Para detectar, mitigar e prevenir ataques DRDoS, é importante entender como eles funcionam, e quais são suas características de tráfego. Este trabalho investiga ataques DRDoS, mais particularmente as tendências recentes de ataques multiprotocolo, que exploram múltiplos protocolos simultaneamente, e ataques *carpet bombing*, que direcionam tráfego para vários endereços em uma mesma sub-rede em vez de para um único host. Um *honeypot* que suporta sete diferentes protocolos foi desenvolvido e uma coleta de dados de 250 dias foi realizada, possibilitando o estudo dos ataques em um ambiente real. Ao todo, foi observado mais de 105.7 GB de tráfego, com quase 10 bilhões de requisições e 360 k ataques DRDoS.

Orientador: Rafael Rodrigues Obelheiro

Joinville, 2019

ANO
2019

TIAGO HEINRICH | CARACTERIZAÇÃO DE ATAQUES DRDOS USANDO HONEYPOT

UNIVERSIDADE DO ESTADO DE SANTA CATARINA – UDESC
CENTRO DE CIÊNCIAS TECNOLÓGICAS – CCT
PROGRAMA DE PÓS GRADUAÇÃO EM COMPUTAÇÃO APLICADA

DISSERTAÇÃO DE MESTRADO

CARACTERIZAÇÃO DE ATAQUES DRDOS USANDO HONEYPOT

TIAGO HEINRICH

Joinville, 2019

UNIVERSIDADE DO ESTADO DE SANTA CATARINA - UDESC
CENTRO DE CIÊNCIAS TECNOLÓGICAS - CCT
MESTRADO EM COMPUTAÇÃO APLICADA - PPGCA

TIAGO HEINRICH

CARACTERIZAÇÃO DE ATAQUES DRDOS USANDO HONEYPOT

JOINVILLE

2019

TIAGO HEINRICH

CARACTERIZAÇÃO DE ATAQUES DRDOS USANDO HONEYPOT

Dissertação submetida ao Programa de Pós-Graduação em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, para a obtenção do grau de Mestre em Computação Aplicada.

Orientador: Dr. Rafael Rodrigues Obelheiro

JOINVILLE

2019

Ficha catalográfica elaborada pelo programa de geração automática da

Biblioteca Setorial do CCT/UDESC,

com os dados fornecidos pelo(a) autor(a)

Heinrich, Tiago
Caracterização de ataques DRDoS usando honeypot / Tiago Heinrich. -- 2019.
70 p.

Orientador: Rafael Rodrigues Obelheiro
Dissertação (mestrado) -- Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada, Joinville, 2019.

1. Ataques de Amplificação. 2. Segurança de rede. 3. Ataque de Negação de Serviço por Reflexão. I. Obelheiro, Rafael Rodrigues . II. Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada. III. Título.

Caracterização de Ataques DRDoS usando Honeypot

por

Tiago Heinrich

Esta dissertação foi julgada adequada para obtenção do título de

Mestre em Computação Aplicada

Área de concentração em "Ciência da Computação",
e aprovada em sua forma final pelo

CURSO DE MESTRADO ACADÊMICO EM COMPUTAÇÃO APLICADA
DO CENTRO DE CIÊNCIAS TECNOLÓGICAS DA
UNIVERSIDADE DO ESTADO DE SANTA CATARINA.

Banca Examinadora:

Prof. Dr. Rafael Rodrigues Obelheiro
CCT/UDESC (Orientador/Presidente)

Prof. Dr. Luciano Paschoal Gaspary -
UFRGS

Prof. Dr. Ricardo José Pfitscher
UNISOCIESC

Joinville,SC, 26 de julho de 2019.

Dedico este trabalho aos meus familiares, amigos, colegas e professores que me acompanharam e me deram forças nessa magnífica trajetória.

AGRADECIMENTOS

Agradeço ao apoio dos meus queridos pais que, sempre estiveram ao meu lado e me auxiliaram nesta caminhada. Em especial agradeço o meu irmão, o qual sempre esteve presente nestes anos de estudo na UDESC e compartilhou comigo esta jornada, tanto nos dias bons como nos dias ruins. Ao Prof. Dr. Rafael Rodrigues Obelheiro por ter me orientado e guiado ao longo deste período, e ter se tornando um amigo ao qual sempre lembrarei e espero ainda continuar convivendo, buscando ajudar mesmo nos problemas aos quais não estiveram relacionado com a pesquisa.

Sou grato também à Profa. Dra. Rebeca Schroeder Freitas pelos ensinamentos e trabalhos realizados na graduação da UDESC, ao qual contribui para o momento que estou agora.

Aos professores Dr. Guilherme Piêgas Koslovski, Dr. Mauricio Aronne Pillon e Dr. Charles Christian Miers pelo apoio ao longo desta jornada e ensinamentos ao decorrer destes anos.

Sou grato também ao Departamento de Ciência da Computação (DCC) por ter contribuído com os laboratórios os quais foram utilizados durante longas horas nas madrugadas para acabar trabalhos e experimentos. Também sou grato ao meu amigo Leonardo Rosa Rodrigues que sempre esteve presente colaborando para os trabalhos, e ajudando nos experimentos realizados durante as madrugadas no DCC, mas principalmente por sempre estar ao meu lado sem hesitar em ajudar. Ao Gustavo Diel que apesar de estarmos em períodos diferentes sempre buscou ajudar e estar presente.

Por fim, agradeço a todos aqueles colegas que estiveram presente na minha caminhada e que tiveram uma contribuição direta ou indireta com a minha caminhada durante este período, vocês tiveram uma contribuição para o momento que estou agora, sendo que sempre poderão contar comigo para auxílio, por fim, um Muito obrigado.

“Obstacles are those frightful things you see when you take your eyes off your goal.”

Henry Ford

RESUMO

Ataques distribuídos de negação de serviço por reflexão (*distributed reflection denial of service*, DRDoS) estão disseminados na Internet. Esses ataques oferecem diversas vantagens para os atacantes, sendo bastante eficazes em provocar a indisponibilidade de *hosts* individuais ou mesmo sub-redes inteiras. Para detectar, mitigar e prevenir ataques DRDoS, é importante entender como eles funcionam, e quais são suas características de tráfego. Este trabalho investiga ataques DRDoS, mais particularmente as tendências recentes de ataques multiprotocolo, que exploram múltiplos protocolos simultaneamente, e ataques *carpet bombing*, que direcionam tráfego para vários endereços em uma mesma sub-rede em vez de para um único *host*. Um *honeypot* que suporta sete diferentes protocolos foi desenvolvido e uma coleta de dados de 250 dias foi realizada, possibilitando o estudo dos ataques em um ambiente real. Ao todo, foi observado mais de 105.7 GB de tráfego, com quase 10 bilhões de requisições e 360 k ataques DRDoS.

Palavras-chaves: Ataques de Amplificação, Segurança de rede e Ataque de Negação de Serviço por Reflexão.

ABSTRACT

Distributed denial-of-service (DRDoS) attacks are widespread on the Internet. These attacks offer several advantages for attackers and are quite effective in causing the unavailability of individual hosts or even entire sub-networks. To detect, mitigate and prevent DRDoS attacks, it is important to understand how they work, and what their traffic characteristics are. This work investigates DRDoS attacks, in particularly the recent trends of multiprotocol attacks, which exploit multiple protocols simultaneously, and carpet bombing attacks, which direct traffic to several addresses on the same subnet rather than to a single host. A honeypot that supports seven different protocols was developed and a data collection of 250 days was made, allowing the study of the attacks in a real environment. In all, over 105.7 GB of traffic was observed, with nearly 10 billion requests and 360 k DRDoS attacks.

Keywords: Amplification Attacks, Network Security, and Denial of Service Attack by Reflection.

LISTA DE ILUSTRAÇÕES

Figura 1 – Esquema de um ataque DDoS. 20
Figura 2 – Evolução anual da vazão de ataques DDoS (2004–2018). 22
Figura 3 – Esquema de um ataque DRDoS. 23
Figura 4 – Esquema de um ataque DRDoS multiprotocolo. 24
Figura 5 – Esquema de um ataque DRDoS usando *carpet bombing*. 25
Figura 6 – Arquitetura do *honeypot* 35
Figura 7 – Fluxo do processamento de requisições no *honeypot* 37
Figura 8 – Número de requisições por dia 43
Figura 9 – Evolução temporal dos ataques DRDoS 45
Figura 10 – FDE da duração dos ataques (mono/multiprotocolo) 46
Figura 11 – FDE das requisições por ataque (mono/multiprotocolo) 46
Figura 12 – Incidência de ataques por dia da semana e horário (monoprotocolo) 46
Figura 13 – Incidência de ataques por dia da semana e horário (multiprotocolo) 46
Figura 14 – Requisições/ataque vs ataques/vítima (monoprotocolo) 48
Figura 15 – Requisições/ataque vs ataques/vítima (multiprotocolo) 48
Figura 16 – Evolução temporal dos ataques *Carpet Bombing* (CB) e *Specific Target* (ST) 50
Figura 17 – FDE da duração dos ataques (CB/ST) 51
Figura 18 – FDE das requisições por ataque (CB/ST) 51
Figura 19 – Incidência de ataques por dia da semana e horário (ST) 51
Figura 20 – Incidência de ataques por dia da semana e horário (CB) 51
Figura 21 – Ataques CB com antecedentes 52
Figura 22 – Requisições/ataque vs ataques/vítima (ST) 53
Figura 23 – Requisições/ataque vs ataques/vítima (CB) 53
Figura 24 – *Carpet bombing* com endereços IP concomitantes 54
Figura 25 – *Carpet bombing* com endereços IP consecutivos 54
Figura 26 – Fator médio de amplificação por protocolo 55

LISTA DE TABELAS

Tabela 1 – Linha temporal de ataques DDoS 21
Tabela 2 – Visão geral dos protocolos de rede analisados 28
Tabela 3 – Estatísticas dos ataques 41
Tabela 4 – Requisições por Protocolo 42
Tabela 5 – Distribuição de protocolos por ataque (monoprotocolo) 43
Tabela 6 – Distribuição de protocolos por ataque (multiprotocolo) 43
Tabela 7 – Distribuição de requisições por protocolo (monoprotocolo) 44
Tabela 8 – Distribuição de requisições por protocolo (multiprotocolo) 44
Tabela 9 – Distribuição de ataques *Distributed Reflection Denial of Service* (DRDoS) por países 47
Tabela 10 – Top cinco ASN por vítimas 48
Tabela 11 – Distribuição de ataques por protocolo (ST) 49
Tabela 12 – Distribuição de ataques por protocolo (CB) 49
Tabela 13 – Distribuição de requisições por protocolo (ST) 49
Tabela 14 – Distribuição de requisições por protocolo (CB) 49
Tabela 15 – Distribuição de ataques DRDoS por países 52
Tabela 16 – Top cinco ASN por vítimas 53
Tabela 17 – Distribuição das consultas observadas 57
Tabela 18 – Tipos (QTYPE) usados nas consultas 57

LISTA DE SIGLAS E ABREVIATURAS

ASN *Autonomous System Number*

CB *Carpet Bombing*

CCTV *Closed-Circuit Television Camera*

CDN *Content Delivery Network*

Chargen *Character Generator Protocol*

CIDR *Classless Inter-Domain Routing*

CFAA *Computer Fraud and Abuse Act*

CLDAP *Connection-less Lightweight Directory Access Protocol*

CPU *Central Processing Unit*

DNS *Domain Name System*

DNSSEC *Domain Name System Security Extensions*

DDoS *Distributed Denial of Service*

DRDoS *Distributed Reflection Denial of Service*

HTTP *Hypertext Transfer Protocol*

ICMP *Internet Control Message Protocol*

IoT *Internet of Things*

IP *Internet Protocol*

LDAP *Lightweight Directory Access Protocol*

mDNS *Multicast Domain Name System*

MS-SQL *Microsoft SQL Server*

NTP *Network Time Protocol*

PLATO *Programmed Logic for Automatic Teaching Operations*

QOTD *Quote of the Day*

RIP *Routing Information Protocol*

RR *Resource Record*

RRL *Response Rate Limiting*

SNMP *Simple Network Management Protocol*

SSDP *Simple Service Discovery Protocol*

ST *Specific Target*

TCP *Transmission Control Protocol*

TFTP *Trivial File Transfer Protocol*

TTL *Time To Live*

UDP *User Datagram Protocol*

UDESC Universidade do Estado de Santa Catarina

WTO *World Trade Organization*

XML *Extensible Markup Language*

LISTA DE SÍMBOLOS

$\approx$	Aproximação
#	Sinal numérico

SUMÁRIO

1 INTRODUÇÃO 16
1.1 OBJETIVO 17
1.2 ESTRUTURA DO DOCUMENTO 18

2 FUNDAMENTAÇÃO TEÓRICA 19
2.1 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO (DDOS) . . . 19
2.2 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO POR REFLEXÃO (DRDOS) 23
2.2.1 DRDoS Multiprotocolo 24
2.2.2 *Carpet Bombing* 24
2.2.3 Protocolos usados em DRDoS 25
2.3 *HONEYPOTS* 29
2.4 TRABALHOS RELACIONADOS 30
2.5 CONSIDERAÇÕES DO CAPÍTULO 32

3 HREFLECTOR, UM HONEYPOT PARA OBSERVAÇÃO DE ATAQUES DRDOS 33
3.1 REQUISITOS 33
3.2 ARQUITETURA 34
3.3 CONSIDERAÇÕES DO CAPÍTULO 37

4 ANÁLISE DE DADOS 38
4.1 IMPLANTAÇÃO 38
4.2 DEFINIÇÕES ADOTADAS 39
4.3 ESTATÍSTICAS GERAIS DO TRÁFEGO 41
4.4 ATAQUES *DRDOS* MONOPROTOCOLO E MULTIPROTOCOLO 42
4.4.1 Características dos Ataques 42
4.4.2 Avaliação de Vítimas 47
4.5 AVALIAÇÃO DE ATAQUES *CARPET BOMBING* 48
4.5.1 Características dos Ataques 49
4.5.2 Avaliação de Vítimas 52
4.6 AVALIAÇÃO DOS *PAYLOADS* 54
4.7 DISCUSSÃO DOS RESULTADOS 58
4.8 CONSIDERAÇÕES DO CAPÍTULO 60

5 CONCLUSÃO 61

REFERÊNCIAS 63

1 INTRODUÇÃO

Ataques de negação de serviço ou *Distributed Denial of Service* (DDoS) estão presentes na Internet há cerca de 25 anos (MANSFIELD-DEVINE, 2015). Nesses ataques, um conjunto de máquinas envia tráfego para uma vítima de forma coordenada. Este volume de dados é responsável pela saturação de recursos computacionais na vítima, causando indisponibilidade de serviços e prejudicando clientes legítimos (NAZARIO, 2008).

Um tipo particular de ataque DDoS são os ataques distribuídos de negação de serviço por reflexão (*Distributed Reflection Denial of Service*, DRDoS), nos quais o tráfego de ataque não é enviado diretamente para a vítima, mas para um conjunto de intermediários, chamados de refletores (PAXSON, 2001). O atacante envia tráfego para um refletor usando como endereço *Internet Protocol* (IP) de origem o endereço da vítima, fazendo com que o refletor direcione o tráfego de resposta para a vítima e não de volta para o atacante. Ataques DRDoS oferecem as seguintes vantagens para um atacante (ROSSOW, 2014):

1. Dificuldade para identificar a origem dos ataques, uma vez que o tráfego recebido pela vítima vem dos refletores, que são meros intermediários explorados inadvertidamente;
2. O tráfego refletido para a vítima geralmente é maior (em largura de banda) do que o tráfego enviado pelo atacante, pois é comum que as respostas sejam maiores que as requisições correspondentes. Esse efeito é conhecido como amplificação; e
3. O uso simultâneo de múltiplos refletores permite que um ataque altamente distribuído seja efetuado a partir de um conjunto reduzido de máquinas.

Diversos protocolos podem ser explorados para ataques DRDoS, tais como *Domain Name System* (DNS), *Network Time Protocol* (NTP) e *Simple Service Discovery Protocol* (SSDP) (PROLEXIC, 2013; ROSSOW, 2014; RYBA et al., 2015). Embora haja a predominância de protocolos de aplicação que adotam o *User Datagram Protocol* (UDP) como protocolo de transporte, ataques DRDoS também podem explorar o *Transmission Control Protocol* (TCP) (KÜHRER et al., 2014b).

Duas tendências recentes em ataques DRDoS são (NETSCOUT, 2019):

1. Ataques multiprotocolo, ou seja, ataques que usam múltiplos protocolos simultaneamente contra uma mesma vítima (NETSCOUT; ARBOR, 2017).

2. Ataques *carpet bombing*, nos quais o tráfego é direcionado para múltiplos endereços IP na mesma sub-rede, em vez de para um único endereço IP.

Em linhas gerais, essas variações de ataques DRDoS objetivam aumentar o poder de fogo dos atacantes, possibilitando que estes atinjam mais facilmente volumes de tráfego suficientes para causar disrupções, e dificultar a detecção e reação aos ataques, ampliando o conjunto de protocolos e alvos que precisam ser monitorados e controlados.

Tendo em vista a relevância dos ataques DRDoS, um foco importante de pesquisa tem sido a análise e caracterização do tráfego associado a esses ataques, com vistas a compreender melhor o seu funcionamento na prática, e assim permitir uma evolução dos mecanismos de defesa. Os trabalhos encontrados na literatura que abordam ataques DRDoS podem ser classificados em dois grupos. O primeiro grupo consiste de trabalhos que estudam um único protocolo, realizando uma caracterização dos ataques e métodos explorados, como pode ser visto em (ANAGNOSTOPOULOS et al., 2013; RUDMAN; IRWIN, 2015; NOROOZIAN et al., 2016; BAIA, 2018; HEINRICH; LONGO; OBELHEIRO, 2017). O segundo grupo abrange trabalhos que abordam diversos protocolos (KÜHRER et al., 2014a; ROSSOW, 2014; THOMAS; CLAYTON; BERESFORD, 2017), verificando como tais protocolos estão sendo explorados e qual o fator de amplificação obtido pelos atacantes. Embora esses trabalhos englobem vários protocolos, eles consideram cada protocolo isoladamente.

A literatura não explora ataques DRDoS multiprotocolo nem ataques *carpet bombing*. O presente trabalho visa a preencher esta lacuna por meio da coleta, análise e caracterização de tráfego de ataques DRDoS, com ênfase em ataques multiprotocolo e *carpet bombing*. A partir de tráfego DRDoS coletado por um *honeypot*[1], são exploradas questões como a duração e a intensidade dos ataques, com que frequência eles ocorrem, quais protocolos são mais usados e quem são as vítimas mais afetadas.

1.1 OBJETIVO

O objetivo geral deste trabalho é analisar e caracterizar o tráfego de ataques DRDoS, com o enfoque em ataques multiprotocolo e ataques *carpet bombing* por intermédio da coleta de dados efetuada por um *honeypot*. Esse objetivo geral desdobra-se nos seguintes objetivos específicos:

- Projetar e implementar um *honeypot* específico para tráfego DRDoS e que possua a capacidade de lidar com múltiplos protocolos;

[1] Um *honeypot* é um recurso computacional que possui a finalidade de ser explorado, atacado ou comprometido (HOEPERS; STEDING-JESSEN; CHAVES, 2007).

- Implantar o *honeypot* na rede da UDESC, e realizar uma coleta de dados de longa duração (6–9 meses); e
- Analisar os dados coletados pelo *honeypot* sob a perspectiva de ataques DRDoS: (1) multiprotocolo; (2) *carpet bombing*.

As contribuições advindas do cumprimento desses objetivos são:

1. A definição de um arquitetura de *honeypot* para observação de tráfego DRDoS, atendendo a requisitos de modularidade, ampla observabilidade e baixo consumo de recursos computacionais e de rede;
2. O mapeamento das técnicas usadas na exploração de diferentes protocolos baseados em UDP para a realização de ataques DRDoS;
3. O primeiro estudo na literatura sobre ataques *carpet bombing*;
4. A caracterização de tipos específicos de ataques *carpet bombing*.

1.2 ESTRUTURA DO DOCUMENTO

Este documento está organizado em cinco capítulos. O Capítulo 2 apresenta a fundamentação teórica necessária para o entendimento do trabalho, junto com a revisão de trabalhos relacionados. O Capítulo 3 discute a implementação do *honeypot*. O Capítulo 4 apresenta a análise dos dados coletados pelo *honeypot*. Por fim, o Capítulo 5 traz as considerações finais e perspectivas futuras da pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo faz uma revisão de conceitos necessários ao entendimento do trabalho. A Seção 2.1 trata de ataques DDoS em geral. A Seção 2.2 aborda de forma específica ataques DRDoS. A Seção 2.3 apresenta os principais aspectos de *honeypots*. A Seção 2.4 discute os trabalhos relacionados.

2.1 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO (DDOS)

Um ataque distribuído de negação de serviço (*distributed denial of service*, DDoS) usa de forma coordenada diversos *hosts* Internet para enviar tráfego para uma vítima, objetivando deixar sistemas computacionais e redes indisponíveis para seus usuários legítimos (NAZARIO, 2008; MANSFIELD-DEVINE, 2015). O atacante não tem a finalidade de invadir ou coletar informações dos usuários, e sim dificultar ou impossibilitar o acesso a certos recursos (CERT.BR, 2016).

A indisponibilidade de recursos computacionais causada por ataques DDoS pode dificultar ou impedir o acesso a serviços essenciais. Ela também pode gerar prejuízos financeiros pela impossibilidade de realizar transações comerciais ou prestação de serviços pela Internet (MANSFIELD-DEVINE, 2016). As principais motivações por trás dos ataques DDoS incluem retaliação (por exemplo, contra grupos anti-SPAM), ganho financeiro mediante extorsão (por exemplo, contra *sites* de apostas), e apoio a causas políticas ou sociais (hacktivismo) (NAZARIO, 2008; MANSFIELD-DEVINE, 2015).

Pela sua natureza, ataques DDoS são difíceis de mitigar, uma vez que, quando o tráfego de ataque atinge a rede da vítima, é provavelmente muito tarde para tomar qualquer atitude. Existem diversas estratégias que podem ser usadas para reduzir o problema, sendo que as mais usadas na prática são (NAZARIO, 2008; TURNER, 2014; WEAGLE, 2016):

1. Ampliar a capacidade de rede para suportar volumes de tráfego acima do esperado.
2. Solicitar que o provedor Internet bloqueie tráfego de ataque o mais próximo da origem e o mais distante da borda possível.
3. Usar uma rede de distribuição de conteúdo ou *Content Delivery Network* (CDN), que replica conteúdo em servidores espalhados pela Internet, para conseguir absorver mais tráfego.

4. Implantar um equipamento (*appliance*) específico para identificação e filtragem de tráfego DDoS na borda da rede da vítima.

5. Usar um serviço de filtragem basedo em nuvem (*scrubber*). Esse serviço, que tem alta capacidade de rede, recebe todo o tráfego que seria direcionado à vítima e repassa apenas o tráfego identificado como legítimo, filtrando tráfego de ataque.

Essas estratégias podem ser adotadas individualmente ou em conjunto, o que é considerado mais eficaz. Por exemplo, existem *appliances* de borda de rede que filtram tráfego até um determinado volume, e redirecionam o tráfego para um serviço de *scrubbing* quando o ataque se torna muito intenso.

A Figura 1 ilustra de forma simplificada um ataque DDoS. Um atacante controla um conjunto de *hosts* intermediários, chamados de agentes ou *bots* – máquinas infectadas com *malware* que permite que elas sejam controladas remotamente. Essa *botnet* (nome dado a um conjunto de *bots* sob controle de uma mesma pessoa ou grupo) recebe comandos do atacante para enviar tráfego de ataque para uma ou mais vítimas. Em vez de *bots*, um atacante pode utilizar máquinas de voluntários que participam de campanhas de hacktivismo (MANSFIELD-DEVINE, 2015). Existem ainda grupos organizados que oferecem *DDoS as a Service* ou *booters*, que alugam suas *botnets* para realização de ataques DDoS, por valores tão baixos quando US$ 1 (SANTANNA et al., 2015).

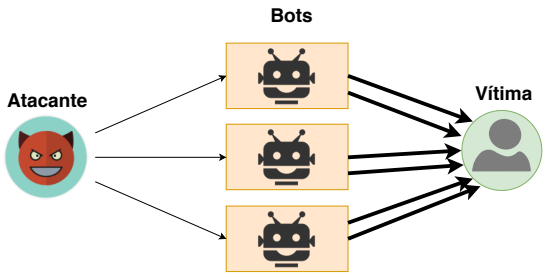

Figura 1 – Esquema de um ataque DDoS.

Fonte: Autor.

A Tabela 1 retrata a evolução dos ataques DDoS ao longo dos anos. A finalidade é a apresentar qual o impacto que os ataques obtiveram ao decorrer dos anos e quais os métodos explorados para a sua realização (REVUELTO; MEINTANIS; SOCHA, 2017).

A Figura 2 mostra a vazão atingida pelo maior ataque DDoS registrado em cada ano, considerando o período entre 2004 e 2018. O gráfico ilustra o crescimento na intensidade dos ataques ao longo dos anos. O volume de tráfego não é a única

1974	O primeiro ataque registrado foi realizado explorando uma vulnerabilidade em um mainframe conhecido como *Programmed Logic for Automatic Teaching Operations* (PLATO) (DENNIS, 2010).
1988	Robert Morris criou um *malware* conhecido atualmente como *worm* (Morris worm), este foi responsável por paralisar grande parte da Internet (WOODY; SHOEMAKER; MEAD, 2012). Um total de 6000 sistemas UNIX foram infectados para a realização do ataque, por consequência foi a primeira pessoa a ser condenada pela *Computer Fraud and Abuse Act* (CFAA) (CORNELL, 1984).
1995	O *Strano Network* abria um conjunto elevado de conexões em páginas web como forma de protesto contra a política nuclear do governo francês (COX, 2014).
1997	A primeira demostração pública do ataque DDoS foi realizada por Khan C. Smith, durante o evento grandes corporações acabaram sendo atacadas.
1998	*The Electronic Disturbance Theater* atraves do *FloodNet* realizou ataques até o final de 1999, auxiliando protestos no México e realizando ataques em *World Trade Organization* (WTO). Em 1998 também foi realizado o primeiro ataque de reflexão conhecido como *Smurf attacks* que explora o *Internet Control Message Protocol* (ICMP) (RYBA et al., 2015).
1999	Surgimento da *botnet Trinoo* utilizada para a realização de ataques DDoS (LEMOS, 2016). No mesmo ano foi avisado sobre a possibilidade de utilizar o DNS para a realização de ataques DDoS (NIST, 1999; CERT/TCC, 1999).
2003	O primeiro *flash worm* (*Slammer worm*) infectou 75 milhões de *hosts* em dez minutos e alcançou 80 milhões de pacotes por segundo.
2009	O *worm MyDoom* foi reaproveitado para infectar 50 mil *hosts* e realizar um ataque que alcançou picos de 13Gbps (ZETTER, 2009).
2012	Crescimento nos ataques DRDoS explorando DNS, *Character Generator Protocol* (Chargen), NTP e *Simple Network Management Protocol* (SNMP) (PROLEXIC, 2013).
2013	30.000 servidores DNS fizeram parte em um ataque contra a *Spamhaus* que atingiu picos de 300 Gbps (PRINCE, 2013). Outros ataques realizados que obtiveram um fator de amplificação próximo a 100 Gbps (RYBA et al., 2015; BREWSTER, 2013)
2014	Com um crescimento no número dos ataques DRDoS (PRINCE, 2014), o NTP foi explorado para realizar ataques que atingiram picos de 400 Gbps (LOPES, 2015).
2016	Mais de 150.000 dispositivos *Internet of Things* (IoT) são explorados para realizar ataques que alcançaram ≈ 1 Tbps de tráfego (em sua grande maioria o tráfego foi gerado por *Closed-Circuit Television Camera* (CCTV)) (KHANDELWAL, 2016).
2018	Atacantes exploram servidores que deixaram serviços Memcached abertos na Internet para realizar ataques ao Github.O ataque deixou os serviços do Github indisponíveis por dois períodos de tempo e alcançou picos de ≈ 1.4 Tbps de tráfego, sendo classificado como o maior ataque de amplificação já registrado (NEWMAN, 2018). Uma semana depois deste ataque a NETSCOUT (BIENKOWSKI; ARBOR, 2018) registrou um ataque de ≈ 1.7 Tbps de tráfego, que foi realizado pelo mesmo vetor explorado anteriormente.

Fonte: Autor.

TABELA 1 Linha temporal de ataques DDoS

característica que tem crescido, a complexidade nos ataques também evoluiu (BIENKOWSKI; ARBOR, 2018) .

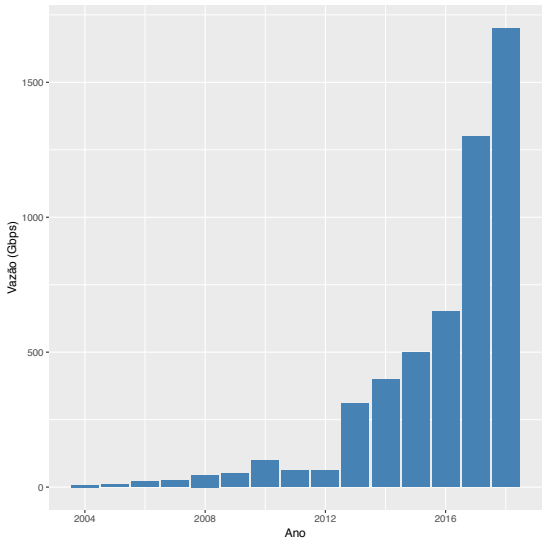

Figura 2 – Evolução anual da vazão de ataques DDoS (2004–2018).

Fonte: (BIENKOWSKI; ARBOR, 2018).

Diversas classificações de ataques DDoS já foram propostas na literatura, tais como (MIRKOVIC; REIHER, 2004; SPECHT; LEE, 2004; KESSLER, 2012; DEKA; BHATTACHARYYA; KALITA, 2017). Mirkovic e Reiher (2004) dividem os ataques em duas classes segundo a fraqueza que eles exploram:

1. Ataques de força bruta ou volumétricos: enviam uma vasta quantidade de requisições legítimas para a vítima, levando à saturação um ou mais de seus recursos (enlaces de acesso, equipamentos de rede, servidores, aplicações).

2. Ataques semânticos ou de vulnerabilidade: exploram uma característica específica ou um *bug* de um protocolo ou aplicação instalada na vítima, levando ao consumo excessivo de recursos computacionais (processador, memória, disco, *sockets*, limites de usuários simultâneos, tabelas do sistema operacional).

Essas classificações não são mutuamente exclusivas. Mesmo que ataques semânticos possam ser eficazes mesmo com baixo volume, nada impede que um ataque de força bruta envie um grande volume de requisições que exploram alguma vulnerabilidade. A maior diferença entre os dois tipos de ataque está nas contramedidas (MIRKOVIC; REIHER, 2004): enquanto muitos ataques semânticos podem ser anulados corrigindo as vulnerabilidades exploradas ou filtrando o tráfego, ataques de força bruta exigem mecanismos que permitam lidar com tráfego excessivo, como já discutido.

2.2 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO POR REFLEXÃO (DRDOS)

Em ataques distribuídos de negação de serviço por reflexão (*distributed reflection denial of service*, DRDoS), os *bots* enviam tráfego de ataque não diretamente à vítima, mas a *hosts* intermediários chamados de refletores (PAXSON, 2001; ROSSOW, 2014), conforme mostrado na Figura 3. Um refletor é qualquer sistema que responda a tráfego IP com endereço de origem forjado (PAXSON, 2001); exemplos incluem nós que respondem a tráfego ICMP e servidores UDP e TCP. 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*, como seria de se esperar. É importante destacar que os refletores não são controlados pelo atacante, mas sistemas vulneráveis ou mal configurados que são abusados para a realização de ataques.

O caso mais interessante de refletor é aquele que oferece amplificação, isto é, cujas respostas são (muito) maiores do que as requisições correspondentes (ROSSOW, 2014). Por exemplo, uma consulta DNS de 40–50 bytes pode induzir uma resposta de até 4 KB. Devido à amplificação, um atacante precisa gerar menos tráfego para produzir o mesmo resultado sobre a vítima, quando comparado a um ataque DDoS sem reflexão.

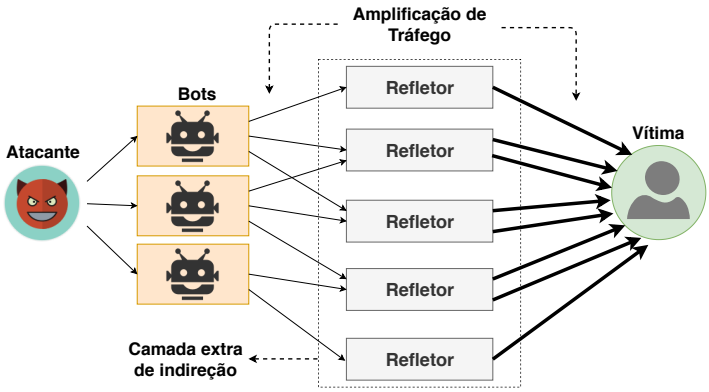

Figura 3 – Esquema de um ataque DRDoS.

Fonte: Autor.

Vários protocolos podem ser explorados para obter reflexão (ROSSOW, 2014). O caso mais comum são servidores baseados em UDP, devido ao fato deste protocolo usar datagramas (ou seja, ser um protocolo sem conexão), mas ICMP e TCP também podem ser usados. A Seção 2.2.3 discute de forma mais detalhada como diversos protocolos são usados em ataques DRDoS.

Os refletores usados em um ataque DRDoS dificultam tanto a mitigação do ataque quanto a identificação do seu autor. A mitigação é prejudicada porque, como

os refletores também podem originar tráfego legítimo, a filtragem indiscriminada de tráfego proveniente dos refletores causará prejuízo a essas requisições legítimas. Além disso, a identificação de autoria fica ainda mais complicada do que em ataques DDoS sem reflexão, devido à necessidade de descobrir quais são os *bots* que estão enviando tráfego para os refletores antes de tentar rastrear quem está controlando esses *bots* (o que não raro envolve mais de uma camada de nós, tipicamente em redes e jurisdições distintas).

2.2.1 DRDoS Multiprotocolo

Ataques DRDoS em que múltiplos protocolos são usados simultaneamente têm sido reportados com alguma frequência (NETSCOUT, 2019). Existem casos em que ataques de força bruta por reflexão são combinados com ataques semânticos, tipicamente contra servidores *Hypertext Transfer Protocol* (HTTP). Em outros casos, refletores de diferentes protocolos são usados ao mesmo tempo, o que chamamos de ataques DRDoS multiprotocolo. A Figura 4 ilustra ataques DRDoS multiprotocolo usando três protocolos, DNS, NTP e Memcached.

O uso de múltiplos protocolos traz como vantagens para os atacantes a possibilidade de usar um universo maior de refletores (no caso de ataques por reflexão); e a dificuldade adicional gerada para a defesa, que não pode simplesmente filtrar todo o tráfego de um protocolo não essencial.

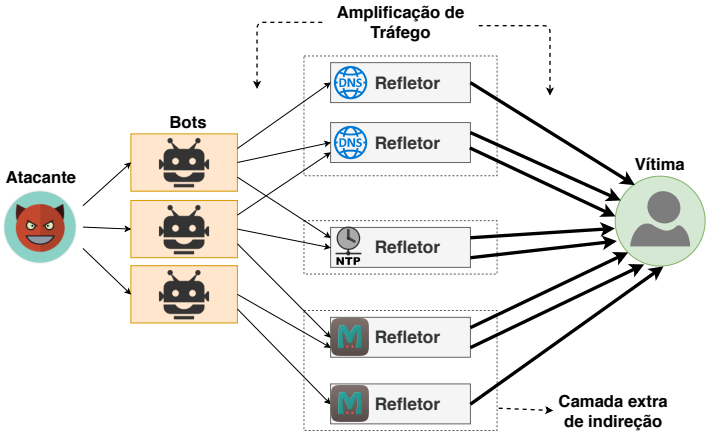

Figura 4 – Esquema de um ataque DRDoS multiprotocolo.

Fonte: Autor.

2.2.2 *Carpet Bombing*

Um método que tem sido empregado em ataques DRDoS é chamado de *carpet bombing*, e consiste em direcionar o tráfego para múltiplos endereços IP na mesma

sub-rede, em vez de para um único endereço IP (NETSCOUT, 2019). O objetivo é saturar os enlaces de acesso das vítimas desejadas, e, ao mesmo tempo, dificultar a detecção e mitigação do ataque. Nesse caso, a detecção exige a identificação de tráfego anômalo em sub-redes inteiras em vez de identificar fluxos anômalos envolvendo um único endereço IP, enquanto a mitigação envolve desviar o tráfego das sub-redes completas para um serviço anti-DDoS (*scrubber*).

Como o ataque pretende saturar o enlace de acesso e/ou o roteador de borda, os endereços IP para os quais o tráfego é enviado não precisam estar ativos na rede. Mesmo que o tráfego seja descartado na borda, ainda assim ele consume largura de banda e capacidade de processamento do roteador. A Figura 5 representa um ataque *carpet bombing*, ao qual um conjunto de hosts em uma rede esta sendo atacado.

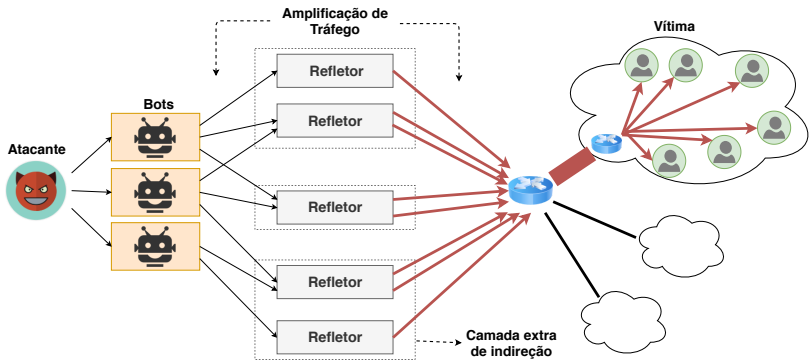

Figura 5 – Esquema de um ataque DRDoS usando *carpet bombing*.

Fonte: Autor.

2.2.3 Protocolos usados em DRDoS

Diversos protocolos podem ser usados para efetuar ataques DRDoS. A maioria são protocolos de aplicação que usam UDP como protocolo de transporte, mas existem também ataques por reflexão usando protocolos como ICMP e TCP. Diversos fatores influenciam a popularidade dos protocolos, principalmente o fator de amplificação alcançado e a disponibilidade de refletores abertos na Internet. Esta seção apresenta os protocolos mais relevantes com base em (DDOSMON, 2018), e discute as características desses protocolos que são exploradas nos ataques.

O protocolo DNS (*Domain Name System*) (MOCKAPETRIS, 1987a; MOCKAPETRIS, 1987b) desempenha uma funcionalidade essencial para a operação da Internet, sendo responsável por, entre outras funcionalidades, realizar a associação de um nome de domínio com um endereço IP. O DNS pode usar tanto UDP quanto TCP como protocolo de transporte, embora o primeiro seja muito mais usado por razões de desempenho. Servidores DNS podem desempenhar dois papeis, o de servidor au-

toritativo e o de servidor recursivo (MOCKAPETRIS, 1987b). Um servidor autoritativo é responsável por um ou mais domínios, e deve responder a consultas de qualquer origem para nomes pertencentes a seus domínios. Para evitar o abuso, incluindo ser usado como refletor, recomenda-se que um servidor autoritativo implemente um mecanismo de limitação de taxa de respostas (*Response Rate Limiting* (RRL)) (GOLDLUST, 2018). Um servidor DNS recursivo, por sua vez, é responsável por resolver nomes para um conjunto específico de clientes. Servidores DNS recursivos deveriam ter acesso restrito a clientes autorizados, mas na prática muitos servidores não implementam essa restrição, o que os torna servidores recursivos abertos, que podem ser usados como refletores (HOEPERS, 2016). O DNS oferece um fator de amplificação próximo a 100, uma vez que consultas na ordem de 40 bytes podem gerar respostas de mais de 4.000 bytes (HEINRICH; LONGO; OBELHEIRO, 2017). Respostas grandes podem ser obtidas consultando domínios que implementam *Domain Name System Security Extensions* (DNSSEC) (extensões de segurança do DNS) (RIJSWIJK-DEIJ; SPEROTTO; PRAS, 2014), ou mesmo domínios criados especialmente com o propósito de gerar amplificação, como descrito em (ANAGNOSTOPOULOS et al., 2013; HEINRICH; LONGO; OBELHEIRO, 2017).

O NTP (*Network Time Protocol*) (VYNCKE, 2019) é um protocolo amplamente utilizado para a sincronização de relógios através da Internet. A amplificação no NTP é obtida usando o comando `MONLIST`, que retorna a lista dos últimos 600 *hosts* que interagiram com o servidor, gerando assim uma resposta grande, que muitas vezes requer múltiplos datagramas. Embora o comando `MONLIST` não faça parte da especificação do NTP, ele é suportado por muitos servidores, que frequentemente não restringem o uso dessa funcionalidade de monitoração a clientes autorizados (CZYZ et al., 2014).

Memcached é um sistema de *cache* em memória com ampla utilização para otimização de banco de dados (MEMCACHED, 2019), que pode usar tanto UDP quanto TCP como protocolo de transporte. As duas maneiras mais populares de explorar o Memcached em ataques DRDoS são (NEWMAN, 2018; BAIA, 2018):

- Realizar consultas solicitando estatísticas do sistema (comando `stats`), o que gera uma mensagem de aproximadamente 1,3 KB contendo várias informações da aplicação, como *uptime*, versão da aplicação e bytes lidos/escritos em memória; e
- Inserir um par chave-valor (comando `set`) em que o conteúdo é volumoso (por padrão os valores são limitados a 1 MB), e posteriormente efetuar consultas com a chave inserida previamente (comando `get`).

Os protocolos Chargen e *Quote of the Day* (QOTD) servem como ferramentas de depuração e medição (POSTEL, 1983a; POSTEL, 1983b). O primeiro envia um número aleatório de caracteres (entre 0 e 512) ao receber um datagrama UDP, cujo conteúdo é ignorado (POSTEL, 1983a). O QOTD é similar, mas envia uma citação (cujo conteúdo não é definido pela especificação) de até 512 caracteres imprimíveis (POSTEL, 1983b). A amplificação ocorre porque, como o conteúdo da requisição é ignorado, esta pode ser muito pequena (uma requisição com 1 byte de *payload* tem 29 bytes com os cabeçalhos IP e UDP).

O SSDP (GOLAND et al., 1999) é utilizado para anúncio e descoberta de serviços na rede, com o intuito de encontrar automaticamente dispositivos no ambiente, como impressoras. Ataques DRDoS usando o SSDP enviam comandos de busca (`M-SEARCH`) especificando como tipo de dispositivo uma das *strings* `upnp:rootdevice` ou `ssdp:all` (MAJKOWSKI, 2017); buscas por esses tipos são respondidos pela maioria dos dispositivos. Cada dispositivo explorado responderá a solicitação, gerando um fator de amplificação de até 30 vezes.

O *Routing Information Protocol* (RIP) (HEDRICK, 1988) é um protocolo de roteamento que usa transporte UDP. A versão 1 do protocolo (RIPv1) pode ser usada em ataques DRDoS, apesar de ter sido oficialmente declarada obsoleta (HALPERN, 1996). O protocolo permite que um roteador solicite rotas para seus supostos vizinhos, tipicamente usando o endereço de *broadcast* 255.255.255.255. Todos os roteadores que recebem essas mensagens enviam sua tabela de roteamento para a origem, o que pode demandar múltiplos pacotes, pois cada mensagem RIP contém no máximo 25 rotas. Em ataques DRDoS, os atacantes enviam um grande número de requisições de rotas para roteadores que respondem a tráfego RIPv1, preferencialmente aqueles que tenham tabelas de roteamento com diversas entradas (AKAMAI, 2016).

O *Connection-less Lightweight Directory Access Protocol* (CLDAP) (YOUNG, 1995) é uma versão simplificada do *Lightweight Directory Access Protocol* (LDAP) sobre transporte UDP. O CLDAP é usado por servidores Active Directory, que provêm serviços de diretório em redes Windows. Para obter amplificação usando CLDAP, um atacante envia requisições de NETLOGON que solicitam uma lista de atributos suportados pelo servidor (MCAULEY, 2016). O fator de amplificação alcançado com o CLDAP pode chegar a 70 vezes (ARTEAGA; MEJIA, 2017).

Muitos jogos *online* usam UDP como transporte. Plataformas de jogos como a Steam (VALVE, 2019) permitem que usuários possam virar *host* dos seus próprios servidores e até mesmo *hosts* privados podem ser explorados para a realização dos ataques (NOLLA, 2013). Este tipo de ataque explora diferentes *payloads* e protocolos, como por exemplo RCON, Quake e Half-life. Uma forma comum de obter amplificação é consultando a lista de servidores conhecidos para o jogo, pois a resposta pode

demandar o envio de vários pacotes (VALVE, 2017).

Protocolo/Seviços	**Referência**	**Fator de Amplificação**
DNS	(HOEPERS, 2016)	28-54
DNSSEC	(RIJSWIJK-DEIJ; SPEROTTO; PRAS, 2014)	40-55
NTP	(CZYZ et al., 2014)	556.9
Memcached	(NEWMAN, 2018; BAIA, 2018)	10.000-51.000
Chargen	(ROSSOW, 2014)	358.8
QOTD	(CERT, 2018)	140.3
SSDP	(MAJKOWSKI, 2017)	30.8
RIP	(AKAMAI, 2016)	131.24
CLDAP	(ARTEAGA; MEJIA, 2017; CHOI; KWAK, 2017)	33-70
LDAP	(CERT, 2018)	46-55
Steam	(NOLLA, 2013; CERT, 2018) (*RCON*)	5.5
Quake 3	(ROSSOW, 2014)	63.9
half-life	(NOLLA, 2013)	109.8
SNMP	(PROLEXIC, 2012; BITAG, 2015)	6.3
Trivial File Transfer Protocol (TFTP)	(SIEKLIK; MACFARLANE; BUCHANAN, 2016)	60
ICMP	(CERT/CC, 1998; KUMAR, 2007)	não disponível
HTTP	(BECKETT; SEZER, 2017)	79-100

Tabela 2 – Visão geral dos protocolos de rede analisados

O *Simple Network Management Protocol* (SNMP) (CASE, 1990) é um protocolo de gerenciamento de redes que usa transporte UDP. O SNMP expõe dados e controles de gerenciamento de equipamentos de rede como variáveis que podem ser consultadas e manipuladas por um agente. Para obter amplificação com o SNMP é usada uma requisição do tipo `GetBulkRequest`, que tem como parâmetro o identificador de uma variável e retorna o valor dessa variável juntamente com o de múltiplas variáveis que a sucedem em ordem lexicográfica (PROLEXIC, 2012; BITAG, 2015).

O *Trivial File Transfer Protocol* (TFTP) (SOLLINS, 1992) é um protocolo simples de transferência de arquivos que usa transporte UDP. O TFTP tipicamente é utilizado em redes locais para transferência de arquivos de configuração e imagens de *boot* entre equipamentos de rede e um servidor. O uso de TFTP em ataques DRDoS envolve a requisição para que o servidor envie um arquivo (tipicamente com um nome curto, como "`/x`") (SIEKLIK; MACFARLANE; BUCHANAN, 2016); mesmo quando o arquivo é inexistente, uma resposta de erro maior do que a requisição é enviada para a vítima (AKAMAI, 2015).

Ataques *smurf* (CERT/CC, 1998) exploram mensagens ICMP Echo Request enviadas para o endereço de *broadcast* de uma rede. A ideia é que todos os *hosts* ativos respondam com uma mensagem ICMP Echo Reply, provocando assim a amplificação. Embora esse ataque tenha se tornado menos eficaz, pois muitos sistemas operacionais modernos desabilitam a resposta a mensagens ICMP Echo Request enviadas para um endereço de *broadcast*, ainda hoje ele pode ser encontrado na Internet.

O protocolo TCP também pode ser explorado para realizar ataques DRDoS (KÜHRER et al., 2014b). Um atacante envia segmentos SYN com endereço IP de origem forjado, e o *host* contactado responde com SYN+ACK para a vítima. Embora os segmentos SYN e SYN+ACK possuam o mesmo tamanho, pode ocorrer amplificação em caso de retransmissão do SYN+ACK. Embora o fator de amplificação raramente passe de seis, ele pode chegar a 20 (KÜHRER et al., 2014b).

A Tabela 2 resume os protocolos usados em DRDoS, apontando trabalhos que exploram cada um e o fator de amplificação proporcionado. Observa-se uma variada gama de protocolos, que inclui protocolos bastante populares (como DNS e NTP), protocolos legados (como Chargen, QOTD e RIPv1) e protocolos de jogos. Este levantamento de protocolos serviu de base no projeto e implementação de um *honeypot* multiprotocolo voltado para a coleta de dados sobre ataques DRDoS.

2.3 *HONEYPOTS*

Um *honeypot* é um recurso computacional que possui o objetivo de ser sondado, atacado ou até mesmo comprometido (SPITZNER, 2003; HOEPERS; STEDING-JESSEN; CHAVES, 2007). *Honeypots* são extensivamente monitorados para possibilitar o estudo do comportamento e das atividades dos atacantes, levando à descoberta de novos ataques e de como ataques já conhecidos na teoria são realizados na prática.

Geralmente um *honeypot* é um *host* que possui um endereço público na Internet, o qual não é anunciado. Por consequência o *host* precisa ser descoberto para a realização de qualquer tipo de interação com o sistema, o que exige algum tipo de mapeamento realizado pelos atacantes. Desta forma, é possível afirmar que qualquer interação realizada com o *honeypot* é considerada suspeita.

Quanto mais funcionalidades um *honeypot* implementa e quanto mais possibilidades de interação ele oferece, maior e mais detalhado é o comportamento dos atacantes que esse *honeypot* pode observar e coletar. No entanto, quanto mais funcionalidade for exposta aos atacantes, maior é o dano potencial que um atacante pode provocar (SPITZNER, 2003). Esse dano pode ser causado ao próprio *honeypot* e/ou a outros sistemas, usando o *honeypot* como uma plataforma de ataque. Esses riscos tipicamente são mitigados instalando o *honeypot* em um segmento de rede isolado

do restante da organização e tendo mecanismos que inutilizem o *honeypot* como ferramenta de ataque a outros *hosts* e redes, principalmente externos.

Tendo em vista o *trade-off* entre visibilidade do comportamento dos atacantes e o risco de abuso, os *honeypots* podem ser classificados de acordo com o seu nível de interatividade (SPITZNER, 2003):

- Um *honeypot* de baixa interatividade basicamente emula algumas funcionalidades de um sistema vulnerável, permitindo uma observação mais restrita do comportamento dos atacantes mas oferecendo um risco menor. Um exemplo seria um *listener* UDP para um dado protocolo que registrasse todas as requisições recebidas e retornasse apenas uma resposta fixa.
- Um *honeypot* de alta interatividade, por outro lado, permite que atacantes interajam com aplicações e serviços reais, o que oferece uma visão mais detalhada de suas atividades mas introduz um nível maior de risco. Um exemplo seria usar um servidor real para um dado protocolo, instrumentado para permitir máxima observabilidade; e
- Entre esses extremos se situam os *honeypots* de média interatividade, que oferecem níveis intermediários de visibilidade e risco.

No caso de ataques DRDoS, que são o foco deste trabalho, o *honeypot* utilizado possui a funcionalidade de refletor. Com isso, ele captura a interação dos *bots* ou agentes com os refletores (Figura 3), e os endereços IP de origem no tráfego de ataque correspondem a endereços de vítimas, já que esses ataques empregam IP *spoofing*. Esse *honeypot* pode ser classificado como de média interatividade, pois, para alguns dos protocolos suportados (DNS e Memcached), o *honeypot* atua como um *proxy*, repassando parte das requisições recebidas para servidores que implementam esses protocolos. Para outros protocolos, o próprio *honeypot* sintetiza respostas, não havendo qualquer interação com servidores reais.

2.4 TRABALHOS RELACIONADOS

Ataques DDoS e DRDoS são explorados de diversas maneiras na literatura, incluindo:

- Evolução temporal de ataques (RYBA et al., 2015; DEKA; BHATTACHARYYA; KALITA, 2017);

- Crescimento dos ataques em decorrência dos mercados de *booters*/*DDoS-for-hire* (MANSFIELD-DEVINE, 2015; SANTANNA et al., 2015; KARAMI; PARK; MCCOY, 2016);
- Algoritmos para a identificação de tráfego DDoS (LIU et al., 2015; MEITEI; SINGH; DE, 2016; ZHANG; ZHANG; YU, 2017; SHARMA; GULERIA; SINGLA, 2018)

O foco deste trabalho é a caracterização de ataques DRDoS reais com base em dados coletados usando um *honeypot*. A seguir são discutidos trabalhos que possuem enfoque na caracterização de tráfego DDoS e DRDoS.

Vários trabalhos são dedicados a um protocolo específico, como DNS (ANAGNOSTOPOULOS et al., 2013; RIJSWIJK-DEIJ; SPEROTTO; PRAS, 2014; FACHKHA; BOUHARB; DEBBABI, 2015; HEINRICH; LONGO; OBELHEIRO, 2017) e NTP (CZYZ et al., 2014; RUDMAN; IRWIN, 2015). As características de ataque examinadas incluem distribuição temporal, intensidade e duração dos ataques, localização das vítimas, atributos de nível de pacote (*Time To Live* (TTL), tamanho), fator de amplificação e *payloads*.

Rossow (2014) estuda como 14 protocolos distintos podem ser explorados em ataques de amplificação, e estima o fator de amplificação que cada um oferece. O trabalho também realiza análise de tráfego: dados de fluxos de um provedor Internet europeu são usados para identificar vítimas e refletores dentro da rede, varreduras de UDP direcionadas a endereços não alocados (*darknet*) foram usados para identificar potenciais atacantes, e *honeypots* foram usados principalmente para confirmar a ocorrência de ataques, sem uma análise mais aprofundada.

Krämer et al. (2015) apresentaram AmpPots, que são *honeypots* projetados para a observação e coleta de tráfego DRDoS envolvendo nove protocolos (NTP, DNS, Chargen, SSDP, MS-SQL, NetBIOS, QOTD, SIP e SNMP). O trabalho analisou dados coletados de 21 AmpPots entre fevereiro e maio de 2015, totalizando mais de 1,5 milhões de ataques, e descreveu características como duração, tipos de *payloads* usados, e geolocalização das vítimas. Eles também realizaram uma análise de *botnets* usadas para DDoS.

Noroozian et al. (2016) analisam tráfego de ataques DRDoS coletados por oito AmpPots entre 2014 e 2015, considerando seis protocolos (NTP, DNS, Chargen, SSDP, QOTD e SNMP). O foco do trabalho é a caracterização das vítimas dos ataques DRDoS, incluindo seu tipo de rede (banda larga, hospedagem, empresa) e geolocalização. O trabalho também discute a duração dos ataques por tipo de vítima.

Thomas, Clayton e Beresford (2017) analisam tráfego DRDoS observado por 65 *honeypots* UDP que implementam oito protocolos (QOTD, Chargen, DNS, NTP,

SSDP, *Microsoft SQL Server* (MS-SQL), Portmap, and *Multicast Domain Name System* (mDNS)). Foram registrados mais de 5,8 milhões de ataques em um período de 1010 dias, tendo sido avaliados o comportamento de varreduras de rede e várias características de ataques, como duração, número de ataques e número de requisições. NTP e DNS foram os protocolos mais populares, e também houve um volume significativo de requisições de SSDP.

Embora os estudos citados tenham investigado ataques DRDoS envolvendo vários protocolos, eles praticamente ignoram como esses protocolos são usados em conjunto. Na realidade, Krämer et al. (2015) reconhecem a existência de ataques usando múltiplos protocolos, mas não exploram esse aspecto. Nenhum desses estudos considera ataques de *carpet bombing*. O diferencial deste trabalho, portanto, reside na investigação de ataques multiprotocolo e de *carpet bombing*, buscando entender suas características e como os ataques multiprotocolo se comparam a ataques que usam um único protocolo.

2.5 CONSIDERAÇÕES DO CAPÍTULO

Ataques DDoS têm sido um problema crescente na Internet ao longo dos anos. Ataques DDoS por reflexão oferecem algumas vantagens aos atacantes, como amplificação do tráfego e maior dificuldade de localização da origem de um ataque devido ao uso de intermediários. A variedade de protocolos que podem ser usados em ataques DRDoS e a ampla disponibilidade de refletores abertos na Internet ajudam a explicar o uso frequente dessa técnica de ataque. Embora existam diversos trabalhos sobre caracterização de tráfego DRDoS, características de ataques mais recentes, como o uso de múltiplos protocolos e de *carpet bombing*, não são discutidas na literatura.

Este trabalho propõe investigar ataques DRDoS multiprotocolo e de *carpet bombing* usando para isso um *honeypot*, uma ferramenta útil para compreender o funcionamento de ataques e acompanhar a evolução das técnicas usadas pelos atacantes. O próximo capítulo descreve o HReflector, um *honeypot* projetado para observação e coleta de tráfego DRDoS.

3 HREFLECTOR, UM HONEYPOT PARA OBSERVAÇÃO DE ATAQUES DRDOS

Para a avaliação de ataques DRDoS foi desenvolvido um *honeypot* capaz de observar e registrar tráfego envolvendo diversos protocolos. Este capítulo apresenta os requisitos do *honeypot* (Seção 3.1) e descreve sua arquitetura (Seção 3.2).

3.1 REQUISITOS

A análise e caracterização do tráfego de ataques DRDoS pressupõe que se tenha acesso a tráfego dessa natureza. Seguindo experiências anteriores (KRÄMER et al., 2015; NOROOZIAN et al., 2016; HEINRICH; LONGO; OBELHEIRO, 2017; THOMAS; CLAYTON; BERESFORD, 2017), neste trabalho é usado um *honeypot* para interagir com atacantes e capturar o tráfego de ataque. Esse *honeypot* deve aparentar atuar como um refletor para diversos protocolos, sem no entanto participar efetivamente de ataques DRDoS. Em outras palavras, a ideia é que o *honeypot* receba as requisições enviadas pelos agentes mas envie uma quantidade mínima de respostas, registrando todas as interações.

AmpPots (KRÄMER et al., 2015) poderiam preencher as necessidades deste trabalho, mas seu código não está disponível. Portanto, constatou-se a necessidade de desenvolver um novo *honeypot* que seja voltado especificamente para coleta e análise de tráfego DRDoS e que suporte múltiplos protocolos. Os principais requisitos funcionais para esse *honeypot* são:

- **RF1** – Armazenar todo o tráfego (requisições e respostas) referente aos protocolos suportados pelo *honeypot*;
- **RF2** – Receber requisições de variados protocolos;
- **RF3** – Descartar tráfego gerado por projetos que varrem a Internet em busca de refletores;
- **RF4** – Contabilizar o tráfego recebido, agregando os dados em ataques; e
- **RF5** – Responder de forma convincente a uma fração configurável de requisições por cliente, oferecendo a ilusão de interação com um refletor real.

Os requisitos não funcionais mais importantes dizem respeito a flexibilidade, desempenho e plataforma operacional, e são:

- **RNF1** – Ter facilidade para adicionar, remover, habilitar e desabilitar protocolos no *honeypot*;
- **RNF2** – Realizar o processamento inicial de requisições (descarte, contabilização e decisão de resposta) sem exigir acessos a disco;
- **RNF3** – Evitar a execução de procedimentos internos de manutenção durante a ocorrência de ataques; e
- **RNF4** – Ser implementado em plataforma compatível com Unix.

3.2 ARQUITETURA

A arquitetura do *honeypot* é mostrada na Figura 6. Para satisfazer o RF1, a aplicação cria um subprocesso que executa a ferramenta Tcpdump (GARCIA, 2010) para capturar e armazenar todo o tráfego de/para as portas TCP e UDP referentes aos protocolos suportados pelo *honeypot*. O Tcpdump armazena os dados em formato binário e com acesso sequencial, garantindo assim eficiência de escrita (KLEPPMANN, 2017). Para evitar problemas com arquivos grandes e facilitar a transferência e compressão dos arquivos de captura, o armazenamento é feito em *chunks* de 100 MB, sendo que o próprio Tcpdump se encarrega de gerenciar a rotação de *chunks*. Esses arquivos de captura são comprimidos e oportunamente transferidos para outro sistema onde será efetuada a análise de dados.

Cada protocolo é implementado em um módulo separado, de modo a atender os requisitos RF2 e RNF1. Foi definido um conjunto de funcionalidades que um módulo deve implementar, e a adição e remoção de módulos requer apenas a modificação de um arquivo fonte da aplicação principal.

Existem vários projetos que varrem a Internet em busca de refletores que podem ser usados em ataques DRDoS, como (SHODAN, 2013; SHADOWSERVER, 2004). Em muitos casos, os refletores identificados são reportados a organismos de atendimento e coordenação de incidentes de segurança, como o CERT.br (CERT.BR, 2016) e o CAIS (CAIS, 2018), que notificam os responsáveis para que estes desativem os refletores ou restrinjam o acesso a eles. Para evitar que o *honeypot* seja erroneamente reportado como um refletor aberto, é necessário descartar o tráfego de varredura gerado por esses projetos, como estipula o RF3. Para isso, optou-se por compilar uma lista de endereços IP usados por tais projetos para efetuar as varreduras e bloquear todo o tráfego originado nesses IPs usando um filtro de pacotes (não mostrado na Figura 6).

Para efetuar a contabilização de requisições e a sua agregação em ataques (RF4), considera-se que um ataque DRDoS é formado pelo conjunto de no mínimo

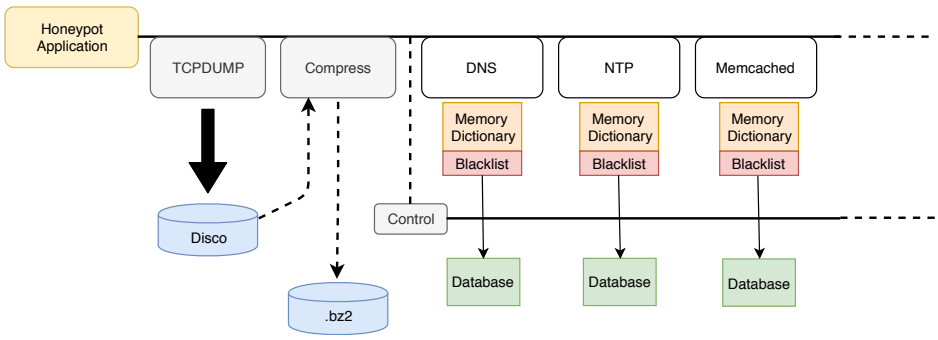

Figura 6 – Arquitetura do *honeypot*

Fonte: Autor.

5 requisições em um intervalo máximo de 60 segundos. Esses parâmetros estão de acordo com as definições apresentadas na Seção 4.2, na página 39.

Para contabilizar os ataques, um módulo mantém uma lista de ataques em andamento, onde cada entrada é formada pelo endereço IP de origem da requisição, um contador de requisições e os *timestamps* da primeira e da última requisições. Se existe na lista um ataque com o mesmo endereço IP de origem e cuja última requisição ocorreu há no máximo 60 segundos, considera-se que a nova requisição pertence a esse ataque, e atualiza-se o contador de requisições e o *timestamp* da última requisição. Caso contrário, cria-se uma nova entrada na lista de ataques em andamento. Para obter eficiência nesse processamento, atendendo ao requisito RNF2, a lista de ataques é implementada usando uma tabela *hash* em memória, representada na Figura 6 como “Memory Dictionary”.

O requisito RF5 determina que um módulo seja capaz de retornar uma resposta coerente a uma requisição, fornecendo um atacante que esteja interagindo com o *honeypot* a ilusão de que este é um refletor real. No entanto, o requisito também exige que o número de respostas por atacante seja limitado, para evitar que o *honeypot* contribua significativamente em ataques DRDoS. Para atender a esse requisito, cada módulo controla o número de requisições recebidas de cada cliente. Quando essa contagem ultrapassa 5 requisições, o endereço IP do cliente é inserido em uma *blacklist*; o limiar de 5 requisições foi estabelecido empiricamente com base no tráfego observado, e pode ser alterado. Ao receber uma requisição, o módulo produz uma resposta apenas se o endereço IP de origem não estiver na *blacklist*. Para satisfazer o requisito RNF2, a lista de requisições por cliente e a *blacklist* também são implementadas usando tabelas *hash* em memória.

As estruturas de dados em memória passam por uma limpeza periódica a cada 10 minutos, de forma a limitar o consumo de recursos. A lista de ataques pendentes é percorrida, e todos os ataques cuja última requisição ocorreu há mais de 5 minutos

são salvos em um banco de dados e removidos da lista. Do mesmo modo, os endereços inseridos na *blacklist* há mais de 24 h são removidos, assim como os endereços na lista de contagem de requisições por cliente que não receberam tráfego nas últimas 24 h (*timestamps* associados a cada entrada são usados para esse fim). Para atender ao requisito RNF3, a *thread* de controle representada na Figura 6 suspende os procedimentos de limpeza quando o *honeypot* está recebendo ataques. Caso uma limpeza seja interrompida, ela só será retomada no próximo período (isto é, após 10 minutos). Os períodos de 5 e 10 minutos foram estabelecidos empiricamente, e podem ser ajustados.

Para satisfazer o requisito RNF4, o *honeypot* foi implementado na linguagem Python, e as demais ferramentas usadas (Tcpdump, SQLite, Unbound e memcached) estão disponíveis em diversas variantes de Unix. Assim, embora a versão atual do *honeypot* utilize a plataforma Linux, o sistema não está atrelado a esse sistema operacional, podendo ser facilmente adaptado a outros sistemas Unix-*like*.

A Figura 7 representa o fluxo de processamento de requisições. Uma requisição enviada por um atacante (1) chega ao *honeypot* e é contabilizada (2). O *honeypot* então consulta o endereço IP de origem na *blacklist* para decidir se uma resposta deve ou não ser enviada. Caso negativo, o processamento da requisição encerra (3). Caso afirmativo, o *honeypot* produz uma resposta para a requisição (4), conforme será detalhado no próximo parágrafo. A resposta obtida é então enviada para o cliente, que pode ser uma vítima (no caso de ataque por reflexão) ou o próprio atacante quando este envia *probes* para o *honeypot*. O passo 6 representa a coleta de tráfego com o Tcpdump, o passo 7 a limpeza periódica das tabelas *hash* em memória, com armazenamento persistente dos dados relevantes para análise posterior em um banco de dados, e o passo 8 representa a compressão das informações capturadas pelo Tcpdump.

O tratamento dado às requisições no passo 4 depende do protocolo. A maioria dos protocolos implementados – Chargen, NTP, QOTD, SSDP e Steam – admite respostas fixas, e portanto o próprio módulo sintetiza uma resposta. Por outro lado, DNS e Memcached têm semânticas mais complexas, onde a resposta é dependente do conteúdo da requisição (por exemplo, em uma resolução de nomes usando o DNS a resposta depende inteiramente do nome consultado). Para esses protocolos, as requisições são repassadas para um servidor local para processamento, e a resposta recebida desse servidor é encaminhada para o cliente. Os servidores locais usam apenas a interface de *loopback*, e não interagem diretamente com clientes externos. Os tratamentos dados às requisições seguem o modelo do AmpPot (KRÄMER et al., 2015), que possui modos de emulação (respostas sintéticas) e *proxy* (repasse para servidor local).

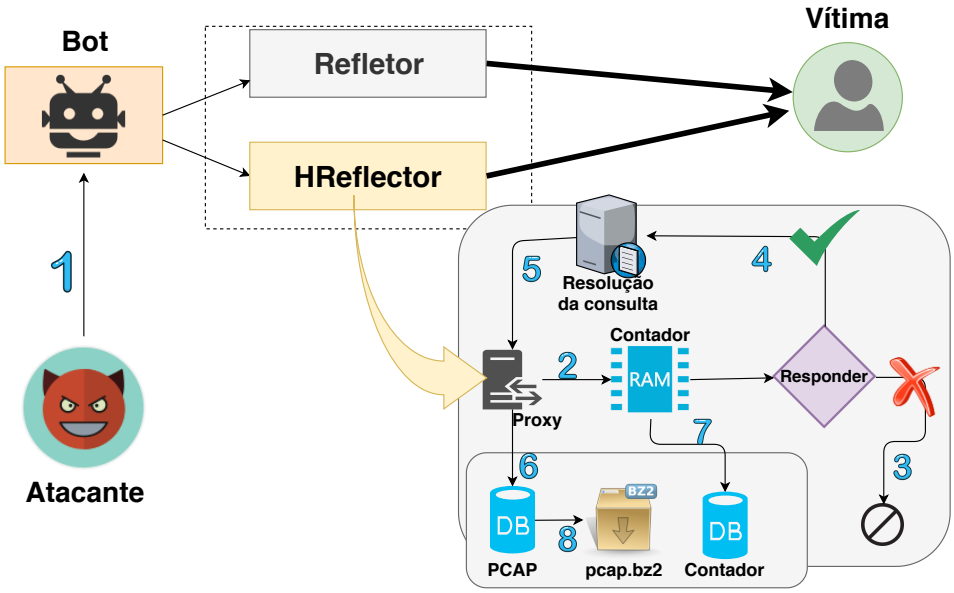

Figura 7 – Fluxo do processamento de requisições no *honeypot*

Fonte: Autor.

3.3 CONSIDERAÇÕES DO CAPÍTULO

A caracterização de ataques DRDoS requer uma ferramenta que permita a coleta do tráfego pertinente. Para esse fim foi desenvolvido o HReflector, um *honeypot* que suporta múltiplos protocolos baseados em UDP. Este capítulo descreveu os requisitos e a arquitetura do *honeypot*.

O próximo capítulo apresenta uma análise de dados coletados com o HReflector ao longo de 255 dias. Durante esse período, o *honeypot* observou mais de 105.7 GB de tráfego, com quase 10 bilhões de requisições e 360 mil ataques DRDoS.

4 ANÁLISE DE DADOS

O HReflector foi implantado na rede da Universidade do Estado de Santa Catarina (UDESC). Este capítulo faz uma análise dos dados coletados pelo *honeypot* durante 255 dias, entre setembro de 2018 e junho de 2019. A Seção 4.1 descreve aspectos operacionais da implantação do HReflector. A Seção 4.2 introduz as definições adotadas na análise. A Seção 4.3 apresenta estatísticas gerais do tráfego coletado. A Seção 4.4 faz uma análise comparativa de ataques DRDoS monoprotocolo e multiprotocolo. A Seção 4.5 examina ataques *carpet bombing*. A Seção 4.6 descreve os *payloads* observados. Por fim, a Seção 4.7 apresenta uma discussão dos resultados.

4.1 IMPLANTAÇÃO

O HReflector foi implantado na rede da UDESC, realizando a coleta de dados 24/7. O sistema possui um endereço IP globalmente roteável e está exposto diretamente à Internet (isto é, não está atrás de um *firewall* ou NAT). As configurações de sistema operacional, *hardware* e *software* da máquina são as seguintes:

- sistema operacional: Slackware Linux (kernel 4.4.14);
- processador: AMD Phenom II X4 B93 (quatro núcleos);
- memória RAM: 4 GB;
- rede: Ethernet 100 Mbps;
- servidor DNS local: Unbound[1];
- servidor Memcached local: memcached[2];
- Python 3;
- SQLite versão 3.13.

Durante a fase inicial de implantação avaliou-se o impacto dos ataques no consumo de recursos do sistema. A maior incidência de tráfego ocorreu em um período de uma hora e meia, no qual houve dois ataques. O sistema recebeu uma média de 737,9 pacotes por minuto, com um mínimo de 435,5 e máximo de 1033,0 pacotes por minuto. Nesse período a utilização de *Central Processing Unit* (CPU) ficou entre 2% e 5%, e a utilização de memória em 7,3%. A utilização de disco ficou entre 3 e 5%,

[1] <https://nlnetlabs.nl/projects/unbound/about/>
[2] <https://www.memcached.org/>

devido à captura de tráfego pelo *Tcpdump*. Portanto, considera-se que o HReflector é capaz de lidar com o tráfego que recebe sem atingir a saturação de seus recursos de *hardware*.

4.2 DEFINIÇÕES ADOTADAS

Um dos princípios de *honeypots* é que, como um *honeypot* não hospeda nenhum serviço oficial, qualquer interação com ele deve ser considerada maliciosa ou, no mínimo, suspeita (SPITZNER, 2003; HOEPERS; STEDING-JESSEN; CHAVES, 2007). No caso do HReflector, o tráfego pode ser dividido basicamente em duas categorias:

1. varreduras (*scans*) em busca de *hosts* e serviços ativos na rede; e
2. ataques DRDoS onde o HReflector está sendo usado como um refletor.

Para seja possível identificar e contabilizar ataques DRDoS, é necessário ter uma definição que permita classificar um conjunto de pacotes recebidos como sendo um ataque. Infelizmente, não existe consenso na literatura sobre essa definição: Krämer et al. (2015), Fachkha, Bou-Harb e Debbabi (2015), Thomas, Clayton e Beresford (2017) e Heinrich, Longo e Obelheiro (2017) usam definições ligeiramente divergentes. Neste trabalho será adotada a definição de Heinrich, Longo e Obelheiro (2017) para ataques DoS explorando o DNS, com uma adaptação mínima (o uso de "vítima" no lugar de "endereço IP de origem") para contemplar ataques de *carpet bombing*:

> **Definição 4.1** (Ataque DRDoS)**.** Um ataque DRDoS consiste em um conjunto com no mínimo 5 requisições com endereço IP de origem referente a uma mesma vítima e com espaçamento máximo de 60 segundos entre requisições consecutivas.

Como um ataque DRDoS pode explorar múltiplos protocolos para realizar a amplificação de tráfego, requisições de diferentes protocolos serão agregadas em um único ataque se forem destinadas à mesma vítima e respeitarem o lapso temporal.

Como ataques DRDoS usam IP *spoofing*, o endereço IP de origem das requisições é o alvo do ataque. A definição de ataque DoS de (HEINRICH; LONGO; OBELHEIRO, 2017) considera que cada endereço IP corresponde a uma vítima distinta, mas ataques de *carpet bombing* são dirigidos contra uma sub-rede, não contra endereços individuais. Descobrir a sub-rede correspondente a um dado endereço IP não é uma tarefa trivial, contudo. Uma possibilidade seria usar dados do WHOIS (ICANN, 2019), que retorna o bloco de endereços *Classless Inter-Domain Routing* (CIDR) a que pertence um endereço IP. Experimentos com esses dados revelaram que os blocos do

WHOIS são muito imprecisos para esse propósito: por exemplo, mais de 12% dos endereços observados pelo *honeypot* estavam associados a blocos CIDR /8 (redes com 16,8 M *hosts*). Esses blocos com muitos endereços são tipicamente de provedores de acesso Internet que não registram no WHOIS como esses endereços são alocados a seus clientes.

A dificuldade de determinar com precisão a sub-rede de um endereço IP aflige também os atacantes, que precisam definir os alvos de seus ataques e frequentemente optam por táticas pouco sofisticadas. Diante disso, optou-se por considerar que todos os endereços IP pertencentes a um mesmo bloco CIDR /24 correspondem a uma única vítima, levando à seguinte definição:

> **Definição 4.2** (Vítima)**.** Uma vítima é constituída pelos três primeiros octetos do endereço IP de origem de um datagrama associado a um ataque DRDoS.

Essa heurística é inevitavelmente imprecisa, podendo juntar ataques separados em um único ataque caso os alvos estejam dentro do mesmo bloco /24. O efeito dessa imprecisão é uma eventual subestimativa de ataques e vítimas, e uma superestimativa do número de requisições por ataque e do número de ataques de *carpet bombing*. Ainda assim, os dados coletados no *honeypot* sugerem uma baixa probabilidade de ocorrência de ataques independentes simultâneos contra alvos no mesmo bloco /24.

Neste capítulo, os ataques DRDoS são analisados segundo dois eixos ortogonais. O primeiro eixo é a quantidade de protocolos por ataque, e o segundo é o número de endereços IP distintos (referentes à mesma vítima) em cada ataque. Esses eixos levam às seguintes definições:

> **Definição 4.3** (Ataque DRDoS Monoprotocolo)**.** Um ataque DRDoS monoprotocolo é um ataque DRDoS no qual é usado apenas um protocolo para gerar amplificação.
>
> **Definição 4.4** (Ataque DRDoS Multiprotocolo)**.** Um ataque DRDoS multiprotocolo é um ataque DRDoS no qual são usados múltiplos protocolos para gerar amplificação.
>
> **Definição 4.5** (Ataque *specific target*)**.** Um ataque *specific target* (ST) é um ataque DRDoS no qual a vítima consiste em um único endereço IP.
>
> **Definição 4.6** (Ataque de *carpet bombing*)**.** Um ataque de *carpet bombing* (CB) é um ataque DRDoS no qual a vítima consiste em mais de um endereço IP na mesma sub-rede.

4.3 ESTATÍSTICAS GERAIS DO TRÁFEGO

A coleta de dados descrita neste capítulo teve início no dia 28/09/2018 e término no dia 09/06/2019, totalizando 255 dias (367.200 minutos). O HReflector não teve *downtime* de mais de um dia, e até o momento nenhuma alteração foi necessária no código da ferramenta. As únicas modificações desde que o *honeypot* entrou em produção foram inclusões de endereços IP na sua *blacklist*.

Durante o período de coleta o HReflector recebeu 105,7 GB de tráfego, contendo um total de 9,99 B de requisições, uma média de 39,1 M de requisições por dia. 97,4% das requisições foram de ataques DRDoS monoprotocolo, e 2,6% de ataques multiprotocolo. Ao todo foram respondidas apenas 0,00019% das requisições recebidas, em decorrência do limite de requisições aplicado no HReflector.

A Tabela 3 apresenta as estatísticas gerais para o tráfego processado pelo HReflector. Observou-se um total de 360 k ataques DRDoS, dos quais 358 k (99,4%) consistem de ataques DRDoS monoprotocolo, 1,9 k (0,5%) de ataques DRDoS multiprotocolo. Os ataques atingiram 35,6 k vítimas distintas; 35,5 k dessas vítimas sofreram ataques monoprotocolo, e 653 sofreram ataques multiprotocolo (a soma é superior ao total porque 541 vítimas sofreram os dois tipos de ataque, e foram contabilizadas em ambas as categorias).

Apenas 6,2% das requisições recebidas fizeram parte de ataques *carpet bombing*. Um total de 14,9 k ataques *carpet bombing* foram identificados, envolvendo 1.170 vítimas (3,2% do total).

Tabela 3 – Estatísticas dos ataques

	# Requisições	%	# Ataques	%	# Vítimas	%
Total	9,991,736,776	100	360,144	100	35,631	–
Monoprotocolo	9,732,966,321	97.4	358,244	99.4	35,519	99.6
Multiprotocolo	258,770,455	2.5	1,900	0.5	653	1.8
Sem CB	9,368,051,916	93.7	345,244	95.8	35,193	98.7
Com CB	623,684,860	6.2	14,900	4.1	1,170	3.2

A Tabela 4 mostra a distribuição de requisições por protocolo. Observa-se uma concentração de 97,9% das requisições em apenas dois protocolos, Chargen e Memcached. Protocolos tradicionalmente apontados como relevantes em termos de tráfego DRDoS (THOMAS; CLAYTON; BERESFORD, 2017; NETSCOUT, 2019), como DNS e NTP, não atingiram 1% do tráfego. A predominância de Chargen, em particular, talvez possa ser explicada pela facilidade de exploração desse protocolo para reflexão, uma vez que um *payload* de 1 byte é suficiente para gerar tráfego amplificado. A alta incidência de Memcached, por sua vez, talvez possa ser explicada pelo elevado fator de amplificação oferecido pelo protocolo: no tráfego observado, Memcached gerou

um fator de amplificação médio de 262. A amplificação dos protocolos e como eles foram explorados serão discutidos em mais detalhes na Seção 4.6.

Tabela 4 – Requisições por Protocolo

Protocolo	Valor	%
Chargen	7,907,367,389	79.1
DNS	86,992,245	0.9
Memcached	1,887,691,357	18.8
NTP	2,279,213	0.0
QOTD	48,210,261	0.5
SSDP	59,195,973	0.6
Steam	338	0.0
Total	9,991,736,776	100.0

A Figura 8 apresenta a evolução temporal do tráfego de ataque recebido no HReflector. A Figura 8(a) mostra o total de requisições, e a Figura 8(b) a distribuição de requisições por protocolo. O volume diário de requisições referentes a ataques DRDoS monoprotocolo é superior ao de requisições de ataques multiprotocolo. Percebe-se, nos últimos dois meses de coleta, um crescimento no volume total de requisições que acompanha o crescimento do tráfego Memcached. Embora ofereçam um alto fator de amplificação (conforme será discutido na Seção 4.6), ataques usando Memcached tornaram-se mais amplamente conhecidos apenas em 2018 (MAJKOWSKI, 2018), o que pode ajudar a explicar o destaque tardio no tráfego coletado pelo *honeypot*.

4.4 ATAQUES *DRDOS* MONOPROTOCOLO E MULTIPROTOCOLO

Esta seção faz uma análise comparativa de ataques DRDoS monoprotocolo e multiprotocolo. A análise desconsidera se os ataques são *carpet bombing* ou não (isso será explorado na Seção 4.5).

4.4.1 Características dos Ataques

As Tabelas 5 e 6 apresentam a distribuição de ataques por protocolo. Os ataques monoprotocolo têm predominância dos protocolos Chargen e Memcached, com 86,4% dos ataques explorando um desses dois protocolos. Nos ataques DRDoS multiprotocolo, 89,7% dos ataques envolvem duas combinações de dois protocolos, Chargen+SSDP (45,8%) e Chargen+DNS (43,9%). No total foram observadas 18 combinações distintas de protocolos. 77,7% dos ataques exploram dois protocolos, 11,1% exploram três protocolos, e 11,2% exploram mais de três protocolos. O número máximo de protocolos observados em um mesmo ataque multiprotocolo foi seis; isso ocorreu em apenas dois ataques.

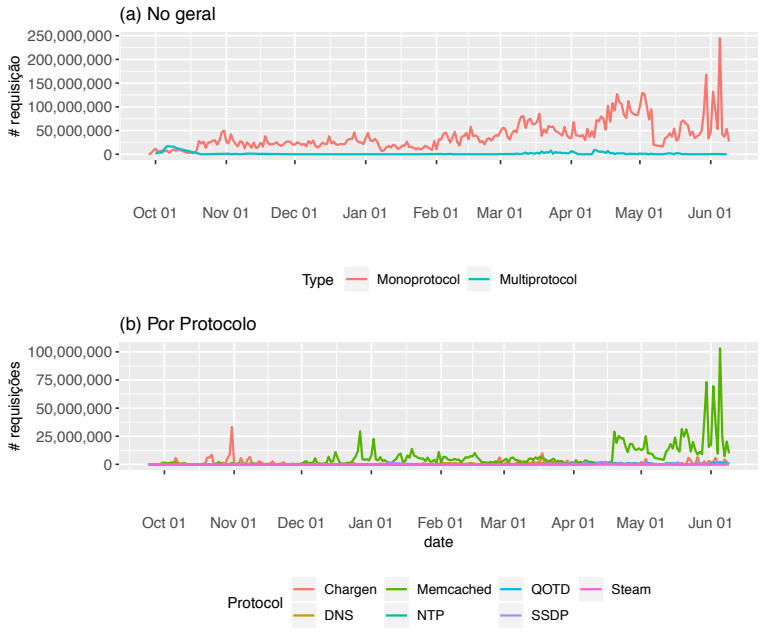

Figura 8 – Número de requisições por dia

Tabela 5 – Distribuição de protocolos por ataque (monoprotocolo)

Protocolo		%
Chargen	166,941	46.6
Memcached	142,581	39.8
DNS	19,703	5.5
SSDP	17,553	4.9
QOTD	9,672	2.7
NTP	1,776	0.4
Steam	18	0.0
Total	358,244	100.0

Tabela 6 – Distribuição de protocolos por ataque (multiprotocolo)

Protocolo		%
Chargen SSDP	870	45.8
Chargen DNS	834	43.9
Memcached Chargen	104	5.5
DNS Memcached	19	1.0
SSDP Memcached	13	0.7
Outros	60	3.1
Total	1900	100.0

As Tabelas 7 e 8 mostram o volume de requisições por protocolo. Em ataques monoprotocolo o Chargen aparece novamente em primeiro lugar, mas com uma proporção de requisições (80,6% do total) muito superior à sua proporção de ataques (46,6%). Essa discrepância indica que os ataques usando Chargen se caracterizam por um grande volume de requisições, possivelmente para compensar seu fator de amplificação não tão elevado. Para ataques DRDoS multiprotocolo, a proporção de requisições é semelhante à de ataques (Tabela 6).

Tabela 7 – Distribuição de requisições por protocolo (monoprotocolo)

Protocolo		%
Chargen	7,853,728,113	80.6
Memcached	1,702,862,445	17.4
DNS	78,681,361	0.8
QOTD	52,667,044	0.5
SSDP	41,308,305	0.4
NTP	3,718,975	0.03
Steam	78	0.0
Total	9,732,966,321	100.0

Tabela 8 – Distribuição de requisições por protocolo (multiprotocolo)

Protocolo		%
Chargen SSDP	123,034,342	47.5
Chargen DNS	107,408,934	45.6
Memcached Chargen	10,715,887	3.9
DNS Memcached	5,450,126	1.3
Memcached SSDP	4,718,562	0.1
Outros	7,442,604	1.6
Total	258,770,455	100.0

A evolução temporal dos ataques DRDoS é apresentada na Figura 9. O gráfico não apresenta nenhuma tendência claramente identificável. A correlação de postos de Spearman entre ataques monoprotocolo e multiprotocolo é muito fraca ($r_s = -0.17, p < 0.0002$), o que indica não haver relação entre o número de ataques de cada tipo. Trinta dias tiveram mais de 2 k ataques. O período de 28 de dezembro até 1 de janeiro apresenta a maior concentração de ataques monoprotocolo; os ataques nesse período tiveram em média 3,2 k requisições e duração de 9,2 minutos. Os ataques DRDoS multiprotocolo não apresentam o mesmo volume diário de ataques dos ataques monoprotocolo: foram em média 1,3 k ataques monoprotocolo e apenas 16 ataques multiprotocolo por dia. O pico de ataques multiprotocolo ocorreu na primeira quinzena de outubro/2018: os ataques tiveram em média 138,6 k requisições e duração de 36,7 minutos. Cabe destacar que esse pico aconteceu no mesmo período do primeiro turno das eleições brasileiras de 2018 (pleito que ocorreu em 7 de outubro), e esses fatos podem estar ligados.

A Figura 10 apresenta as funções de distribuição empírica (FDEs) para a duração dos ataques. A duração é medida como a diferença de tempo entre a primeira e a última requisição em um ataque. Ambos as distribuições (monoprotocolo e multiprotocolo) apresentam assimetria, com caudas longas à direita. Os ataques DRDoS multiprotocolo têm proporcionalmente maior duração do que os ataques monoprotocolo. A duração média observada foi de 552 s (monoprotocolo) e 1.344 s (multiprotocolo), com uma mediana de 302 s (monoprotocolo) e 70 s (multiprotocolo). Ao todo 151 ataques multiprotocolo (8,5%) e 11,9 k ataques monoprotocolo (3,4%) dura-

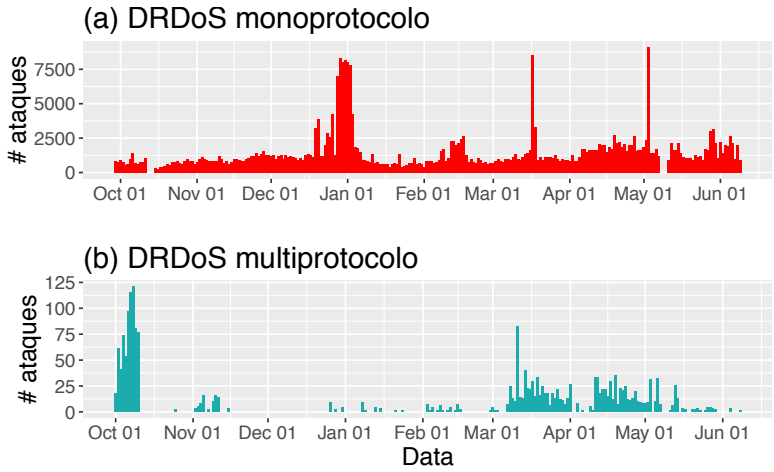

Figura 9 – Evolução temporal dos ataques DRDoS

ram mais do que uma hora. O maior ataque multiprotocolo registrado teve duração de 16 h, enquanto que para ataques monoprotocolo o maior ataque teve duração de 114,2 h (4,8 dias).

A Figura 11 apresenta as FDEs para o número de requisições por ataque. Tem-se novamente distribuições assimétricas com cauda à direita. Os ataques DRDoS multiprotocolo possuem proporcionalmente mais requisições do que os ataques DRDoS monoprotocolo. O número médio de requisições por ataque foi 26,5 k (monoprotocolo) e 140,4 k (multiprotocolo), com uma mediana de 2,3 k (monoprotocolo) e 48,0 k (multiprotocolo). Foram observados 16,5 k ataques monoprotocolo (4,8%) e 613 ataques multiprotocolo (34,5%) com mais de 100 k requisições. O maior ataque monoprotocolo teve 33,1 M requisições, enquanto que o maior ataque multiprotocolo teve 6,4 M requisições. Analisando as Figuras 9, 10 e 11 em conjunto, é possível apontar que os ataques DRDoS multiprotocolo, embora menos frequentes, geralmente têm uma duração mais longa e um maior volume de requisições do que os ataques DRDoS monoprotocolo.

O período em que os ataques são realizados é apresentado nas Figuras 12 e 13, com o fuso horário de Brasília (GMT-3). Para os ataques DRDoS monoprotocolo há uma distribuição dos ataques ao decorrer dos dias e horários, com uma pequena concentração às quartas e quintas, entre 10h e 16h. Ataques DRDoS multiprotocolo têm uma ligeira concentração de ataques entre 1h e 9h. Os ataques multiprotocolo também são um pouco mais frequentes nos finais de semana e na madrugada de segunda-feira. A correlação de postos de Spearman entre ataques monoprotocolo e multiprotocolo por dia e hora é muito fraca ($r_s = 0{,}006, p < 0{,}9$), indicando que não há nenhuma relação discernível entre o número de ataques de cada tipo nos mesmos *slots* de tempo.

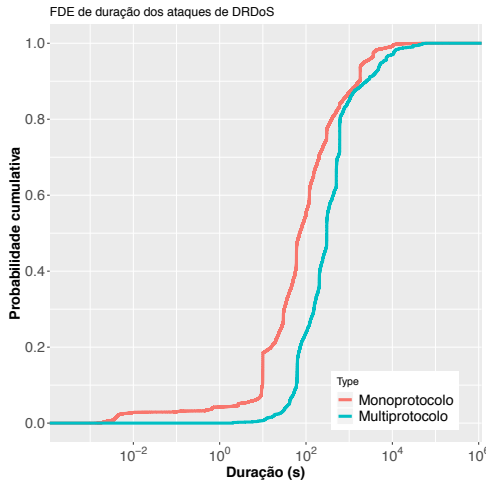

Figura 10 – FDE da duração dos ataques (mono/multiprotocolo) [eixo x em escala log]

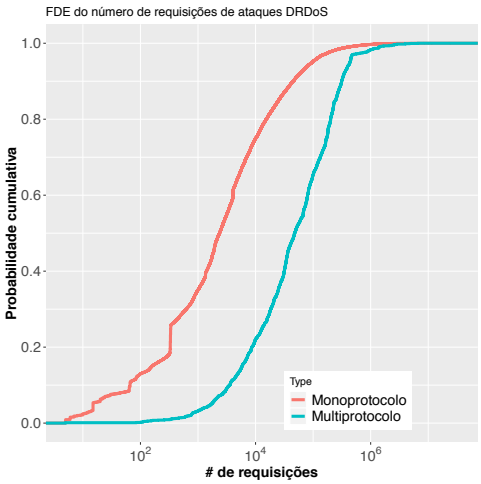

Figura 11 – FDE das requisições por ataque (mono/multiprotocolo) [eixo x em escala log]

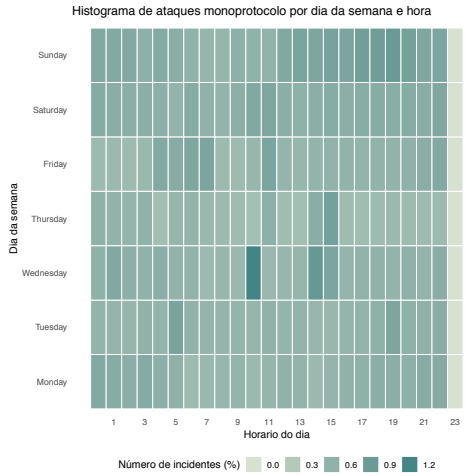

Figura 12 – Incidência de ataques por dia da semana e horário (monoprotocolo)

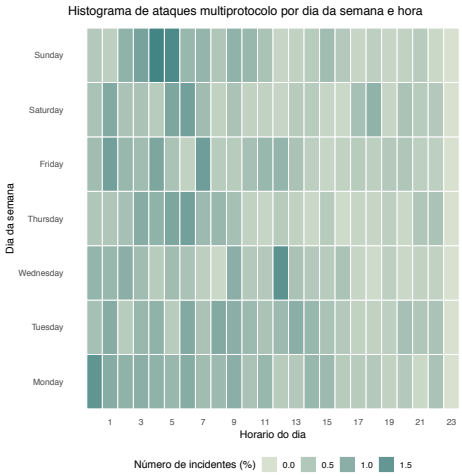

Figura 13 – Incidência de ataques por dia da semana e horário (multiprotocolo)

4.4.2 Avaliação de Vítimas

Ao todo 320 k endereços IP distintos tiveram alguma interação com o HReflector. Destes, 157,6 k endereços foram alvos de ataques DRDoS, tendo sido agregados em 35,6 k vítimas segundo a Definição 4.2 (página 40).

Para efetuar a geolocalização das vítimas, foram usados os dados do WHOIS (ICANN, 2019): uma consulta ao WHOIS por um endereço IP retorna diversos atributos referentes ao bloco de endereços no qual esse IP se insere, dentre os quais o país. Uma limitação inerente a essa abordagem é que organizações que utilizam provedores de nuvem ou redes de distribuição de conteúdo podem usar endereços IP atribuídos a esses provedores e que são identificados no WHOIS como pertencentes a outros países (como o país sede do provedor, por exemplo). A despeito dessa limitação, os dados do WHOIS são os mais fidedignos disponíveis publicamente, não sendo factível, com base apenas nos endereços IP, identificar os que porventura tenham sido classificados de forma errônea.

A Tabela 9 apresenta a distribuição de vítimas por país. Ataques monoprotocolo afetaram vítimas em 193 países, e 49 países receberam ataques multiprotocolo. Estados Unidos (US), China (CN) e Brasil (BR) aparecem entre os cinco países com mais ataques, absorvendo 83,4% dos ataques monoprotocolo e 96,1% dos ataques multiprotocolo. Em ambos *rankings*, o país com mais ataques aparece bem à frente do segundo colocado. A correlação de postos de Spearman para a incidência de ataques monoprotocolo e multiprotocolo (considerando apenas países com pelo menos um ataque de cada tipo) é muito forte ($r_s = 0{,}99, p < 0{,}001$), o que sugere que a incidência de ataques dos dois tipos é praticamente a mesma.

Tabela 9 – Distribuição de ataques DRDoS por países

Monoprotocolo	%	Multiprotocolo	%
US	63.3	BR	45.2
BR	18.0	CN	26.6
HK	9.2	US	24.3
CH	2.7	FR	1.6
CN	2.1	CA	0.4
Outros	4.7	Outros	1.9

A Tabela 10 apresenta os cinco *Autonomous System Number* (ASN) com mais vítimas de ataques DRDoS. Em termos de ASNs, os ataques monoprotocolo estão mais concentrados (apenas dois ASNs receberam 54,1% dos ataques) do que os ataques multiprotocolo, em que os cinco ASNs com mais ataques respondem por apenas 39,8% do total. Os top 3 para ambos os tipos de ataques – ASNs 7922 (*Comcast Cable Communications*, 53667 (*Frantech Solutions*) e 28653 (*Wireless Internet*) – são os mesmos (em ordens diferentes), recebendo 64,5% dos ataques monoprotocolo e

28,2% dos ataques multiprotocolo. Quase todos os ASNs listados na tabela pertencem a provedores de serviços de Internet, com exceção do ASN 263251 (*Alibaba Cloud Computing*), que é um provedor de conteúdo, e do ASN 53667, que é de uma empresa que oferece serviços de proteção contra ataques DDoS.

Tabela 10 – Top cinco ASN por vítimas

Monoprotocolo			Multiprotocolo		
ASN	País	%	ASN	País	%
7,922	US	35.7	53,667	US	11.4
53,667	US	18.4	28,653	BR	10.0
28,653	BR	10.4	7,922	US	6.8
134,548	SC	9.2	37,963	CN	6.1
42,570	CH	2.8	263,251	BR	5.5
Outros	–	23.5	Outros	–	60.2

As Figuras 14 e 15 mostram gráficos da média de requisições por ataque *versus* o número de ataques por vítima. As vítimas que sofreram menos ataques receberam as maiores quantidades de requisições, e parece não haver relação significativa entre as variáveis. De fato, o coeficiente de correlação de postos de Spearman para requisições médias por ataque *versus* ataques por vítima é moderada em ataques monoprotocolo ($r_s = 0{,}40, p < 0{,}001$), e fraca em ataques multiprotocolo ($r_s = 0{,}20, p < 0{,}3$), o que confirma a ausência de relação entre essas duas características.

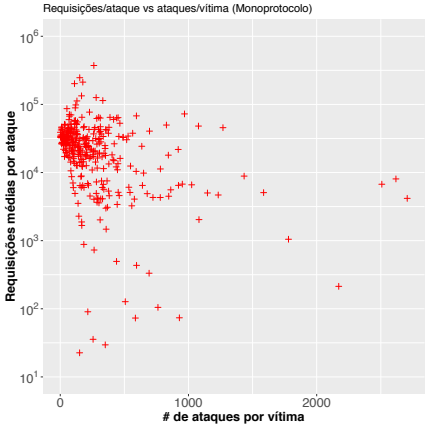

Figura 14 – Requisições/ataque vs ataques/vítima (monoprotocolo) [eixo y em escala log]

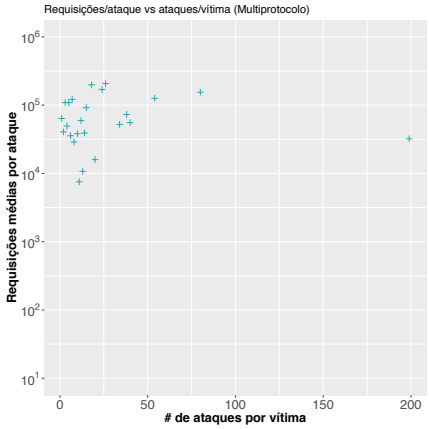

Figura 15 – Requisições/ataque vs ataques/vítima (multiprotocolo) [eixo y em escala log]

4.5 AVALIAÇÃO DE ATAQUES *CARPET BOMBING*

Esta seção faz uma análise comparativa de ataques *Carpet Bombing* (CB) e *Specific Target* (ST), segundo as definições da Seção 4.2 (página 40).

4.5.1 Características dos Ataques

Conforme mostrado anteriormente na Tabela 3 (página 41), foram observados 14,9 k ataques CB, envolvendo 623,7 M requisições e afetando 1,2 k vítimas. 98,5% dos ataques CB foram monoprotocolo, e apenas 1,5% foram multiprotocolo.

As Tabelas 11 e 12 apresentam a distribuição de ataques por protocolo. Chargen e Memcached aparecem entre os três primeiros nos dois rankings, somando 86,0% dos ataques ST e 34,3% dos ataques CB. A diferença mais notável entre os dois tipos de ataque é que SSDP, usado em menos de 5% dos ataques ST, é o protocolo mais comum em ataques CB, sendo usado em 60,0% dos ataques.

Tabela 11 – Distribuição de ataques por protocolo (ST)

Protocolo		%
Chargen	160,355	46.4
Memcached	136,843	39.6
DNS	18,959	5.4
SSDP	16,863	4.8
QOTD	9,476	2.7
Outros	2,748	1.1
Total	345,244	100.0

Tabela 12 – Distribuição de ataques por protocolo (CB)

Protocolo		%
SSDP	8,953	60.0
Chargen	3,379	22.6
Memcached	1,754	11.7
DNS	455	3.0
NTP	101	0.6
Outros	258	2.1
Total	14,900	100.0

As Tabelas 13 e 14 mostram as distribuições de requisições por protocolo. Memcached e Chargen ocupam o topo em ambos os *rankings* (com posições invertidas), respondendo por 96,6% das requisições em ataques ST e 97,2% em ataques CB. Há um contraste notável entre a distribuição de requisições e a de ataques: ataques CB que exploraram o SSDP (protocolo usado em 60,0% dos ataques) possuem um volume baixo de requisições (menos de 178 requisições por ataque, em média) quando comparados aos ataques CB com Memcached e Chargen, que atingem médias de 288,5 k e 30,0 k requisições por ataque, respectivamente.

Tabela 13 – Distribuição de requisições por protocolo (ST)

Protocolo		%
Chargen	746,917,945	79.6
Memcached	159,543,380	17.0
DNS	12,541,718	1.2
SSDP	5,922,064	0.6
QOTD	4,684,026	0.5
Outros	7,196,058	1.1
Total	9,368,051,91	100.0

Tabela 14 – Distribuição de requisições por protocolo (CB)

Protocolo		%
Memcached	506,044,875	81.0
Chargen	101,464,934	16.2
DNS	2,912,144	0.4
QOTD	2,685,142	0.4
SSDP	1,591,444	0.3
Outros	8,986,321	1.7
Total	623,684,860	100.0

A Figura 16 mostra a evolução temporal de ataques CB e ataques ST. Ataques ST são distribuídos de forma irregular, e apresentam os mesmos picos já discutidos na Seção 4.4.1; no total 123 dias tiveram pelo menos 1.000 ataques. Na Figura 16(a)

destaca-se um pico com 4,2 k ataques em um único dia. O que ocorreu neste dia foram 84 ataques contra 31 blocos CIDR com tamanhos entre /19 e /23, pertencentes a sete ASNs distintos em seis países (25 dos 31 blocos pertencem ao ASN 53667, que provê serviços anti-DDoS); esses ataques foram imprecisamente contabilizados como ataques distintos (um por bloco /24) de acordo com as Definições 4.1 e 4.2. A correlação de postos de Spearman entre o número de ataques CB e ST por dia ($r_s = 0{,}04, p < 0{,}4$) revela que não há correlação entre os ataques.

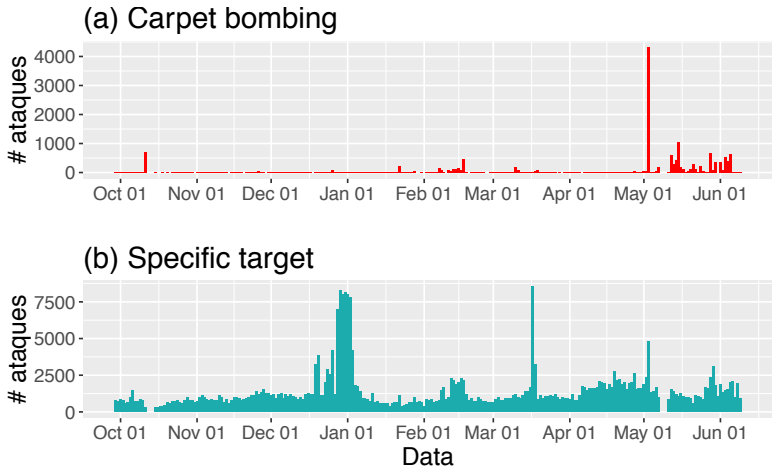

Figura 16 – Evolução temporal dos ataques CB e ST

As funções de distribuição empírica (FDEs) para a duração dos ataques são apresentadas na Figura 17. As distribuições são assimétricas, com caudas à direita, e razoavelmente similares. Os ataques CB têm um tempo médio de duração de 9,2 minutos, já ataques ST têm uma duração média de 27,7 minutos, com medianas de 92 s (CB) e 71 s (ST) . O maior ataque CB registrado teve duração de 89,3 h (3,7 dias) e 114,2 h (4,8 dias) para ataques ST.

A Figura 18 mostra as FDEs para o número de requisições por ataque. As distribuições são assimétricas, com caudas à direita. As medianas são de 199 (CB) e 2,3 k (ST) requisições por ataque. O maior ataque CB teve 27,0 M requisições, enquanto que o maior ataque ST teve 33,1 M requisições. A distância entre as curvas indica que ataques CB têm proporcionalmente menos requisições por ataque do que os ataques ST; isso é reflexo da alta incidência de ataques usando SSDP e contendo poucas requisições (Tabelas 11 e 13).

A avaliação dos incidentes por dia da semana é apresentado nas Figuras 19 e 20, com o fuso horário de Brasília (GMT-3). Os ataques CB têm maior frequência no período da manhã, principalmente na sexta-feira entre as 4 h e 6 h. Os ataques ST estão distribuídos ao decorrer do dia. A correlação de postos de Spearman entre

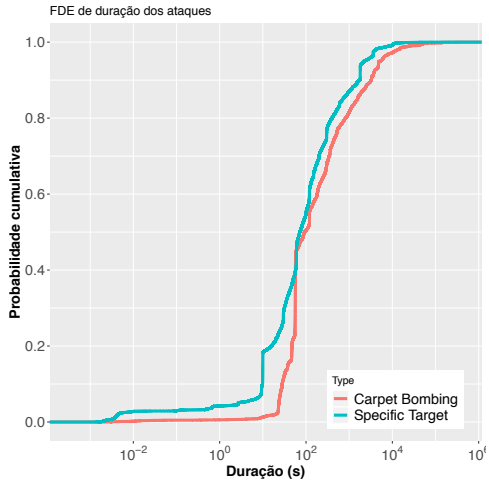

Figura 17 – FDE da duração dos ataques (CB/ST) [eixo x em escala log]

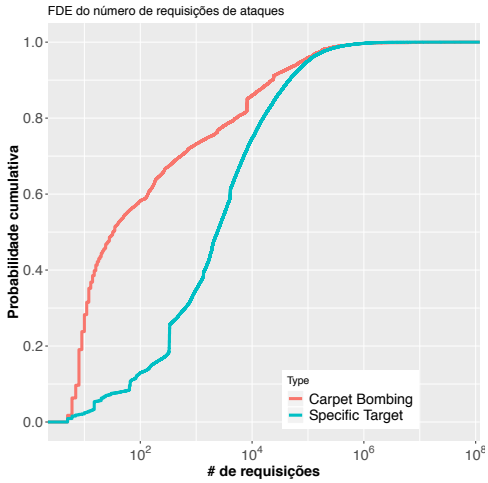

Figura 18 – FDE das requisições por ataque (CB/ST) [eixo x em escala log]

ataques ST e CB por dia/hora é fraca ($r_s = -0.22, p < 0.003$), o que reforça a conclusão de que não existe uma relação entre os períodos de ataques dos dois tipos.

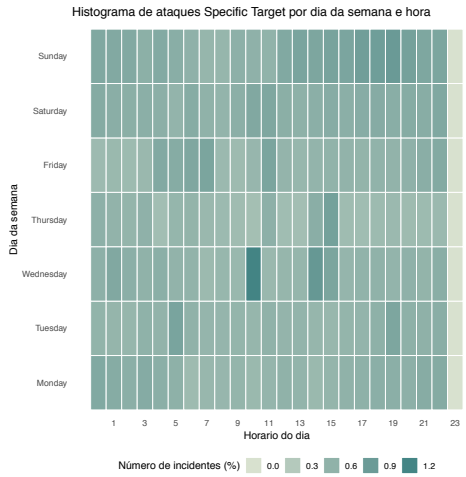

Figura 19 – Incidência de ataques por dia da semana e horário (ST)

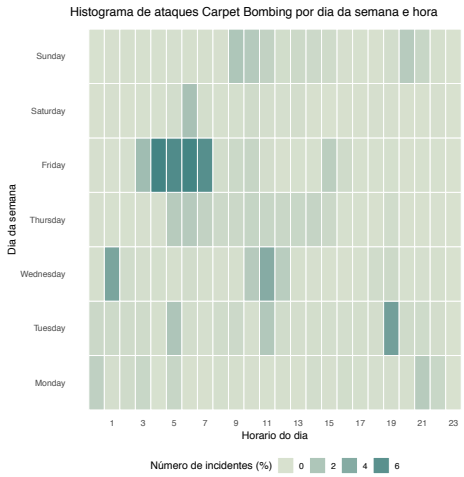

Figura 20 – Incidência de ataques por dia da semana e horário (CB)

Com relação à anatomia dos ataques, a Figura 21 ilustra um tipo particular de ataque CB. Ele foi chamado de ataque com antecedentes, pois o ataque contra múltiplos endereços IP de uma sub-rede ocorre depois de alguns dias em que são observados ataques a um único endereço IP da sub-rede em cada dia. Esses ataques são considerados os antecedentes do CB porque, embora os endereços IP variem, as características desses ataques – protocolo (Chargen e Memcached), duração, número de requisições – são parecidas entre si. No tráfego coletado pelo HReflector, 12,3% dos

ataques CB observados tiveram antecedentes. Os ataques antecedentes tiveram em média 271 segundos de duração e 10,4 k requisições por ataque, enquanto os ataques finais tiveram em média 284 segundos de duração e 11,9 k requisições por endereço IP da sub-rede.

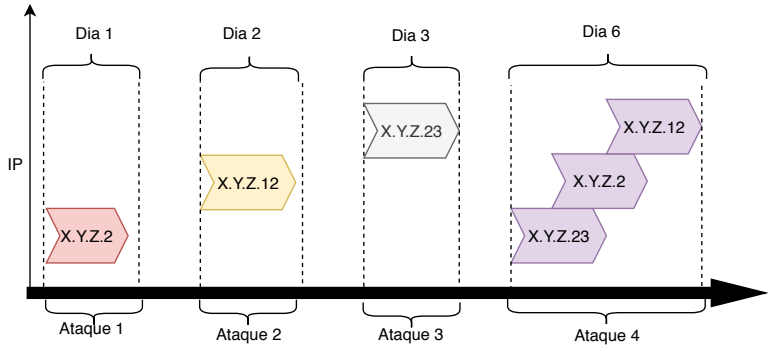

Figura 21 – Ataques CB com antecedentes

Fonte: Autor.

4.5.2 Avaliação de Vítimas

A Tabela 15 apresenta a distribuição de ataques ST e CB por país. Brasil e Estados Unidos assumem a liderança em ambos os *rankings*, somando 79,8% dos ataques ST e 93,4% dos ataques CB. Cabe destacar que, pela localização do HReflector, um número elevado de ataques no Brasil já era esperado. A correlação de postos de Spearman para o número de ataques por país (considerando apenas países com pelo menos um ataque de cada tipo) é muito forte ($r_s = 0{,}99, p < 0{,}001$), o que sugere que a incidência dos dois tipos de ataque é praticamente a mesma.

Tabela 15 – Distribuição de ataques DRDoS por países

Specific Target (ST)	%	*Carpet Bombing* (CB)	%
US	62.9	US	66.6
BR	16.9	BR	26.8
HK	10.3	CZ	4.1
CH	3.1	MK	1.0
CN	2.4	NL	0.3
Outros	4.4	Outros	1.2

A Tabela 16 apresenta os cinco ASNs com mais vítimas de ataques DRDoS. Para ambos os tipos esses cinco ASNs concentram pelo menos 78% das vítimas, e o ASN com mais vítimas está bem distante do que vem em segundo lugar (no caso de ataques CB, mais de 50% das vítimas estão em um único ASN). Quase todos os ASNs são provedores de serviços de Internet, à exceção de 53667 (provedor anti-DDoS).

Tabela 16 – Top cinco ASN por vítimas

Specific Target (ST)			*Carpet Bombing* (CB)		
ASN	País	%	ASN	País	%
7,922	US	40.0	53,667	US	55.3
53,667	US	13.9	28,331	BR	7.4
28,653	BR	11.2	28,241	BR	6.3
134,548	SC	10.3	6,315	US	5.0
42,570	CH	3.1	197,013	CZ	4.0
Outros	–	21.5	Outros	–	22.0

As Figuras 22 e 23 mostram a média de requisições por ataque *versus* o número de ataques por vítima. Para os dois tipos de ataques, os ataques mais intensos afetaram vítimas que receberam poucos ataques. Foram registrados em média 12 ataques CB e 9 ataques ST por vítima. A correlação de postos de Spearman entre as variáveis é forte para ataques ST ($r_s = 0{,}60, p < 0{,}001$) e fraca para ataques CB ($r_s = 0{,}37, p < 0{,}001$), o que indica que a probabilidade de que vítimas que recebem mais ataques sofram ataques mais intensos é maior para ataques ST do que para ataques CB.

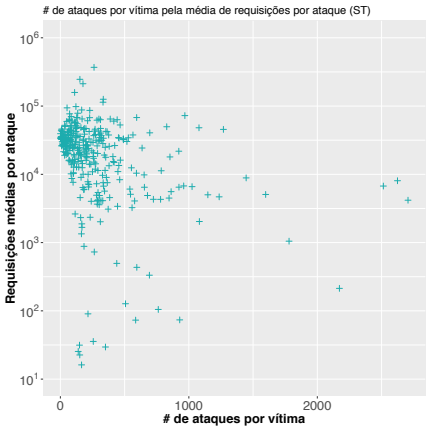

Figura 22 – Requisições/ataque vs ataques/vítima (ST) [eixo y em escala log]

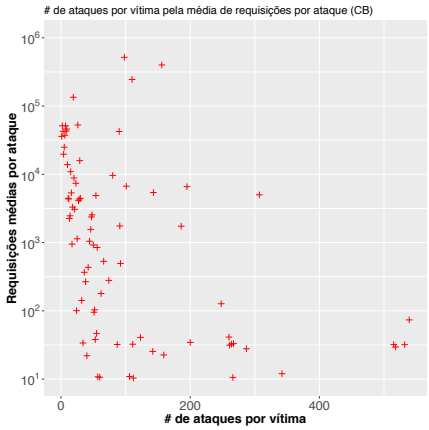

Figura 23 – Requisições/ataque vs ataques/vítima (CB) [eixo y em escala log]

Em termos de anatomia de ataques, as Figuras 24 e 25 esquematizam duas variantes típicas observadas no HReflector. A diferença entre elas é se os múltiplos endereços IP da sub-rede vítima são usados concomitantemente (Figura 24) ou de forma consecutiva (Figura 25), não necessariamente em sequência numérica.

Ao considerar a fração da sub-rede que foi usada em cada ataque *carpet bombing*, é possível identificar que 2,3% dos ataques monoprotocolo e 45,4% dos ataques multiprotocolo exploraram mais de 50% dos endereços do bloco /24. 96,4% dos ataques monoprotocolo e 49,0% dos ataques multiprotocolo tiveram cobertura de 30%

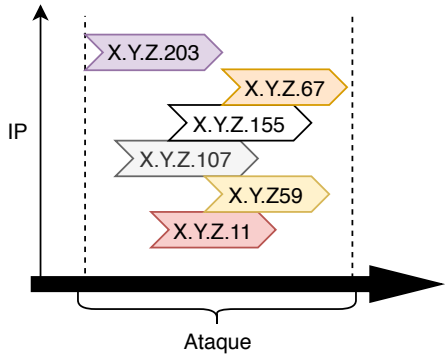

Figura 24 – *Carpet bombing* com endereços IP concomitantes

Fonte: Autor.

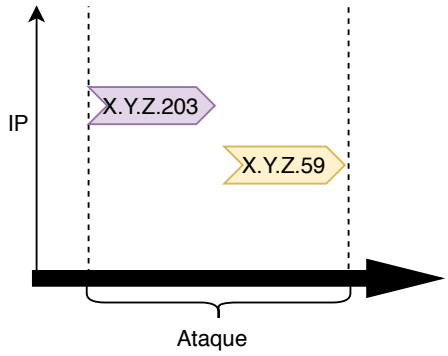

Figura 25 – *Carpet bombing* com endereços IP consecutivos

Fonte: Autor.

ou menos da sub-rede. Uma hipótese para a exploração relativamente baixa das sub-redes é o fato do *honeypot* constituir apenas um refletor, sendo possível que outros refletores tenham coberto outras porções dos blocos de endereços IP.

4.6 AVALIAÇÃO DOS *PAYLOADS*

A avaliação de *payloads* consiste na análise do conteúdo das requisições enviadas pelos atacantes, buscando uma melhor compreensão de como os ataques são realizados e a identificação de eventuais padrões no tráfego. Os protocolos implementados no HReflector apresentam diferentes características no que diz respeito à amplificação obtida:

1. Para Chargen e QOTD, é gerada uma resposta padrão/aleatória independente da requisição recebida pela aplicação. Então, quanto menor a requisição enviada, maior o fator de amplificação, e menos recursos despendidos pelo atacante;
2. Para DNS, NTP, SSDP e Steam, a requisição enviada pelo atacante tem direta influência no fator de amplificação que será obtido, mas o atacante tem controle limitado sobre o resultado produzido; e
3. Para Memcached, o atacante tem um controle maior sobre o resultado gerado e, consequentemente, sobre o fator de amplificação alcançado.

A Figura 26 apresenta a amplificação média mensurada para cada protocolo no HReflector (Steam foi desconsiderado devido ao baixo volume de tráfego observado). O protocolo com maior amplificação foi de longe Memcached, com 262×, enquanto SSDP veio em segundo lugar, com 97×. Chargen e QOTD, que retornam respostas fixas, obtiveram fatores de amplificação semelhantes (90 e 78, respectivamente),

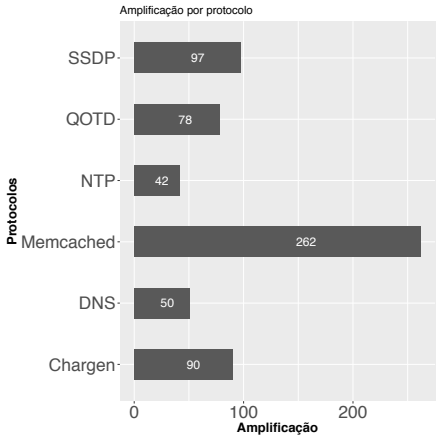

Figura 26 – Fator médio de amplificação por protocolo

que são superiores ao de protocolos que teoricamente oferecem mais flexibilidade para o atacante, como DNS e NTP, com fatores de amplificação de 50 e 42. Comparando com os fatores de amplificação reportados por Rossow (2014), os valores observados são superiores para DNS e SSDP e inferiores para Chargen, NTP e QOTD (Memcached não foi incluído naquele estudo). O fator de amplificação do DNS foi inferior aos reportados em (HEINRICH; LONGO; OBELHEIRO, 2017), que encontrou amplificações médias de 96,3 e 74,1 nos dois conjuntos de dados descritos (a amplificação do DNS será retomada na análise dos *payloads* do protocolo).

Comparando com a popularidade dos protocolos (por exemplo, Tabelas 5 e 6, página 43), percebe-se que os protocolos que aparecem com mais frequência, Memcached e Chargen, estão entre os maiores fatores de amplificação. Mesmo o fator mínimo de 42, obtido com o NTP, ainda oferece uma amplificação considerável para um atacante.

Para os protocolos cujas respostas não dependem do conteúdo das requisições (Chargen e QOTD), os atacantes podem maximizar o fator de amplificação reduzindo ao mínimo o tamanho do *payload*. No tráfego observado, as consultas recebidas para o QOTD não possuem mais que dois bytes, e 99,1% delas têm apenas um byte. Para o Chargen a situação é ainda mais extrema, pois 100,0% das consultas têm apenas um byte. Esse byte é uma letra do alfabeto, aparentemente aleatória (todas as letras aparecem com aproximadamente a mesma frequência).

Os protocolos cujo fator de amplificação depende do *payload* são DNS, NTP, SSDP e Steam. Começando pelo mais simples, as requisições TCP e UDP recebidas pela Steam têm a finalidade de autenticar com o RCON, para realizar interações com o servidor e buscar informações da aplicação. As tentativas observadas no HReflector estão limitadas na busca de uma aplicação (serviço de jogo), ao qual possibilite a

amplificação de tráfego.

As consultas do SSDP são bastante focadas em amplificação de tráfego: 99,9% das requisições foram buscas por dispositivos utilizando `M-SEARCH`, conforme descrito na Seção 2.2.3 (página 27). As consultas que não consistiram deste tráfego são consultas mal formuladas ou tentativas de interações, para as quais nenhuma resposta foi gerada.

O NTP é explorado através do comando `MONLIST`, que retorna uma lista dos últimos 600 *hosts* que interagiram com o serviço (Seção 2.2.3, página 26). O tráfego NTP observado pelo *honeypot* teve muito pouca variação: 99,9999% das requisições foram `MONLIST`, e o restante foram tentativas de interação com o servidor NTP que foram ignoradas pelo HReflector.

No DNS, o fator de amplificação depende do *Resource Record* (RR) especificado na consulta. Um RR é formado por um nome de domínio (QNAME), um tipo (QTYPE) e uma classe (QCLASS), geralmente IN (Internet). Em uma consulta, o QTYPE ANY é usado para retornar todos os RRs com mesmo QNAME, independente de seu QTYPE. As requisições DNS recebidas pelo HReflector contêm 7.534 RRs distintos. A Tabela 17 apresenta os cinco RRs mais populares, que representam 98,5% de todos os RRs. A última coluna apresenta o tamanho máximo de resposta para o RR observado no *honeypot*, que induzem fatores de amplificação entre 7,7 (`067.cz ANY`) e 154,3 (`1x1.cz ANY`); desconsiderando o primeiro, os demais têm um fator médio de amplificação de 95,0.

Chama a atenção que o RR predominante, `067.cz ANY`, presente em quase 72% das requisições, gere um fator de amplificação pequeno (7,7). A explicação é que esse RR foi muito usado em ataques DRDoS no passado (THOMAS; CLAYTON; BERESFORD, 2017), quando chegou a gerar respostas de 6,5 KB[3], que ofereciam uma amplificação de 191×. A hipótese mais provável é que o conteúdo desse domínio tenha sido alterado, reduzindo o tamanho das respostas, mas ainda existam ferramentas de ataque que usam esse RR. Os demais domínios que aparecem na tabela, assim como a versão antiga de `067.cz`, possuem diversos RRs relativos às extensões de segurança do DNS (DNSSEC), cujo potencial para amplificação já foi apontado na literatura (RIJSWIJK-DEIJ; SPEROTTO; PRAS, 2014).

A distribuição de consultas por QTYPE é apresentada na Tabela 18. Foram observados onze tipos distintos (ANY, A, TXT, RRSIG, PTR, SOA, NS, DNSKEY, MX, CNAME, SRV), com 99,8% das consultas com o QTYPE ANY. A ampla predominância de ANY já havia sido observada em outros estudos como (HEINRICH; LONGO; OBELHEIRO, 2017)).

[3] <http://dnsamplificationattacks.blogspot.com/2014/11/domain-067cz.html>

Tabela 17 – Distribuição das consultas observadas

RR	%	Tamanho da resposta
`067.cz ANY`	71,6	268 B
`1x1.cz ANY`	9,2	5,4 KB
`leth.cc ANY`	8,8	4,2 KB
`pnnl.gov ANY`	6,8	2,7 KB
`dfafacts.gov ANY`	2,1	2,9 KB
Outros	1,5	–

Tabela 18 – Tipos (QTYPE) usados nas consultas

QTYPE	%
ANY	99.8
A	0.07
TXT	0.015
RRSIG	0.008
PTR	0.0004
Outros	0.1

O protocolo que oferece a maior flexibilidade para um atacante e, por consequência, o maior fator de amplificação, é o Memcached. Como discutido na Seção 2.2.3 (página 26), o Memcached pode ser explorado de duas formas: (1) solicitando estatísticas do sistema (comando `stats`) e (2) associando um valor a uma chave (`set`) e posteriormente fazendo repetidas consultas por essa chave (`get`).

Foram observados no HReflector 1,1 k *payloads* distintos para Memcached, dos quais 3,1% são variações de `stats` e 91,6% são `set` ou `get`. Os 5,1% restantes consistem em requisições malformadas (requisições HTTP e SSDP que são descartadas pelo *honeypot*) ou limpeza das chaves encontradas em memória (`flush_all`).

O comando `stats` a mensagem retorna uma lista padrão de 1364 bytes, com informações da aplicação como tempo de atividade, versão, bytes lidos e escritos em memoria, dentre outros. Este método corresponde a 5,9% das requisições Memcached processadas pelo HReflector, e gera um fator de amplificação médio de 32,1.

As requisições envolvendo associação e consulta de valores em memória correspondem a 93,6% do tráfego Memcached processado pelo *honeypot*. Quase sempre, um valor é associado a uma chave e, na sequência, essa chave passa a ser consultada repetidamente. Em três ataques, porém, antes do ataque volumétrico por repetição massiva de consultas, o atacante verificava se o valor havia sido efetivamente associado à chave, repetindo a associação caso a verificação falhasse. Houve também ataques em que, após um valor ser associado a uma chave, foram realizadas tentativas de acrescentar mais conteúdo para a chave.

A maior parte (68,4%) dos valores atribuídos às chaves são conteúdo aleatório. Os 31,6% restantes consistem de textos e arquivos *Extensible Markup Language*

(XML). Alguns dos valores não aleatórios contêm informações sobre os atacantes, como nome da organização e apelido do atacante. Em média esses valores têm tamanho de 1,8 KB.

Muitas das chaves usadas em tráfego de ataque tinham características semelhantes. Foram encontrados dois padrões em 86,6% das chaves, indicando que são atribuídas pelo mesmo conjunto de ferramentas; os 13,4% restantes são *hashes* aleatórios. Uma pequena quantidade de chaves (22, ou 1,9%) não foram adicionadas na memória antes do início do ataque; assim, o atacante enviou consultas em série para o refletor que, em vez de enviar o conteúdo desejado, emitiu uma mensagem de erro para a vítima.

Considerando o conjunto dos *payloads* analisados, é possível identificar um *trade-off* entre facilidade para o atacante e fator de amplificação obtido. Protocolos mais simples, como Chargen e QOTD, não atingem os maiores fatores de amplificação mas são facilmente explorados. Protocolos mais complexos, como DNS e Memcached, podem produzir fatores maiores de amplificação, mas exigem um pouco mais de sofisticação para produzirem o efeito desejado. O caso do RR `067.cz ANY` no DNS é exemplar: a má escolha do RR produz uma amplificação bem menor do que a pretendida. Por outro lado, uma requisição Chargen precisa apenas estar sintaticamente correta para gerar a amplificação desejada. A alta popularidade de Chargen sugere que, para alcançar o volume de tráfego necessário para causar a indisponibilidade da vítima, muitos atacantes optam pela simplicidade e preferem recrutar um maior número de refletores do que depender do maior fator de amplificação oferecido por um protocolo mais complexo.

4.7 DISCUSSÃO DOS RESULTADOS

Com base nas diferentes métricas e aspectos de ataques DRDoS explorados no decorrer deste capítulo, é possível destacar as principais conclusões que podem ser extraídas do conjunto de análises efetuadas:

1. Ataques multiprotocolo e *carpet bombing* representam uma pequena parte dos ataques DRDoS observados pelo HReflector – 0,5% e 4,1% dos ataques, respectivamente – sendo que ataques CB são mais comuns do que ataques multiprotocolo. Apenas 223 ataques (0,06% do total de ataques observados) foram ataques combinando as duas características (multiprotocolo e *carpet bombing*).

2. Ainda não é possível definir se existe ou não uma tendência de crescimento para os ataques multiprotocolo e CB.

3. Foram identificados ataques CB com características bem definidas – ataques com antecedentes, ataques com endereços concomitantes, ataques com endereços consecutivos – que não haviam sido descritas na literatura.

4. Ataques multiprocolo e CB tipicamente possuem maior volume de requisições do que ataques monoprotocolo e ST: a fração de *requisições* multiprotocolo/CB é maior do que a fração de *ataques* multiprotocolo/CB. Isso significa que esses novos tipos de ataque tendem a gerar um maior impacto do que os tipos mais tradicionais.

5. Chargen e Memcached foram os protocolos mais usados, tanto em número de ataques quanto em número de requisições. Eles possuem tendências inversas: o uso de Chargen caiu ao longo do período de observação, e o de Memcached subiu. SSDP e DNS são os protocolos mais usados em conjunto com esses dois em ataques multiprotocolo. SSDP também é frequentemente usado em ataques CB, embora com baixo volume de requisições.

6. Estados Unidos, Brasil e China são os países que sofreram maior incidência de ataques de todos os tipos. A presença do Brasil provavelmente foi influenciada pela localização do *honeypot*, e os outros dois países tradicionalmente encabeçam listas de alvos de ataques.

7. A análise dos *payloads* revela que todos os protocolos oferecem fatores de amplificação importantes, e que existe um aparente *trade-off* entre protocolos simples, que oferecem menos amplificação com menor chance de erros, e protocolos mais complexos, que podem alcançar maior amplificação mas têm maior chance de erro.

Por fim, é importante reconhecer as limitações do presente estudo. A principal delas é que o HReflector oferece um único ponto de observação, e portanto uma visão restrita do tráfego de ataque DRDoS. Dispor de um conjunto maior de *honeypots* permitiria ampliar essa visão e correlacionar dados coletados em diferentes pontos da rede. Outro ponto é que as definições de ataques e vítimas introduzidas na Seção 4.2, que são absolutamente necessárias para a classificação do tráfego, foram estabelecidas de forma empírica, e estão sujeitas a imprecisões. Quanto a isso, destaca-se que inexiste consenso na literatura sobre a definição de um ataque DRDoS, e que as definições de vítimas existentes não levam em consideração a ocorrência de ataques *carpet bombing*.

4.8 CONSIDERAÇÕES DO CAPÍTULO

Este capítulo apresentou uma análise de dados de tráfego DRDoS coletados durante 255 dias usando o HReflector. Foram caracterizados e comparados ataques monoprotocolo e multiprotocolo, assim como ataques *specific target* e *carpet bombing*. Também foram avaliados os protocolos usados nos ataques e os *payloads* empregados pelos atacantes, assim como a distribuição de vítimas dos diferentes tipos de ataques.

A conclusão geral da análise é que as novas estratégias de ataques DRDoS – ataques multiprotocolo e *carpet bombing* –, embora ainda representem uma pequena fração dos ataques, mostram-se potencialmente mais perigosos do que os ataques DRDoS tradicionais. A identificação de alguns padrões de ataques *carpet bombing* pode contribuir para a definição de novas heurísticas de detecção e mitigação desses ataques.

5 CONCLUSÃO

Ataques distribuídos de negação de serviço por reflexão (DRDoS) são uma ameaça significativa na Internet. A facilidade de realização de ataques, a amplificação de tráfego que pode ser obtida, a disponibilidade de refletores abertos que podem ser explorados nos ataques, e a dificuldade de identificação dos seus autores são fatores que concorrem para que eles continuem acontecendo. A sua ampla utilização apresenta um impacto em decorrência do volume de dados gerado pelos refletores, provocando indisponibilidade de serviços e prejudicando tráfego de usuários legítimos.

A compreensão dos ataques DRDoS permite a identificação de métodos explorados pelos atacantes e identificação de características dos ataques, o que permite o desenvolvimento de técnicas de detecção e mitigação dos ataques. Avaliando os estudos realizados na literatura que abordam ataques DRDoS, é possível apontar um escopo não abordado para (1) ataques DRDoS multiprotocolo, que exploram múltiplos protocolos de forma simultânea, e (2) ataques *carpet bombing*, nos quais o tráfego de ataque é direcionado para uma sub-rede em vez de um único endereço IP.

Desta forma, o objetivo desta dissertação consistia na análise e caracterização de ataques DRDoS multiprotocolo e *carpet bombing*, comparando-os a ataques mais tradicionais. Para atingir esse objetivo, foi projetado e implementado o HReflector, um *honeypot* que possibilita aos atacantes a utilização de múltiplos protocolos para a amplificação do tráfego. Os protocolos suportados pelo *honeypot* são Chargen, DNS, Memcached, NTP, QOTD, SSDP e Steam. O HReflector foi implantado na rede da UDESC e realizou a coleta de dados em um período de 255 dias, durante o qual foram observadas quase 10 bilhões de requisições. A base analisada foi distribuída de duas maneiras diferentes, buscando avaliar (1) ataques monoprotocolo e multiprotocolo, e (2) ataques *Specific Target* (ST) e *Carpet Bombing* (CB).

A análise dos dados revelou que ataques DRDoS multiprotocolo e *carpet bombing* possuem potencial ofensivo significativo, mesmo que ainda representem pequenas frações dos ataques recebidos. Isso se justifica pelo maior volume de requisições desses ataques em relação aos ataques monoprotocolo e ST. Com relação aos protocolos, os mais usados foram Chargen e Memcached, este com expressivo fator médio de amplificação (262×). Em ataques multiprotocolo, esses protocolos aparecem em conjunto com DNS e SSDP. A descrição de diferentes padrões de ataques *carpet bombing* pode auxiliar na concepção de estratégias de detecção e mitigação para esses ataques.

A continuação desta pesquisa pode se dar em diversas frentes. Uma delas é justamente investigar estratégias de detecção e mitigação para ataques *carpet bombing*, partindo dos padrões de ataques identificados nesta dissertação (ataques com antecedentes, ataques com endereços IP concomitantes/consecutivos). Uma segunda frente é dar prosseguimento à análise realizada neste trabalho, alargando o período de observação com vistas a identificar tendências e novas características de ataques. A terceira frente seria expandir o conjunto de *honeypots*, criando uma infraestrutura distribuída com instâncias do HReflector em múltiplas redes, de modo a aumentar a quantidade de tráfego DRDoS observado e permitir a correlação de ataques entre os vários *honeypots*. Por fim, pode-se ainda mencionar a ampliação do conjunto de protocolos suportados pelo HReflector, incorporando especialmente protocolos de adoção recente na Internet cujo uso em ataques DRDoS não esteja ainda disseminado.

REFERÊNCIAS

AKAMAI. **Threat Advisory: Trivial File Transfer Protocol (TFTP) Reflection DDoS**. 2015. <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/trivial-file-transfer-protocol-reflection-ddos-threat-advisory.pdf>.

AKAMAI. **Akamai [state of the Internet]**. [S.l.], 2016. Threat Advisory: RIPv1 Reflection DDoS.

ANAGNOSTOPOULOS, M. et al. DNS amplification attack revisited. **Computers & Security**, Elsevier, v. 39, p. 475–485, 2013.

ARTEAGA, J.; MEJIA, W. **CLDAP Reflection DDoS**. 2017. <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/cldap-threat-advisory.pdf>.

BAIA, K. Analysis and prevention of memcache udp reflection amplification attack. International Journal of Science, v. 5, 2018.

BECKETT, D.; SEZER, S. Http/2 tsunami: Investigating http/2 proxy amplification ddos attacks. In: IEEE. **Emerging Security Technologies (EST), 2017 Seventh International Conference on**. [S.l.], 2017. p. 128–133.

BIENKOWSKI, T.; ARBOR, N. **No Sooner Did the Ink Dry: 1.7Tbps DDoS Attack Makes History**. 2018. CERT-EU Security Whitepaper 17-003, <https://www.netscout.com/news/blog/security-17tbps-ddos-attack-makes-history> visited in November 2018.

BITAG. Report, **SNMP Reflected Amplification DDoS Attack Mitigation**. 2015. A Near-Uniform Agreement Report.

BREWSTER, T. **Cyber Attacks Strike Zimbabweans Around Controversial Election**. 2013. <https://www.silicon.co.uk/workspace/zimbabwe-election-cyber-attacks-123938?inf_by=5bdcee79671db805298b4e9b> visited in November 2018.

CAIS. **Centro de Atendimento a Incidentes de Segurança**. 2018. <http://www.cais.rnp.br/> visited in September 2018.

CASE, J. **A Simple Network Management Protocol (SNMP)**. [S.l.], 1990. <https://tools.ietf.org/html/rfc1157>.

CERT. **Alert (TA14-017A) UDP-Based Amplification Attacks**. 2018. <https://www.us-cert.gov/ncas/alerts/TA14-017A> visited in November 2018.

CERT.BR. **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)**. 2016. Disponível em <http://www.cert.br/docs/whitepapers/ddos/>.

CERT/CC. **Smurf IP Denial-of-Service Attacks**. [S.l.], 1998. <http://www.cert.org/advisories/CA-1998-01.html>.

CERT/TCC. **Advisory CA-1999-14 Multiple Vulnerabilities in BIND**. 1999. <https://www-uxsup.csx.cam.ac.uk/pub/webmirrors/www.cert.org/advisories/CA-1999-14.html> visited in November 2018.

CHOI, S.-J.; KWAK, J. A study on reduction of DDoS amplification attacks in the UDP-based CLDAP protocol. In: IEEE. **Computer Applications and Information Processing Technology (CAIPT), 2017 4th International Conference on**. [S.l.], 2017. p. 1–4.

CORNELL. **Fraud and related activity in connection with computers**. 1984. <https://www.law.cornell.edu/uscode/text/18/1030> visited in November 2018.

COX, J. **The History of DDoS Attacks as a Tool of Protest**. 2014. <https://motherboard.vice.com/en_us/article/d734pm/history-of-the-ddos-attack> visited in November 2018.

CZYZ, J. et al. Taming the 800 pound gorilla: The rise and decline of ntp ddos attacks. In: ACM. **Proceedings of the 2014 Conference on Internet Measurement Conference**. [S.l.], 2014. p. 435–448.

DDOSMON. **Insight into Global DDoS Threat Landscape**. 2018. <https://ddosmon.net/insight/> visited in November 2018.

DEKA, R. K.; BHATTACHARYYA, D. K.; KALITA, J. K. Ddos attacks: Tools, mitigation approaches, and probable impact on private cloud environment. **arXiv preprint arXiv:1710.08628**, 2017.

DENNIS, D. **Perhaps the First Denial-of-Service Attack?** 2010. <http://www.platohistory.org/blog/2010/02/perhaps-the-first-denial-of-service-attack.html> visited in November 2018.

FACHKHA, C.; BOU-HARB, E.; DEBBABI, M. Inferring distributed reflection denial of service attacks from darknet. **Computer Communications**, v. 62, p. 59–71, 2015.

GARCIA, L. M. **tcpdump & libpcap**. 2010. <https://www.tcpdump.org/> visited in November 2018.

GOLAND, Y. Y. et al. **Simple Service Discovery Protocol/1.0 Operating without an Arbiter**. 1999. <https://tools.ietf.org/html/draft-cai-ssdp-v1-03> visited in November 2018.

GOLDLUST, S. **A Quick Introduction to Response Rate Limiting**. 2018. <https://kb.isc.org/docs/aa-01000>.

HALPERN, J. **RIPv1 Applicability Statement for Historic Status**. [S.l.], 1996. <https://tools.ietf.org/html/rfc1923>.

HEDRICK, C. **Routing Information Protocol**. [S.l.], 1988. <https://tools.ietf.org/html/rfc1058>.

HEINRICH, T.; LONGO, F. S.; OBELHEIRO, R. R. Experiências com um honeypot DNS: Caracterização e evolução do tráfego malicioso. Joinville, Novembro de 2017. XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg).

HOEPERS, C. **Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos**. 2016. <https://www.cert.br/docs/whitepapers/dns-recursivo-aberto/>.

HOEPERS, C.; STEDING-JESSEN, K.; CHAVES, M. **Honeypots e Honeynets: Definições e Aplicações**. 2007. <http://www.cert.br/docs/whitepapers/honeypots-honeynets/>.

ICANN. **About WHOIS**. 2019. <https://whois.icann.org/en/about-whois/>.

KARAMI, M.; PARK, Y.; MCCOY, D. Stress testing the booters: Understanding and undermining the business of ddos services. In: INTERNATIONAL WORLD WIDE WEB CONFERENCES STEERING COMMITTEE. **Proceedings of the 25th International Conference on World Wide Web**. [S.l.], 2016. p. 1033–1043.

KESSLER, G. C. Denial-of-service attacks. In: BOSWORTH, S.; KABAY, M. E.; WHYNE, E. (Ed.). **Computer Security Handbook, 6th Ed**. John Wiley & Sons, Inc., 2012. cap. 18. Disponível em: <https://doi.org/10.1002/9781118851678>.

KHANDELWAL, S. **World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices**. 2016. <https://thehackernews.com/2016/09/ddos-attack-iot.html> visited in September 2018.

KLEPPMANN, M. **Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems**. first. [S.l.]: O'Reilly Media, 2017. v. 1. 624pgs.

KRÄMER, L. et al. Amppot: Monitoring and defending against amplification ddos attacks. In: SPRINGER. **International Workshop on Recent Advances in Intrusion Detection**. [S.l.], 2015. p. 615–636.

KÜHRER, M. et al. Exit from hell? reducing the impact of amplification ddos attacks. In: **USENIX Security Symposium**. [S.l.: s.n.], 2014. p. 111–125.

KÜHRER, M. et al. Hell of a handshake: Abusing tcp for reflective amplification ddos attacks. In: **WOOT**. [S.l.: s.n.], 2014.

KUMAR, S. Smurf-based distributed denial of service (ddos) attack amplification in internet. In: IEEE. **Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on**. [S.l.], 2007. p. 25–25.

LEMOS, R. **How DDoS Attacks Techniques Have Evolved Over Past 20 Years**. 2016. <http://www.eweek.com/security/how-ddos-attacks-techniques-have-evolved-over-past-20-years> visited in November 2018.

LIU, C. et al. Detect the reflection amplification attack based on udp protocol. In: IEEE. **Communications and Networking in China (ChinaCom), 2015 10th International Conference on**. [S.l.], 2015. p. 260–265.

LOPES, W. R. **Ataques DDoS Panorama, Mitigação e Evolução**. 2015. <ftp://ftp.registro.br/pub/gter/gter39/08-AtaquesDdosPanoramaMitigacaoEvolucao.pdf> visited in November 2018.

MAJKOWSKI, M. **Stupidly Simple DDoS Protocol (SSDP) generates 100 Gbps DDoS**. 2017. <https://blog.cloudflare.com/ssdp-100gbps/>.

MAJKOWSKI, M. **Memcrashed – Major Amplification Attacks from UDP Port 11211**. 2018. <https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/>.

MANSFIELD-DEVINE, S. The growth and evolution of ddos. **Network Security**, Elsevier Science Publishers B. V., Amsterdam, The Netherlands, The Netherlands, v. 2015, n. 10, p. 13–20, out. 2015. ISSN 1353-4858. Disponível em: <http://dx.doi.org/10.1016/S1353-4858(15)30092-1>.

MANSFIELD-DEVINE, S. Ddos goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare. **Network Security**, v. 2016, n. 11, p. 7 – 13, 2016. ISSN 1353-4858. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1353485816301040>.

MCAULEY, C. **Following the Crumbs-Deconstructing the CLDAP DDoS Reflection Attack**. 2016. <https://www.ixiacom.com/company/blog/following-crumbs-deconstructing-cldap-ddos-reflection-attack>.

MEITEI, I. L.; SINGH, K. J.; DE, T. Detection of ddos dns amplification attack using classification algorithm. In: ACM. **Proceedings of the International Conference on Informatics and Analytics**. [S.l.], 2016. p. 81.

MEMCACHED. **Memcached**. 2019. <https://memcached.org> visited in November 2018.

MIRKOVIC, J.; REIHER, P. A taxonomy of DDoS attack and DDoS defense mechanisms. **ACM SIGCOMM Computer Communication Review**, v. 34, n. 2, p. 39–53, abr. 2004.

MOCKAPETRIS, P. **DOMAIN NAMES - CONCEPTS AND FACILITIES**. [S.l.], 1987. <https://tools.ietf.org/html/rfc1034>.

MOCKAPETRIS, P. **DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION**. [S.l.], 1987. <https://tools.ietf.org/html/rfc1035>.

NAZARIO, J. DDoS attack evolution. Elsevier, v. 2008, n. 7, p. 7–10, 2008. Network Security.

NETSCOUT. **Dawn of the Terrorbit Era**. [S.l.], 2019. <https://www.netscout.com/>.

NETSCOUT; ARBOR. **Insight into the Global Threat Landscape**. 2017. Netscout Arbor's 13th Annual Worldwide Infrastructure Security Report.

NEWMAN, L. H. **GITHUB Survived the Biggest DDoS Attack Ever Recorded**. 2018. <https://www.wired.com/story/github-ddos-memcached/> visited in September 2018.

NIST. **CVE-1999-1379 Detail**. 1999. <https://nvd.nist.gov/vuln/detail/CVE-1999-1379> visited in November 2018.

NOLLA, A. **Amplification DDoS attacks with game servers**. 2013. <http://grehack.org/files/2013/talks/talk_3_5-nolla-ddos_amplification_attacks_with_game_servers-grehack.pdf> visited in November 2018.

NOROOZIAN, A. et al. Who gets the boot? analyzing victimization by ddos-as-a-service. In: SPRINGER. **International Symposium on Research in Attacks, Intrusions, and Defenses**. [S.l.], 2016. p. 368–389.

PAXSON, V. An analysis of using reflectors for distributed denial-of-service attacks. **ACM SIGCOMM Computer Communication Review**, ACM, v. 31, n. 3, p. 38–47, 2001.

POSTEL, J. **Character Generator Protocol**. 1983. <https://tools.ietf.org/html/rfc864> visited in November 2018.

POSTEL, J. **Quote of the Day Protocol**. 1983. <https://tools.ietf.org/html/rfc865> visited in November 2018.

PRINCE, M. **The DDoS That Almost Broke the Internet**. 2013. <https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/> visited in November 2018.

PRINCE, M. **Technical Details Behind a 400Gbps NTP Amplification DDoS Attack**. 2014. <https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/> visited in November 2018.

PROLEXIC. **An Analysis of DrDoS SNMP/NTP/CHARGEN Reflection Attacks**. 2012. Part II of the DrDoS White Paper Series.

PROLEXIC. **Distributed Reflection Denial of Service (DRDoS) Attacks An Introduction to the DrDoS White Paper Series**. 2013. <https://news.asis.io/sites/default/files/Distributed_Reflection_DoS_Attacks_White_Paper_A4_031513.pdf> visited in November 2018.

REVUELTO, V.; MEINTANIS, S.; SOCHA, K. **DDoS Overview and Response Guide**. 2017. CERT-EU Security Whitepaper 17-003, <https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf> visited in November 2018.

RIJSWIJK-DEIJ, R. van; SPEROTTO, A.; PRAS, A. Dnssec and its potential for ddos attacks: a comprehensive measurement study. In: ACM. **Proceedings of the 2014 Conference on Internet Measurement Conference**. [S.l.], 2014. p. 449–460.

ROSSOW, C. Amplification hell: Revisiting network protocols for ddos abuse. In: **In Proceedings of the 2014 Network and Distributed System Security Symposium, NDSS**. [S.l.: s.n.], 2014.

RUDMAN, L.; IRWIN, B. Characterization and analysis of ntp amplification based ddos attacks. In: IEEE. **Information Security for South Africa (ISSA), 2015**. [S.l.], 2015. p. 1–5.

RYBA, F. J. et al. Amplification and drdos attack defense–a survey and new perspectives. **arXiv preprint arXiv:1505.07892**, 2015.

SANTANNA, J. J. et al. Booters—an analysis of ddos-as-a-service attacks. In: IEEE. **Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on**. [S.l.], 2015. p. 243–251.

SHADOWSERVER. **The Shadowserver Foundation**. 2004. <https://www.shadowserver.org/wiki/pmwiki.php/Main/HomePage> visited in September 2018.

SHARMA, R.; GULERIA, A.; SINGLA, R. Characterizing network flows for detecting dns, ntp, and snmp anomalies. In: **Intelligent Computing and Information and Communication**. [S.l.]: Springer, 2018. p. 327–340.

SHODAN. **The search engine**. 2013. <https://www.shodan.io/> visited in September 2018.

SIEKLIK, B.; MACFARLANE, R.; BUCHANAN, W. J. Evaluation of tftp ddos amplification attack. **Computers & security**, Elsevier, v. 57, p. 67–92, 2016.

SOLLINS, K. **THE TFTP PROTOCOL (REVISION 2)**. [S.l.], 1992. <https://tools.ietf.org/html/rfc1350>.

SPECHT, S. M.; LEE, R. B. Distributed denial of service: Taxonomies of attacks, tools, and countermeasures. In: **ISCA PDCS**. [S.l.: s.n.], 2004. p. 543–550.

SPITZNER, L. Honeypots: Catching the insider threat. In: **Proceedings of the 19th Annual Computer Security Applications Conference**. Washington, DC, USA: IEEE Computer Society, 2003. (ACSAC '03), p. 170–. ISBN 0-7695-2041-3. <http://dl.acm.org/citation.cfm?id=956415.956438>.

THOMAS, D. R.; CLAYTON, R.; BERESFORD, A. R. **1000 days of UDP amplification DDoS attacks**. 2017. 79–84 p. Electronic Crime Research (eCrime), 2017 APWG Symposium on.

TURNER, R. **Tackling the DDoS Threat to Banking in 2014**. 2014.

VALVE. **Master Server Query Protocol**. 2017. <https://developer.valvesoftware.com/wiki/Master_Server_Query_Protocol>.

VALVE. **Steam**. 2019. <https://store.steampowered.com/>.

VYNCKE, E. **Network Time Protocol**. [S.l.], 2019. <https://tools.ietf.org/wg/ntp/>.

WEAGLE, S. **Benefits of Real-Time DDoS Protection**. 2016. <https://www.corero.com/blog/724-benefits-of-real-time-ddos-protection-.html>.

WOODY, C.; SHOEMAKER, D.; MEAD, N. **Foundations for Software Assurance**. 2012. <https://www.us-cert.gov/bsi/articles/knowledge/principles/foundations-software-assurance> visited in November 2018.

YOUNG, A. **Connection-less Lightweight X.500 Directory Access Protocol**. [S.l.], 1995. <https://tools.ietf.org/html/rfc1798>.

ZETTER, K. **Lazy Hacker and Little Worm Set Off Cyberwar Frenzy**. 2009. <https://www.wired.com/2009/07/mydoom/> visited in November 2018.

ZHANG, B.; ZHANG, T.; YU, Z. Ddos detection and prevention based on artificial intelligence techniques. In: IEEE. **Computer and Communications (ICCC), 2017 3rd IEEE International Conference on**. [S.l.], 2017. p. 1276–1280.