from: [4] ~ Edited

Detecção de Refletores - DNS

Passo 1:

Detectar DDoS 

Passo 2:

Detectar Refletores 

Conclusão

Conclusão

- Os gráficos em [2] revelam a grande vulnerabilidade de servidores a ataques DDoS por amplificação nos dias atuais
- Meios de combater estes ataques se tornam cada vez mais necessários
- A variabilidade de ataques DDoS requer um estudo mais específico sobre cada variação
- A quantidade de grandes servidores que podem ser usados como refletores ainda é imensa
- Portanto, neste trabalho, a detecção específica de refletores é uma forte instância da contribuição para mitigar ataques DDoS
- Esta contribuição busca minimizar o processamento para verificar o ataque

Trabalhos Futuros

Trabalhos Futuros

- Implementação da ferramenta de detecção dos refletores (Protocolo DNS), para verificar a efetividade do projeto atual sem modificações;
- Verificar a implementação da detecção do DDoS, ou reutilizar módulos existentes;
- Extensão para outros protocolos vulneráveis.

Referências

[1] kaspersky, “Novo método amplifica ataques DDoS”. Fonte: https://www.kaspersky.com.br/blog/novo-metodo-amplifica-ataques-ddos/10120/

[2] DDoS Mon, “Insight into Global DDoS Threat Landscape”. Fonte: https://ddosmon.net/insight/

[3] Firewall.cx, “Formato da mensagem de resposta do DNS”. Fonte: http://www.firewall.cx/networking-topics/protocols/domain-name-system-dns/161-protocols-dns-response.html

[4] Verisign, “Ataque de Inundação de UDP”, Fonte: https://www.verisign.com/pt_BR/security-services/ddos-protection/denial-of-service/index.xhtml