Detecção de refletores em ataques DDoS volumétricos

Yan Victor dos Santos[1]

Departamento de Ciência da Computação, Universidade de Brasília

***Abstract*— A estrutura cliente-servidor tem grande importância para o funcionamento da rede mundial de computadores. Sua grande e complexa movimentação faz com que se torne possível a ocorrência de inúmeras ações mal intencionadas. Dentre estas ações, podemos citar o ataque de negação de serviço distribuído. Com a intenção de negar o serviço, o atacante pode causar diversos danos ao servidor e seus clientes. Dentre as principais formas de realizar o ataque de negação de serviço, encontra-se a utilização de refletores por meio a técnica de *spoofing*, que falsifica o endereço de origem para atacar a vítima por meio de um servidor intermediário. Este trabalho tem por objetivo detectar refletores em ataques DDoS volumétricos, ao explorar uma característica de servidores DNS.**

I. INTRODUÇÃO

Com o avanço tecnológico, torna-se importante considerar que o número de usuários e serviços disponibilizados têm crescido cada vez mais na rede. A grande quantidade de serviços desencadeia o desenvolvimento de arquiteturas que estão desprovidas de segurança, uma vez que a implementação segura necessita de um custo que pode ser considerado alto, dependendo da complexidade de sua estrutura. Com a falta de segurança, usuários mal intencionados ganham espaço para colocar em prática seus objetivos.

Dentre os diversos tipos de ataques existentes na rede, é nosso objeto de pesquisa o ataque conhecido como "Ataque de Negação de Serviço", ou *Distribued Denial of Service* (DDoS). Este trabalho foca em ataque volumétrico, pois sua execução torna ainda mais complexo o tratamento do problema. O ataque DDoS, um dos mais recorrentes, é capaz de impedir que o servidor possa prover serviço por um determinado período de tempo, e até que o servidor tenha ciência de que seu serviço está fora do ar, muitos danos podem ocorrer. Por este motivo, torna-se necessário compreender melhor a ameaça com o objeto de resolvê-la, ou pelo menos reduzir seu impacto, para assegurar a confiabilidade e disponibilidade do sistema.

Em geral, este tipo de ameaça gera um grande volume de dados que pode ser detectado analisando o tráfego da rede, sendo possível verificar quais *hosts* estão enviando um grande número de pacotes. Estes *hosts* se tornam potenciais atacantes durante a detecção. Entretanto, existe uma variação do ataque que é caracterizada por gerar volume de dados por meio de um grande número de computadores controlado por um *host* principal, chamados de *BotNets*. Cada máquina envia um número razoável de dados, cuja soma tende a inundar o servidor, dificultando a detecção dos computadores, além de esconder o IP (Internet Protocol) do controlador.

Para este trabalho, vamos considerar métodos existentes para detecção de ataques DDoS volumétricos, considerando a existência (ou não existência) de *botnets* durante um ataque. Uma vez que a detecção já tenha ocorrido, verificamos uma nova configuração de elementos que abre portas para mais uma variação da ameaça, conhecida como ataque por reflexão, cuja principal característica é usar o método de *spoofing* para inundar a vítima de pacotes de respostas de um determinado refletor. Portanto, o foco principal do trabalho será propor uma solução para reduzir o problema de ataques por refletores em DDoS. O algoritmo a ser estudado será objeto de criação de uma ferramenta que permitirá a execução de futuros testes para avaliar o desempenho, identificação de falsos positivos e casos de testes.

O resto do artigo está organizado da seguinte forma. A seção 2 fornece os conceitos e informações necessárias para a compreensão do trabalho. A seção 3 apresenta a apresenta o foco do problema e os efeitos do ataque DDoS. A seção 4 aborda a identificação de ataques DDoS. A seção 5 apresenta a conclusão, seguida da seção 6 que cita os trabalhos futuros.

II. FUNDAMENTAÇÃO TEÓRICA

A. O ATAQUE DE NEGAÇÃO DE SERVIÇO

O ataque de negação de serviço, ou ataque DoS, é um dos principais problemas que ameaçam grandes servidores, e podem ser altamente prejudiciais em termos de custos, política, integridade e privacidade, disponibilidade, entre outros. Sua estrutura tem como principal objetivo inundar a rede do servidor, impedindo que exista a comunicação descrita pela arquitetura cliente-servidor, evitando assim que qualquer serviço, inicialmente disponível, possa ser executado conforme o proposto pelo projeto. Isso quer dizer que o principal objetivo é causar uma negação de serviço por parte da vítima.

Existem diversas formas de negar o serviço de servidores. Para uma boa compreensão do funcionamento de refletores, vale citar o ataque direto entre agentes, caso *fim-a-fim* (atacante e vítima), que envia um grande número de pacotes direto para a rede para tentar inundá-la e impedir que haja comunicação com outros clientes. Uma proposta de detecção para este tipo de ataque é encontrar a vítima por meio de análise de tráfego para encontrar qual *host* está com um

[1]Graduando em Ciência da Computação, Universidade de Brasília.
Email: yanvictor_ds@hotmail.com
Matrícula: 14/0033599

comportamento anormal ao tentar conversar com o servidor. Mas nosso objetivo principal não é propor soluções para este problema em específico.

Uma das variações do ataque direto insere terceiros no caminho com o objetivo de tornar volumétrica a quantidade de volume de dados a serem enviados para o *host* final. Este ataque é conhecido como negação de serviço distribuído, ou DDoS. Este ataque se adapta ao avanço da capacidade do computador de armazenar e processar requisições, necessitando uma quantidade maior de pacotes para gerar negação de serviço. Os computadores, considerados como terceiros, são os chamados *BotNets*, máquinas infectadas pelo atacante e controlados para cumprir o objetivo principal de inundar a rede, além de esconder o endereço IP do principal atacante. Esta característica dificulta a detecção do ataque DDoS seguido do tratamento após a conclusão da identificação do ataque. É trabalhoso identificar máquinas mal-intencinadas, uma vez que elas não precisam enviar um número anormal de pacotes para gerar um grande volume de dados.

Uma vez que o DDoS foi detectado, considerando as dificuldades encontradas, tais como o uso de *BotNets*, vamos explorar o conceito de refletores na próxima subseção com o objetivo de detectar sua existência neste tipo de ataque.

B. ATAQUE POR REFLEXÃO

Dentre as categorias já mencionadas, o ataque pode ocorrer de forma direta ou por amplificação (reflexão). Quando o atacante decide tentar negação de serviço de forma direta, então a rede da vítima é inundada diretamente pelo computador que está sob controle direto do atacante, ou por computadores que estão sendo diretamente controlados pela máquina mestre. De qualquer forma, o endereço dos mesmos estão sendo diretamente expostos no *log* de controle vítima. O ataque por amplificação requer o uso de um servidor intermediário, conhecido como refletor, que é responsável por estourar o *slot* do alvo, que fica impedido de responder a novas solicitações. Na internet existem inúmeros servidores que podem ser caracterizados como vulneráveis a se tornarem refletores, por consequência do seu funcionamento e protocolos utilizados por eles. Devido ao grande número de protocolos, para este trabalho, vamos trabalhar especificamente com protocolo o DNS (Domain Name System) para melhor entender a natureza do ataque, de maneira instanciada.

Para falar de ataque DDoS por reflexão, vamos compreender o funcionamento do servidor DNS, que é muito alvejado para ser refletor em ataques deste tipo. Um servidor DNS contém nomes que apelidam diversos IP's na internet, estes nomes são recuperados de maneira hierárquica, dependendo do seu domínio. Por exemplo, suponha o endereço "www.exemplo.com". O endereço real do servidor, localizado através deste domínio, é uma sequência de números, e não simplemesmente seu apelido correspondente. Entretanto, se todos os sites tivessem de ser acessados por meio desta sequência de números, quase nenhum usuário conseguiria acessá-los devido à dificuldade de decorar estes

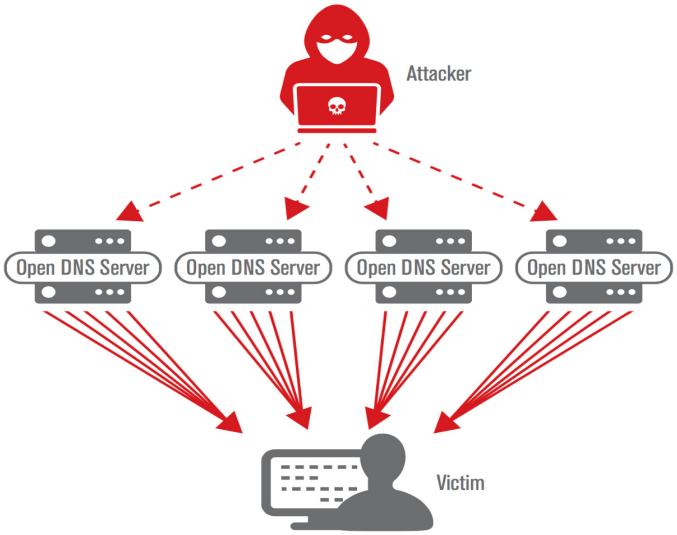

Fig. 1. Ilustração de Ataque por Amplificação [1]

endereços IP's. Para resolver este problema, os servidores DNS guardam os apelidos correspondentes a estes endereços. Portanto, se você deseja acessar "www.exemplo.com", a busca é feita primeiro no servidor DNS, que lhe retornará o enderço IP correspondente ao servidor requerido.

A imensa quantidade de usuários acessando sites em um mesmo momento requer busca quase instantânea por processamento rápido para encontrar o endereço referente ao nome solicitado no servidor DNS. A necessidade da velocidade e grande quantidade de usuários torna inviável o uso de protocolos do tipo TCP/IP, uma vez que sua estrutura requer uma conexão ponta a ponta entre cliente e servidor. No caso UDP, esta conexão não é necessária, tornando rápido o processo de pedido e resposta. Com base nestas informações, podemos destacar que protocolos que trabalham de maneira semelhante se tornam vulneráveis a uma grande quantidade de ataques que o DNS costuma sofrer. Por este motivo, para entendermos melhor a estrutura de um ataque por reflexão, também vamos tornar como parte do nosso objeto de pesquisa um servidor DNS como sendo refletor. Para isto, é necessário entender como funciona o ataque por reflexão.

No ataque por reflexão, utiliza-se a técnica de *spoofing* para alterar o IP de origem, inserindo em seu lugar o IP da vítima. Desta maneira, o atacante pode fazer requisições válidas como se fosse a vítima. É comum em ataques deste tipo o abuso do controle de máquinas vulneráveis para a criação de *BotNets*, tornando ainda mais intensa a quantidade de pacotes que indundam a rede da vítima. Neste caso, todos as máquinas da ponta devem estar com seus endereços de origem adulterados para o IP da vítima que se quer atacar. Com apenas um comando vindo da máquina controladora, as máquinas "zumbis"podem, em um mesmo momento para um mesmo recurso, requisitar objetos para um ou mais refletores.

A estrutura do ataque é descrita por uma quantidade massiva de requisições feitas a servidores que utilizam

protocolos favoráveis para o ato que, em nossa pesquisa, focamos no protocolo UDP. O protocolo UDP permite ao servidor receber inúmeras requisições e responder, assim que o recurso estiver disponível, o pedido feito por um cliente. Não há necessidade de *Handshake* de três vias, o que torna a resposta ainda mais rápida. Uma vez que o pedido feito por uma máquina com IP adulterado, será então respondido para a vítima, obtendo assim a característica de ataque por reflexão. Como pode-se observar na Figura 1, os servidores vulneráveis que respondem ao pedido do atacante e enviam a resposta para a vítima são tratados como intermediários no processo, ou melhor, como refletores.

Por mais que os impactos do DDoS por reflexão possam ser grandes, a estrutura de implementação não necessariamente é complexa. Além do mais, a requisição é tratada como válida por parte do refletor, uma vez que não se detecta facilmente adulteração no IP, pelo menos não ainda por parte do servidor de amplificação. A velocidade de resposta e facilidade na implementação permite tornar um grande ataque em uma ferramenta de baixo custo de implementação, sendo esta uma das principais características que atrai a atenção de usuários mal intencionados na rede.

Uma vez que o básico funcionamento do ataque foi mencionado, é compreensível a visualização de um servidor DNS ser bastante alvejado para a reflexão. A rápida resposta de um servidor DNS, juntamente com a facilidade de pedir informações em grande escala e obtenção de respostas maiores que as *queries* feitas, faz com que ele se torne uma classe de servidores propícios para inundar a rede de alguém. A próxima seção apresentará a frequência dos ataques que utilizam DNS para reforçar a necessidade de suporte para mitigação deste problema.

III. DDoS NA VISÃO DO ATACANTE

A. IMPACTOS DO ATAQUE DDoS

O ataque DDoS, como já apresentado, tem dificultado diariamente o serviço de milhões de servidores no mundo. Dentre estes servidores, encontram-se serviços críticos que vão desde atuações em compras e vendas de acessórios online, até controle de acesso em grandes estações metroviárias. Um simples ataque pode gerar consequências catastróficas e desencadear problemas que podem ser fáceis ou complexos de se resolver [7]. É alarmante a situação em que ataques como negação de serviço são fáceis de se implementar, e pode ser feito por qualquer usuário razoavelmente experiente em computação. A prova da facilidade se dá por sua frequente execução, divulgada em diversos lugares da rede. O grande número de ataques requer uma reação urgente e imediata por parte da comunidade de segurança na computação.

Um exemplo da capacidade do ataque é o recente DDoS feito ao GitHub que, dentro de 10 minutos, começou a ter muitos problemas, segundo o site da *wired* [10]. O ataque desfrutou do uso de milhares servidores *memchached*, fazendo com que o GitHub fosse atigindo com aproximadamente 1,35 terabits de pacotes por segundo (ápice), segundo o site. O ataque resultou na negação de serviço que retirou o GitHub do ar por aproximadamente 5 minutos, sem contar o tempo de instabilidade que a aplicação teve. Este acontecimento reforça que não importa se sua aplicação foi construída visando o máximo de segurança contra invsores, se você não puder lidar com 1,35 terabits de uma só vez entrando em sua rede em um segundo, então poderás ter muitos problemas pela frente. E como este problema pode ser reduzido? Bem, uma vez que a falha de segurança não está necessariamente na vítima e sim no refletor, necessita-se investir em mecanismos que identifiquem tráfegos anômalos dentro da sua própria rede. Assim fica exposto se alguém está tentando usar o seu serviço como reflexão para atacar alguém.

Embora haja bastante recurso e ferramentas que auxiliam para evitar o estado de vulnerabilidade de um refletor, ainda assim existem inúmeros serviços na rede que se encontram nesta condição. Infelizmente não se pode esperar até todos estes servidores ficarem seguros, é necessário se proteger do lado da vítima com o que for possível. Uma vez que esta necessidade passa a existir, este trabalho propõe uma forma de reduzir o problema, mitigando ataques DDoS por reflexão no lado da vítima. Assim todos os pontos da rede que estão abertos a sofrerem um ataque refletido por algum servidor como o DNS ou *memcached*, terão formas de identificar o ataque e se defender dele. Para isto, exploramos uma característica dos refletores que usam o protocolo UDP para estruturar a proposta que será descrita nas próximas seções.

B. A ESCOLHA DO DDoS

Como descrito anteriormente, o DDoS é relativamente fácil de ser desenvolvido, se comparado à outras ferramentas de ataque. Se o ataque utilizar refletores, então a quantidade de recursos necessários é ainda mais reduzida. Para verificar a frequência com que o ataque o ocorre, utilizamos como base o site *ddosmon* [3], que disponibiliza dados sobre a ocorrência de ataques considerando o tempo, o local, métodos do DDoS mais frequentes e protocolos mais utilizados para o ataque. Os dados foram disponibiliados se baseando nos últimos três meses.

A Figura 2 apresenta os dez países que mais sofreram com o ataque DDoS no último mês. Como podemos ver, a China lidera como alvo do ataque, ultrapassando os 400k de ataques. Em seguida, podemos observar que os Estados Unidos apresentou também um grande número de alvos, ultrapassando os 300k. Já na terceira posição, se encontra o Brasil, com quase 50k de ataques nos últimos meses, fator alarmante para os servidores que estão localizados aqui no Brasil. Embaixo vemos França e alguns outros países que não ficaram distantes da nossa condição, demonstrando que esse tipo de ataque costuma ocorrer com frequência no mundo inteiro.

Os dados divulgados por [3] demonstram o quanto é estável a ocorrência de DDoS em diversos lugares do mundo, necessitando de ferramentas que torne possível a defesa para estas ocasiões. Tem-se de considerar que um país, como a China, pode ter inúmeros serviços comprometidos pela recorrente instabilidade na disponibilidade dos servidores, o

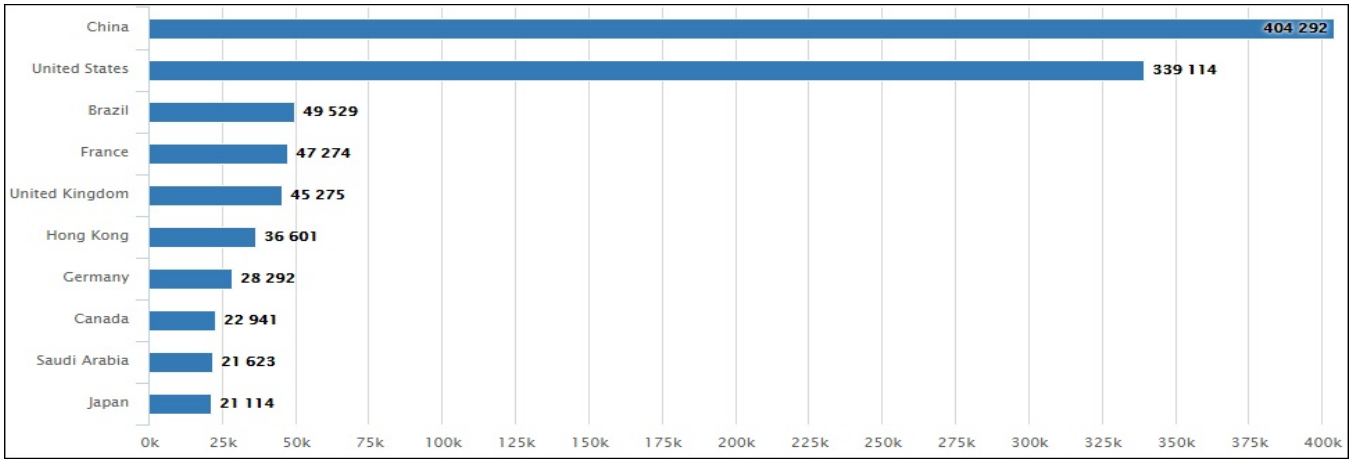

Fig. 2. Os 10 Principais Países Alvos de DDoS [3]

que é bastante preocupante para um país cujos habitantes utilizam e abusam do uso da internet diariamente. Dentre os ataques observados, existem muitas chances de servidores alvos serem de grande importância, uma vez que os ataques normalmente não visam atingir pequenos negócios, e sim para satisfazer algum interesse próprio que pode ser *cybercrime*.

As estatísticas sobre o Brasil reforçam a necessidade de se definir métricas sobre soluções viáveis para este problema. Como já dito anteriormente, é preciso compreender melhor o ataque DDoS, que possui muitas maneiras de se implementar. Uma forma de mitigar é instanciar este problema para um caso específico, como o DDoS volumétrico com uso de refletores, compreender e em seguida propor uma solução para esta instância. Esta continua sendo a principal motivação deste trabalho. Por fim, ainda sobre a Figura 2, precisamos destacar que os números somam mais de um milhão de ataques registrados nos últimos três meses, em cima dos 10 países apresentados. O que podemos notar a respeito desta informação? Precisamos compreender os motivos desta ameaça ser tão visada para atacantes.

C. ATAQUE COM REFLETORES E PROTOCOLOS

Sabemos que o ataque DDoS trabalha muito bem com o uso de refletores, o que motiva o uso constante deles. Para compreendermos melhor a eficácia deste método, vamos analisar os dados divulgados da *ddosmon* mais uma vez sobre os protocolos mais utilizados para tornar um servidor em refletor.

Precisamos lembrar o papel de servidores DNS para a visibilidade no mundo do *cybercrime*. Servidores DNS, por meio do protocolo UDP, não se preocupam em entregar sem problemas em 100% dos casos, o que é característico de serviços que desfrutam do protocolo UDP. A "despreocupação"do protocolo sobre quem estão enviando os pacotes de resposta faz com que este serviço se torne viável para ser usado por alguém com más intenções, e que deseje lotar o *slot* da rede a ponto de negar o serviço desejado. O

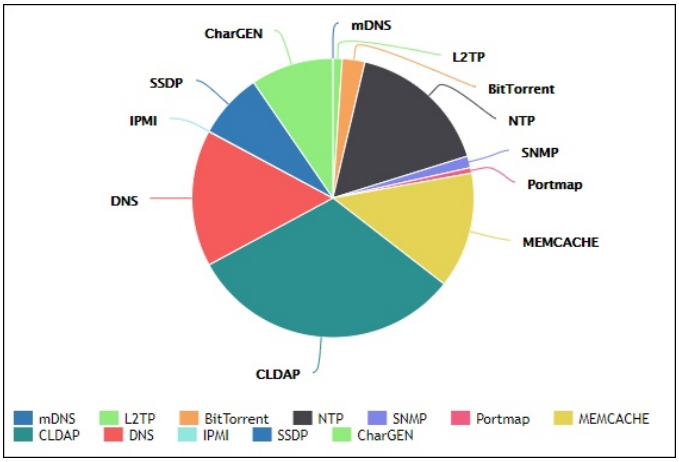

Fig. 3. Frequência de Protocolos Usados Para Reflexão [3]

principal problema deste tipo de serviço é á sua consideração de pacote legítimo para usuários que adulteraram o IP, tornando-o incapaz de detectar que está sendo usado como refletor para atacar. Este é um dos principais problemas de servidores como o DNS. Por este motivo, são constantemente utilizados para ataques DDoS por reflexão, como pode ser visto na Figura 3. Este índice se dá pela facilidade de atacantes se aproveitarem das portas abertas ao ataque, como descrito nas seções anteriores. Este índice incentiva a pesquisa do trabalho iniciando pelo protocolo DNS.

Assim como a frequência sobre os protocolos, podemos verificar que sua relação com o tempo de utilização gera uma tendência do uso dos protocolos, mostrando que a eficácia na proteção pode não ser tão boa quanto se esperava com o avanço da tecnologia. Por este motivo, reforçamos a necessidade de se atentar para ataques DDoS que ocorrem com frequência, com tendência a aumentar, conforme é apresentado no gráfico da Figura 4. Os danos discutidos mostram a recompensa que ataques de baixos esforços

podem ter.

A Figura 4 apresenta as tendências de usos de protocolos para ataques por reflexão. Os dados coletados em 22 de junho de 2018 reforça a alta taxa de uso de servidores DNS. Podemos observar que, por um período de 3 meses, a taxa se manteve praticamente constante, o que leva a concluir que atacantes possuem ciência da eficácia de utilização de servidores DNS para se efetuar um ataque em larga escala por meio de refletores. A ampliação gera ganhos suficientes para convencer que sua estrutura é ótima para um grupo mal intencionado poder economizar com recursos disponíveis. E o ponto mais importante desta análise é de longe a sua tendência constante em um período tão recente.

Para entendermos melhor os dados apresentados nas figuras anteriores, precisamos analisar quais efeitos causam este tipo de resultado. Primeiro, vamos considerar pontos essenciais que levam este tipo de ataque ser tão viável ainda nos dias atuais. Estes pontos são:

- Poucos recursos podem gerar grandes impactos.
- A origem não ataca diretamente a vítima.
- A resposta pode ser bem maior que a requisição.
- A resposta é rápida.
- O tráfego é considerado legítimo pelo lado do refletor.
- Enquanto o ataque é trivial, a detecção e a resposta ao ataque ainda é lenta [6]

Os pontos acima destacam características importantes que reforçam a ocorrência de DDoS por reflexão. Diferentemente do ataque direto, o uso de refletores permite uma "pseudo"camuflagem do atacante, o que permite segurança durante o processo de *spoofing* [5]. Isto quer dizer que o IP que chega no refletor não é o IP real do atacante, e sim o da vítima (adulterado). Consequentemente, o IP que alcança a vítima também não é do atacante, e sim do refletor. A amplificação é o ponto chave deste tipo de ataque, com pequenos pedidos pode-se gerar imensas respostas que irão direto para o servidor da vítima. O planejamento se torna menos trabalhoso com o uso da aplificação. Além de inundar com inúmeros pacotes maiores que as requisições, a processo de resposta é feito rapidamente. Este conjunto de características torna esta variação do DDoS muito atraente.

Segundo a *ddosmon*, este tipo de ataque representa 70% dos registrados. Também como afirmação, "Ataques por reflexão com UDP continuam a liderar nos últimos dias"[3]. Em uma análise sobre a utilização de *memcache* para ataques de negação de serviço por reflexão, pesquisadores da Cloudflare destacaram diversos problemas que permitem a utilização de refletores para este tipo de ataque. "A especificação do UDP mostra ser um dos melhores para amplificação! Há absolutamente zero verificações, e os dados são entregues ao cliente com velocidade máxima! Além disso, o pedido pode ser minúsculo e a resposta enorme", disseram os pesquisadores em [2]. Um bom exemplo sobre a variação de tamanho entre pedido e resposta se encontra em uma *querie* do tipo ANY, que pede ao servidor todos os registros para um *host* específico. Este tipo de *querie* contém um número pequeno de bytes, enquanto o total de registros retornados pelo servidor DNS é grande o suficiente para chamar a atenção de possíveis ameaças.

É indispensável concluírmos que precisamos de soluções ou pelo menos maneiras eficientes de mitigar o problema. Existem diversas ferramentas disponíveis que detectam e tratam um ataque DDoS em tempo real. A próxima seção descreverá como é possível detectar refletores em um ataque DDoS através do tráfego que chega na vítima.

IV. DETECÇÃO DE REFLETORES

Este trabalho tem como proposta a detecção de refletores em ataques DDoS em tempo de execução. Para isto, vamos dividir o processo em duas etapas:

1) Detecção de um ataque DDoS.
2) Detecção de possíveis refletores.

No primeiro item, para que haja a existência de refletores como ameaças reais, primeiro deve-se identificar a ocorrência de tentativa de inundação da rede. Isto quer dizer que primeiro alguém está tentando causar uma negação de serviço. Caso isto ocorra, pode-se tentar identificar qual o método utilizado para tentar o ataque. No segundo item, considerando a existência de um ataque DDoS, focamos em detectar a existência de refletores durante o ataque com um comportamente característico existente neste tipo de ameaça. Uma vez que as duas etapas foram feitas, conseguimos ampliar a defesa no lado do servidor sobre possíveis ataques com refletores, mitigando o problema de servidores DNS alvos em potenciais que ainda não se adaptaram de forma segura ao surgimento de ameaças na internet. Uma vez que estes alvos ainda existem em grande número, seguir os dois passos descritos é uma maneira de proteger a vítima. Portanto, vamos descrever melhor como é feito o processo do item 2, que é o foco do nosso trabalho.

A. IDENTIFICAÇÃO DO ATAQUE DDOS

Para identificarmos um ataque DDoS, existem diversas ferramentas de suporte já implementadas que podemos utilizar para este passo. Portanto, vamos considerar este passo apenas como um auxílio ao projeto principal que é detectar a existência de refletores dentro do DDoS. Qualquer ferramenta eficiente na detecção da negação de serviço garante a possibilidade de integrar o passo 2 a ponto de recebermos mais informações sobre o ataque.

Existem diversas formas de detectarmos um ataque de negação de serviços, dentre elas verifica-se o *log* gerado na rede sobre o tráfego de pacotes que entram e saem. Este monitoramento permite analisar a existência de comportamentos anômalos, tais como excesso de pacotes ou requisições chegando na rede com um mesmo IP de origem. Este tipo de ameaça caracteriza um ataque possivelmente não distribuído, porém a capacidade da máquina de enviar pacotes pode ser muito alta. Não há como ter certeza sobre o paradeiro do atacante, uma vez que o IP pode ser direto da máquina mestre ou de algum computador pertencente à uma *BotNet*. Caso o tipo de pacote não seja uma requisição e sim uma resposta, existe uma possibilidade do IP pertencer a um refletor. Isto será discutido na subseção a seguir.

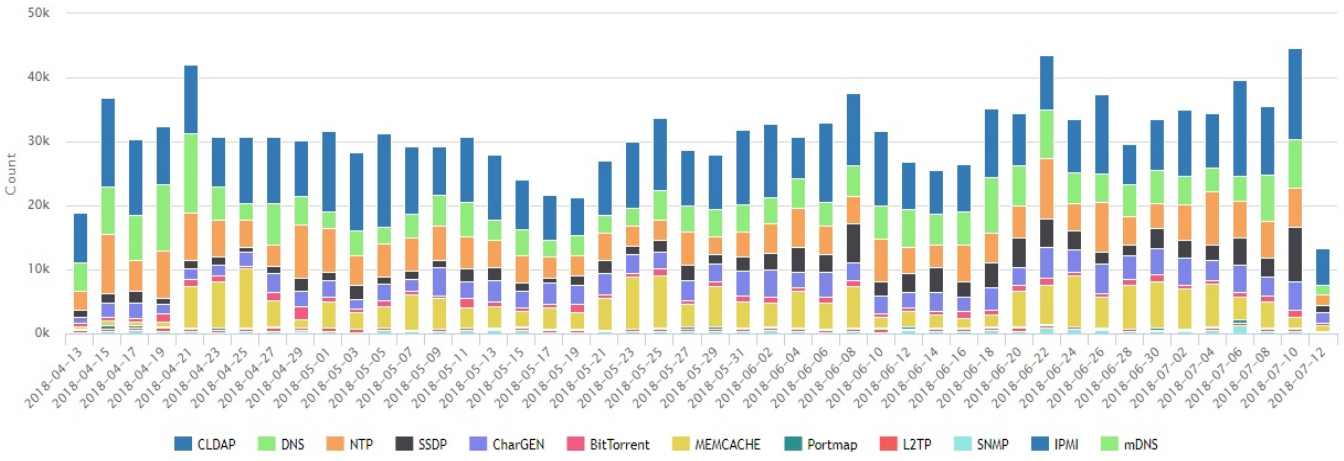

Fig. 4. Tendências de Protocolos Usados Para Reflexão [3]

B. METODOLOGIA, IDENTIFICANDO REFLETORES

Após concluir o passo 1, ou seja, a ameaça foi detectada, precisamos descobrir se os pacotes que estão chegando são de origem de um ou mais refletores. Para isto, vamos compreender o comportamento de um refletor.

Para entendermos melhor, vamos considerar um conjunto D de servidores DNS que está sendo usado por um atacante A para efetuar ataques por reflexão contra uma vítima V. Neste caso, o ataque tem característica de DDoS volumétrico. Entretanto, para que se consiga utilizar um conjunto D para atacar V, é preciso um grupo de máquinas, controladas por um computador mestre de A, que tenham seus respectivos IP's adulterados para V e estejam fazendo requisições legítimas para o conjunto D. Este último então responde volumetricamente para V que logo entra em negação de serviço.

Diante do comportamente do tráfego entre o conjunto D e a vítima V, podemos destacar o grande número de pacotes de resposta chegando até V sem que ele tenha solicitado antes, como apresentado na Figura 1. Este comportamento é característico da técnica de *spoofing*, cujo D acredita que está respondendo para o mesmo cliente que havia pedido anteriormente à resposta. Podemos utilizar tal informação para identificar a existência de refletores durante um ataque.

A detecção será feita por uma ferramenta que escutará o tráfego UDP ou ICMP que passa até V. Com foco em UDP, e como grande parte das arquiteturas de módulos de segurança, o objetivo desta ferramenta é analisar pacotes que entram e saem da rede com o objetivo de tomar alguma atitude pré-programada caso ache necessário. Uma vez identificado o protocolo UDP, deve-se verificar se está partindo de um servidor DNS, SNMP, NTP, etc. Em nosso trabalho, iremos inicialmente analisar os pacotes de um conjunto D, analisando o protocolo e a porta 53 (DNS), além de se basear na possível existência de respostas não requisitadas anteriormente pelo servidor V. Uma vez que este comportamento foi detectado, então os pacotes devem ser dropados para evitar negação de serviço. As informações são guardadas em uma tabela de estados, que guardam a sessão que identifica a comunicação entre a requisição feita e a resposta dada por ambos os lados.

A tabela de estados consiste em guardar informações sobre o tipo do pacote, protocolo utilizado, origem e destino para verificar se existe algum desbalanceamento referente a ele. A verificação é feita incrementando (requisição) ou decrementando (resposta) um contador de controle de acesso que da suporte ao servidor V. Caso V faça um pedido, então o contador é incrementado em 1 para o destino especificado. Caso o V receba uma resposta, então o contador é decrementado em 1 para a origem também especificada. Caso haja um desbalanceamento, ou seja, o contador fique negativo devido a grande quantidade de respostas [8] que estão chegando sem ter requisição pendente na tabela, significa que os pacotes podem estar vindo de um refletor. Vale ressaltar que este caso só deverá ser solidificado caso seja detectado a tentativa de DDoS sobre o serviço de V. O acesso eficiente à tabela deve garantir um controle preciso sobre o tráfego, sendo fácil de identificar anomalias na rede com respeito a possível surgimento de refletores na rede. Desta maneira torna-se mais fácil tomar uma decisão se baseando na origem do refletor uma vez que os dados estarão registrados na tabela.

Uma vez que, por meio da verificação da sessão, um refletor foi identificado, deve-se anotar seu endereço em uma *BlackList* que conterá todos os IP's de quem se deve dropar os pacotes não confiáveis. Em seguida, todos os pacotes do refletor devem ser dropados até que se possa entrar em contato com o serviço vulnerável responsável pela reflexão. Um esquema da arquitetura de atuaçaõ da ferramenta pode ser visualizado na Figura 5.

Embora a ideia da detecção seja simples, precisamos considerar o caso em que a ameaça parte de um grande grupo de refletores, como é proposto em DDoS volumétrico. Neste caso, reforça-se a necessidade de utilizar um contador para cada sessão para evitar falsos positivos. Desta maneira, para n refletores, as sessões destes irão denunciar contadores

negativos revelando a atuação de cada servidor DNS como sendo agentes de reflexão durante o ataque que já foi identificado no primeiro passo. Todos deverão estar na *BlackList*, tendo seus respectivos pacotes dropados. Devido a necessidade de grande processamento, a tabela de estados deve possuir acesso quase que instantâneo para evitar contribuindo não intencionalmente para o ataque de negação. Agora que apresentamos o funcionamento da detecção, vamos analisar a posição arquitetural do módulo de segurança descrito na próxima subseção.

C. ARQUITETURA DE DETECÇÃO EM TEMPO DE EXECUÇÃO

A Figura 5 apresenta resumidamente a atuação da ferramenta implementada que age durante um ataque vindo de A, com uso de uma *BotNet* com endereços falsificados para um grupo de servidores vulneráveis à reflexão. Em seguida, o tráfego é filtrado pela ferramenta antes de chegar na vítima.

A ferramenta por sua vez é composto pelo módulo detector de DDoS, como mencionado no passo 1. O ataque será identificado imediatamente, disparando a verificação da existência de refletores por meio da tabela de estados que verificará a sessão referente a cada pacote de resposta que chegará na rede. Para cada refletor que envia pela interface A, o contador irá ficar negativo, identificando a sua existência. Portanto, os IP's de cada ameaça será registrado na *BlackList*, também localizada no módulo de segurança, que verificará na *WhiteList* se outros pacotes são realmente legítimos, e estes não serão dropados, e sim repassados à vítima pela interface B. Este modo de verificação irá garantir que somente pacotes legítimos de não refletores irão alcançar a vítima, mesmo sob ataque DDoS volumétrico. Desta forma, o impacto será reduzido e o problema mitigado.

Para servidores que possuem sistema de segurança como o *Firewall*, pode-se utilizar a ferramenta como parte do módulo da segurança, e seremos então responsáveis apenas pela detecção dos refletores. Sua localização deve estar antes do *Firewall* para que o mesmo não drope os pacotes antes da ferramenta conseguir construir um *log* para análise.

A implementação dos dois passos permite uma maior segurança do lado da vítima que, pode estar sob ataque de negação de serviço volumétrico com uso de refletores. Este trabalho difere-se de [8] por sua verificação em primeira instância do surgimento de DDoS, o que reduz a necessidade de verificar uma razão entre pedidos e respostas em larga escala, como descrito em [9]. Esta necessidade se dá pelo tratamento individual para cada sessão, ao invés de considerar o tráfego inteiro no cálculo do contador principal. Na pior das hipóteses onde o serviço da vítima irá ficar fora do ar, ainda assim os *logs* denunciarão o IP de todos os refletores utilizados durante o ataque, além de evitar que clientes legítimos sejam confundidos com ameaças. Portanto este método teoricamente se torna eficaz e de grande suporte para reduzir ataques DDoS que tanto complicam servidores, como mostrado nos dados registrados por [3].

V. CONCLUSÃO

A necessidade de suporte a servidores que são alvos de ataques constandes de negação de serviço motiva a pesquisa sobre métodos de se identificar não só máquinas refletoras de um ataque DDoS, como também o próprio autor do ataque. Os dados mostrados em [3] revelam que as ferramentas de defesa hoje existentes não estão dando o suporte que deveriam, ou as aplicações não estão fazendo o uso destas ferramentas por diversos motivos, tais como preço do produto, custo de implementação, dificuldade de manutenção, etc. Embora para algumas empresas seja inviável manter um módulo de segurança que defenda todos os tipos de ataques diferentes na rede, temos que considerar que o DDoS ainda é um dos mais recorrentes ataques nos dias atuais. Portanto, é indispensável considerar o foco da proteção sobre os ataques que ocorrem principalmente no Brasil, como é mostrado na Figura 2.

A identificação por meio de pacotes de resposta reduz o retrabalho e analisa em tempo real os pacotes que estão chegando na rede, evitando perda de processamento por sua simplicidade de implementação. A detecção é simples e fácil de se verificar, uma vez que basta analisar o contador referente à sessão de tráfego anômalo. Sua identificação se mostra teoricamente eficaz, rápido e de raros falsos positivos, uma vez que se o módulo de detecção de DDoS do passo 1 já identificou o ataque, então o comportamento de mais respostas do que requisições condenam quase precisamente quais são os IP's dos possíveis agentes de reflexão. Esta implementação permite cortar refletores um a um, em ataques volumétricos. Portanto, falsos positivos acontecerão em baixa taxa. A identificação sempre registrará em *log*, permitindo ao usuário uma análisa manual sobre os dados, e isolará a vítima evitando assim que ela esteja exposta na internet.

Por fim, é importante destacar que em um cenário onde existem muitos ataques frequentes no mundo todo, as soluções instanciadas de cada variação do DDoS podem ajudar a reduzí-lo como um todo, independente de esteja utilizando a técnica de amplificação, ataque direto, uso de *BotNet*, etc. Por este motivo, este trabalho contribui com a instância do uso de refletores, que pode ser integrada a outras instâncias de soluções em outas partes. Desta maneira trabalhamos melhor contra ameaças no dia-a-dia, reduzimos o número de ataque e geramos segurança e disponibilidade nos serviços propostos no mundo.

VI. TRABALHOS FUTUROS

Como trabalho futuro, pretende-se implementar a ferramenta descrita na seção anterior. Esta ferramenta possibilitará a execução de testes sobre servidores DNS para verificar a sua eficiência e modo de fazer a busca na tabela de estados para evitar processamento desnecessário e, por fim, apresentar os resultados em um novo trabalho refinado que contrubuirá fortemente para a comunidade de segurança na T.I. como um todo.

Após a ferramenta ser implementada e trouxer bons resultados, pretende-se extender os protocolos de DNS para

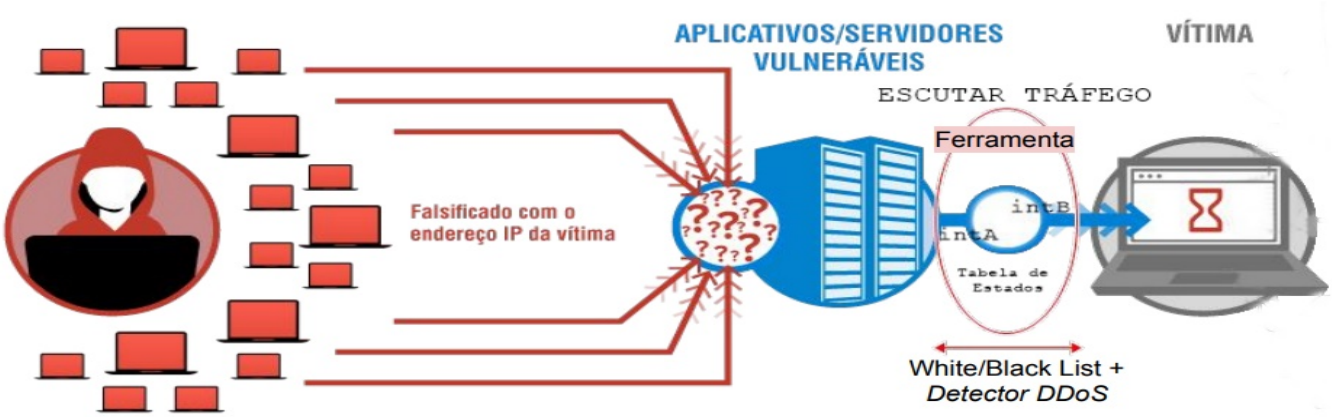

Fig. 5. Arquitetura/Esquema Geral Da Detecção de Refletores [4]

outros tipos de protocolos que também são vulneráveis ao ataque por reflexão.

REFERENCES

[1] Circleid, "DNS-Based Threats: DNS Reflection and Amplification Attacks". Acessado em 12/07/2018. Disponível em: http://www.circleid.com/posts/20180129_dns_based_threats_dns_reflection_and_amplification_attacks/

[2] kaspersky, “Novo método amplifica ataques DDoS”. Acessado em 12/07/2018. Disponível em: https://www.kaspersky.com.br/blog/novo-metodo-amplifica-ataques-ddos/10120/

[3] DDoS Mon, “Insight into Global DDoS Threat Landscape”. Acessado em 12/07/2018. Disponível em: https://ddosmon.net/insight/

[4] Verisign, “Ataque de Inundação de UDP”, Obs.: A imagem foi modificada. Acessado em 12/07/2018. Disponível em: https://www.verisign.com/pt_BR/security-services/ddos-protection/denial-of-service/index.xhtml

[5] D. Mukhopadhyay, Byung-Jun Oh, Sang-Heon Shim, Young-Chon Kim. "A Study on Recent Approaches in Handling DDoS Attacks".

[6] Alexandru G. Bardas, Loai Zomlot, Sathya Chandran Sundaramurthy. "Classification of UDP Traffic for DDoS Detection".

[7] M. Sachdeva, G. Singh, K. Kumar and K. Singh. "Measuring Impact of DDOS Attacks on Web Services".

[8] David Huistra. "Detecting Reflection Attacks in DNS Flows".

[9] G. Kambourakis, T. Moschos, D. Geneiatakis, S. Gritzalis. "Detecting DNS Amplification Attacks".

[10] Wired, "GitHub Survived the Biggest DDoS Attack Ever Recorded". Acessado em 12/07/2018. Disponível em: https://www.wired.com/story/github-ddos-memcached/