Ataques de Amplificação

O que são, como funcionam e como proteger sua infraestrutura

Lucas Rayan Guerra

Introdução

Os ataques de Negação de Serviço Distribuído (DDoS) continuam a ser uma das maiores ameaças à disponibilidade de serviços na internet. Entre as diversas técnicas utilizadas por cibercriminosos, os ataques de amplificação e reflexão (Amplification/Reflection) se destacam pela sua capacidade de gerar volumes massivos de tráfego com um esforço relativamente baixo por parte do atacante. Este tipo de ataque explora a natureza de protocolos de rede que não exigem autenticação e que respondem a pequenas requisições com respostas muito maiores.

Esta cartilha técnica foi elaborada com o objetivo de fornecer um entendimento aprofundado sobre o que são os ataques de amplificação, como funcionam, e, mais importante, como proteger os sistemas contra essa vulnerabilidade crescente. Abordaremos os vetores de ataque mais comuns, seus fatores de amplificação e as medidas de mitigação específicas para cada serviço.

O Que São e Como Funcionam os Ataques de Amplificação?

Um ataque de amplificação é uma forma de ataque de reflexão DDoS. A técnica envolve três participantes:

Atacante
O agente malicioso que inicia o ataque

Refletor
Servidores ou dispositivos na internet com serviços mal configurados ou vulneráveis que são usados para "refletir" e "amplificar" o tráfego

Vítima Final
O alvo real do ataque, cujo endereço IP é usado de forma fraudulenta pelo atacante

O funcionamento do ataque pode ser dividido em três etapas principais, sendo elas:

1 - Requisição com IP falsificado (IP Spoofing)
O atacante envia um grande número de pequenas requisições a um ou mais servidores refletores, mas o IP de origem dessas requisições é falsificado (spoofed) para ser o IP da vítima final. A maioria desses ataques utiliza o protocolo UDP (User Datagram Protocol), que é "connectionless" (não estabelece uma conexão formal como o TCP), facilitando o spoofing do IP de origem, pois não há um handshake de três vias para validar o endereço.

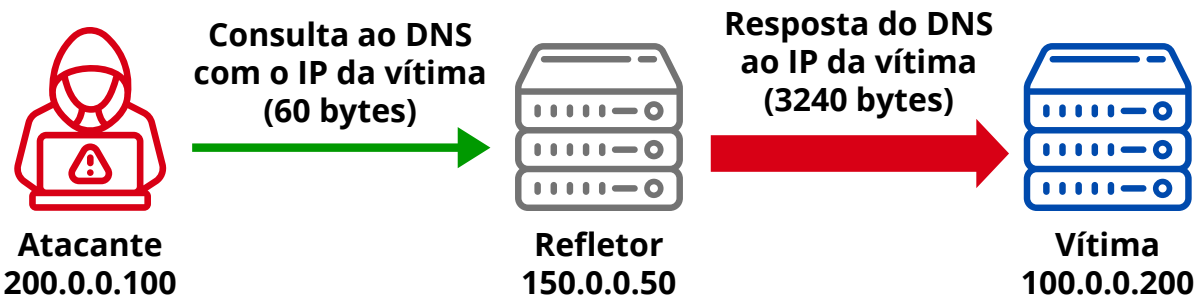
2 - Resposta Amplificada do Refletor.
Os servidores refletores, ao receberem as requisições, respondem de forma legítima. No entanto, o protocolo explorado tem uma característica fundamental: a resposta é significativamente maior do que a requisição original. Essa desproporção é o que define o fator de amplificação (Bandwidth Amplification Factor - BAF). Por exemplo, uma consulta DNS de 64 bytes pode gerar uma resposta de 3.456 bytes, resultando em um fator de amplificação de 54x.

3 - Inundação da Vítima Final
Como as requisições originais tinham o IP da vítima como origem, todas as respostas ampliadas dos servidores refletores são direcionadas para a vítima final. O atacante, utilizando uma botnet, pode enviar requisições para milhares de refletores simultaneamente. O resultado é um volume massivo e avassalador de tráfego que inunda a infraestrutura de rede do alvo, consumindo toda a sua largura de banda e recursos, e tornando seus serviços indisponíveis para usuários legítimos.

Para que fique mais interessante, vamos imaginar um cenário hipotético com as seguintes informações:

IP do atacante: 200.0.0.100
IP da vítima: 100.0.0.200
IP do refletor: 150.0.0.50
Serviço do refletor: DNS Recursivo

Agora vamos a ilustração do cenário.



Perceba que com uma única requisição, o atacante conseguiu criar um tráfego de 3.240 bytes para a vítima, o que é bem pouco. Mas se esse mesmo atacante realizasse 50.000 requisições por segundo, ele criaria um tráfego de 1,29 gigabits/s para a vítima.

Como Proteger os Sistemas

A proteção contra ataques de amplificação envolve duas frentes: prevenir que seus sistemas sejam usados como refletores e proteger sua infraestrutura de ser a vítima final de um ataque.

Prevenindo que Seus Sistemas Sejam Usados como Refletores

Operadores de rede e administradores de sistemas têm a responsabilidade de garantir que seus dispositivos não se tornem parte de um ataque DDoS. As principais medidas incluem:

- **Filtragem de Ingressão:** Provedores de internet (ISPs) devem implementar a filtragem de pacotes na borda de suas redes para descartar tráfego de saída que tenha um endereço IP de origem de fora do seu bloco de IPs. Isso impede que atacantes dentro da sua rede lancem ataques com IP spoofing [1].

- **Configuração Segura de Serviços:** Desabilite ou restrinja o acesso a serviços UDP que podem ser explorados. Se um serviço não precisa estar publicamente acessível, ele deve ser bloqueado por firewall. Para serviços necessários, o acesso deve ser limitado a uma lista de IPs confiáveis (ACLs).

- **Atualização e Patching:** Mantenha todos os sistemas e softwares atualizados para corrigir vulnerabilidades conhecidas que possam ser exploradas em ataques de amplificação.

Protegendo Sua Infraestrutura Contra Ataques

Defender dispositivos e sistemas de ataques desse tipo já é um tanto mais complicado. Porém, existem algumas medidas possíveis, sendo elas:

- **Serviços de Mitigação de DDoS:** Para organizações que são alvos frequentes, a contratação de um serviço especializado em mitigação de DDoS é essencial. Esses serviços possuem a capacidade de rede e as ferramentas necessárias para absorver e filtrar grandes volumes de tráfego malicioso antes que ele atinja sua infraestrutura.

- **Rate Limiting:** Implementar limites de taxa (rate limiting) para respostas de certos protocolos pode ajudar a reduzir a eficácia de um ataque, embora possa não ser suficiente para ataques de grande volume.

- **Firewalls de Borda:** Configure firewalls nos roteadores de borda para bloquear tráfego de portas UDP conhecidas por serem usadas em ataques de amplificação, se esses serviços não forem utilizados em sua rede.

Além das medidas específicas, é fundamental adotar monitoramento contínuo de tráfego com ferramentas de análise de fluxo (NetFlow, sFlow) e sistemas IDS/IPS. Essas soluções permitem identificar rapidamente padrões suspeitos, seja o uso indevido de seus serviços como refletores ou ataques volumétricos direcionados à sua infraestrutura, reduzindo significativamente o tempo de resposta a incidentes.

A segmentação adequada de rede, ACLs restritivas e políticas de menor privilégio fortalecem a defesa em profundidade. Para provedores de internet (ISPs), técnicas como BGP Flowspec e RTBH oferecem bloqueio seletivo de tráfego malicioso na borda da rede. A proteção contra amplificação é um processo contínuo de revisão e ajustes que deve ser integrado à cultura operacional da organização.

BCP 38: A Defesa Contra IP Spoofing

A *"Best Current Practice 38"* é uma recomendação da Internet Engineering Task Force (IETF) que instrui provedores de internet a implementar filtros de pacotes na borda de suas redes.

Segundo a BCP 38, o roteador de borda deve verificar cada pacote de saída. Se o Endereço IP de Origem não pertencer ao bloco de endereços alocado para aquela rede específica, o pacote deve ser descartado imediatamente. Ao impedir que pacotes com IPs falsificados saiam da rede, a BCP 38 elimina a raiz dos ataques de amplificação: a capacidade do atacante de se passar pela vítima.

Análise Detalhada por Serviço Vulnerável

A seguir, estão listados os 11 serviços mais comumente explorados em ataques de amplificação, seus fatores de amplificação e como mitigar a vulnerabilidade em cada um.

Fatores de Amplificação por Protocolo

Serviço	Protocolo/Porta	Fator de Amplificação
Memcached	UDP/11211	de 10.000x a 51.200x
NTP	UDP/123	556,9x (monlist)
CHARGEN	UDP/19	358,8x
DNS Recursivo	UDP/53	de 28x a 54x
SNMP	UDP/161	de 6,3x (média) a > 100x
SSDP	UDP/1900	30,8x
TFTP	UDP/69	60x
Portmapper (RPC)	UDP/111	de 7x a 28x
LDAP	UDP/389	de 46x a 55x
NetBIOS	UDP/137	3,8x
mDNS	UDP/5353	de 2x a 100x

Memcached

Um sistema de cache em memória distribuído, usado para acelerar aplicações web dinâmicas. Seu fator de amplificação é extremamente alto, podendo chegar a 51.200x [2].

Atacantes se conectam a servidores Memcached mal configurados (com a porta 11211/UDP exposta) e armazenam um grande volume de dados. Em seguida, eles enviam uma requisição GET para esses dados, falsificando o IP da vítima. O servidor envia o payload massivo para a vítima. As medidas de proteção são:

- **Desabilitar o Suporte a UDP:** A maioria das implementações de Memcached não precisa de UDP. Desabilite-o na inicialização.

- **Firewall:** Nunca exponha a porta 11211 (TCP ou UDP) à internet. O acesso deve ser restrito à sua rede de aplicação interna.

NTP (Network Time Protocol)

Serviço utilizado para sincronizar os relógios de computadores em uma rede. Seu fator de amplificação a até 556,9x [3].

A vulnerabilidade mais explorada é o comando "*monlist*", que retorna uma lista dos últimos 600 clientes que se conectaram ao servidor NTP. Uma pequena requisição para "*monlist*" pode gerar uma resposta massiva. As medidas de proteção são:

- **Atualize o Servidor NTP:** Versões do ntpd a partir da 4.2.7p26 desabilitaram o comando monlist por padrão.

- **Desabilite "*monlist*" Manualmente:** Em versões mais antigas, adicione "*disable monitor*" ao arquivo de configuração "*ntp.conf*".

- **Use ntpq e ntpdc com Cautela:** Restrinja o acesso a esses comandos de consulta para evitar outros abusos.

CHARGEN (Character Generator Protocol)

É um protocolo de depuração antigo que gera um fluxo de caracteres. Seu fator de amplificação é de 358,8x [4].

O atacante envia um pequeno pacote UDP para a porta 19/UDP de um servidor com CHARGEN habilitado. O servidor responde com um pacote contendo uma string de caracteres, que é muito maior. As medidas de proteção são:

- **Desabilite o Serviço:** CHARGEN é um serviço obsoleto e inseguro. Ele deve ser desabilitado em todos os sistemas.

SNMP (Simple Network Management Protocol)

Usado para gerenciar e monitorar dispositivos de rede como roteadores, switches e servidores. Seu fator de amplificação varia de 6,3x a mais de 100x, dependendo da quantidade de dados solicitada [6].

Atacantes enviam requisições SNMP (como "*GetBulk*") com o IP da vítima para dispositivos com community strings padrão (ex: "public", "private"). A resposta, contendo uma grande quantidade de dados de gerenciamento, é muito maior que a requisição. As medidas de proteção são:

- **Altere as Community Strings Padrão:** Nunca use "public" ou "private". Utilize strings complexas e únicas.

- **Use SNMPv3:** A versão 3 do SNMP oferece autenticação e criptografia, tornando-a imune a ataques de reflexão simples.

- **Restrinja o Acesso:** Configure ACLs (Access Control Lists) para permitir que apenas estações de gerenciamento autorizadas consultem os dispositivos via SNMP.

- **Bloqueie a Porta /UDP:** Na borda da rede, bloqueie o tráfego SNMP vindo da internet se o gerenciamento remoto não for necessário.

DNS Recursivo (Domain Name System)

Servidores DNS abertos (Open Resolvers) que respondem a consultas recursivas de qualquer cliente na internet. Seu fator de amplificação varia entre 28 e 54x [5].

O atacante envia uma consulta DNS para um tipo de registro que gera uma resposta grande (como ANY ou registros TXT de DNSSEC), usando o IP da vítima como origem. O servidor DNS aberto responde à vítima com os dados amplificados. As medidas de proteção são:

- **Restrinja a Recursão:** Configure seu servidor DNS para realizar consultas recursivas apenas para clientes da sua própria rede (ACLs).

- **Implemente Response Rate Limiting (RRL):** Tecnologias como RRL em servidores BIND ajudam a mitigar a amplificação, limitando o número de respostas idênticas enviadas a um mesmo cliente.

SSDP (Simple Service Discovery Protocol)

Parte do padrão UPnP (Universal Plug and Play), usado por dispositivos de rede (impressoras, roteadores, câmeras) para se anunciarem na rede local. Seu fator de amplificação é tipicamente em torno de 30x [7].

Atacantes enviam uma requisição de descoberta "*M-SEARCH*" para dispositivos vulneráveis, falsificando o IP da vítima. Os dispositivos respondem com um arquivo XML de descrição, que é muito maior que a requisição. As medidas de proteção são:

- **Bloqueie a Porta 1900/UDP:** Na borda da rede, bloqueie todo o tráfego de entrada e saída na porta 1900/UDP. Este protocolo foi projetado para uso em redes locais e nunca deve ser exposto à internet.

TFTP (Trivial File Transfer Protocol)

Um protocolo simples para transferência de arquivos, frequentemente usado para inicializar estações de trabalho sem disco e fazer backup de configurações de dispositivos de rede. Seu fator de amplificação pode chegar a 60x [8].

O atacante solicita um arquivo grande de um servidor TFTP público, falsificando o IP de origem para o da vítima. O servidor então envia o arquivo em múltiplos pacotes UDP para a vítima. As medidas de proteção são:

- **Desabilite o Serviço:** Se o TFTP não for necessário, desabilite-o.
- **Firewall:** Coloque o servidor TFTP atrás de um firewall e restrinja o acesso apenas a IPs autorizados.
- **Bloqueie a Porta 69/UDP:** Bloqueie o acesso externo à porta 69/UDP na borda da rede.

Portmapper (RPCbind)

Um serviço usado em sistemas Unix-like para mapear serviços RPC (Remote Procedure Call) para as portas de rede em que eles estão escutando. Seu fator de amplificação fica entre 7 e 28x [9].

O atacante envia uma requisição "*PMAP_DUMP*" para o serviço Portmapper (porta 111/UDP), que responde com uma lista de todos os serviços RPC registrados, gerando uma resposta muito maior que a requisição. As medidas de proteção são:

- **Firewall:** Bloqueie o acesso à porta 111/UDP da internet. O Portmapper raramente precisa de acesso público.
- **Desabilite RPC se não for necessário:** Em muitos sistemas modernos, o Portmapper pode ser desabilitado se não houver serviços RPC em uso.

LDAP (Lightweight Directory Access Protocol)

É um protocolo para acessar e manter serviços de informação de diretório distribuído. Seu fator de amplificação varia entre 46 e 55x [10].

Atacantes enviam uma consulta de busca para um servidor LDAP com a porta 389/UDP exposta. A resposta, contendo entradas do diretório, é enviada para o IP falsificado da vítima. As medidas de proteção são:

- **Bloqueie a Porta 389/UDP:** O acesso LDAP a partir da internet é raramente necessário e deve ser bloqueado. Se for preciso, use LDAP sobre SSL/TLS (LDAPS, porta 389/TCP) e restrinja o acesso com ACLs.

NetBIOS (Network Basic Input/Output System)

Serviço antigo usado para descoberta de nomes em redes locais Windows. Seu fator de amplificação é relativamente baixo, em torno de 3,8x, mas ainda eficaz em grande escala [11].

Atacantes enviam uma requisição de status de nome para um servidor NetBIOS Name Server (NBNS) na porta 137/UDP. A resposta com informações do dispositivo é maior que a requisição. As medidas de proteção são:

- **Bloqueie as Portas 137-139/UDP:** Esses serviços são legados e inseguros, e nunca devem ser expostos à internet.

mDNS (multicast DNS)

Usado para descoberta de serviços e resolução de nomes em redes locais sem a necessidade de um servidor DNS central (usado por tecnologias como Apple Bonjour). Seu fator de amplificação varia entre 2 e 10x [12].

Similar ao SSDP, atacantes enviam consultas para a porta 5353/UDP de dispositivos vulneráveis, que respondem com informações de serviço para o IP falsificado da vítima. As medidas de proteção são:

- **Bloqueie a Porta 5353/UDP:** O mDNS é projetado para redes locais. Bloqueie o acesso a esta porta na borda da rede.

Conclusão

Os ataques de amplificação representam uma ameaça significativa e persistente devido à abundância de serviços mal configurados na internet. Para profissionais de DevOps e operações de provedores, a defesa é uma responsabilidade compartilhada. É imperativo não apenas proteger a própria infraestrutura contra esses ataques, mas também garantir que seus sistemas não sejam cooptados para atacar terceiros.

A implementação de práticas de configuração segura, como a desativação de serviços desnecessários, o uso de firewalls, a aplicação de ACLs e a adoção do BCP 38, são passos fundamentais para mitigar essa classe de ameaças. A vigilância contínua e a atualização dos sistemas são a linha de frente na batalha contra os ataques de DDoS por amplificação.

Referências

[1] IETF. (1998). BCP 38 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.

[2] Cloudflare. (2018). Memcrashed - Major amplification attacks from UDP port 11211.

[3] Cloudflare. (2014). Technical Details Behind a 400Gbps NTP Amplification DDoS Attack.

[4] CISA. (2014). UDP-Based Amplification Attacks.

[5] Cloudflare. DNS Amplification DDoS Attack.

[6] Imperva. SNMP Reflection / Amplification DDoS Attack.

[7] Cloudflare. SSDP DDoS Attack.

[8] Akamai. Attack types - TFTP Reflection.

[9] Lumen. (2015). A New DDoS Reflection Attack: Portmapper.

[10] F5 Labs. (2016). Old Protocols, New Exploits: LDAP Unwittingly Serves DDoS Amplification Attacks.

[11] INCIBE. (2021). DrDoS: characteristics and operation.

[12] Vercara. (2025). Multicast DNS (mDNS) Amplification DDoS.

Apêndice A - Checklist de Proteção (ISPs)

Filtragem e Validação
□ Implementar BCP 38 (Ingress Filtering) na borda da rede.
□ Validar endereços IP de origem em todo tráfego de saída.
□ Descartar pacotes com IPs falsificados (spoofed).

Configuração de Serviços
□ Desabilitar serviços UDP desnecessários em infraestrutura própria.
□ Implementar ACLs para restringir acesso a serviços de gerenciamento.
□ Manter sistemas de roteamento e servidores atualizados.

Monitoramento e Mitigação
□ Monitorar tráfego UDP para detectar padrões de amplificação.
□ Estabelecer parcerias para mitigação (Scrubbing Centers).

Apêndice B - Checklist de Proteção (Operações)

Infraestrutura Interna
□ Desabilitar UDP em serviços Memcached (-U 0).
□ Restringir acesso a SNMP, NTP e DNS (apenas IPs internos).
□ Migrar para SNMPv3 (com autenticação e criptografia).

Firewall de Borda
□ Bloquear portas UDP vulneráveis para tráfego externo:
19, 53, 69, 111, 123, 137, 161, 389, 1900, 5353, 11211
□ Implementar Rate Limiting para serviços DNS públicos.
□ Monitorar tráfego de saída para detectar padrões de spoofing.

Resposta a Incidentes
□ Estabelecer plano de resposta a DDoS com contatos do ISP.
□ Realizar testes periódicos de segurança e varreduras de vulnerabilidade.