allot
See. Control. Secure.

DDoS ATTACK HANDBOOK

Enterprise

CONTENTS

INTRODUCTION

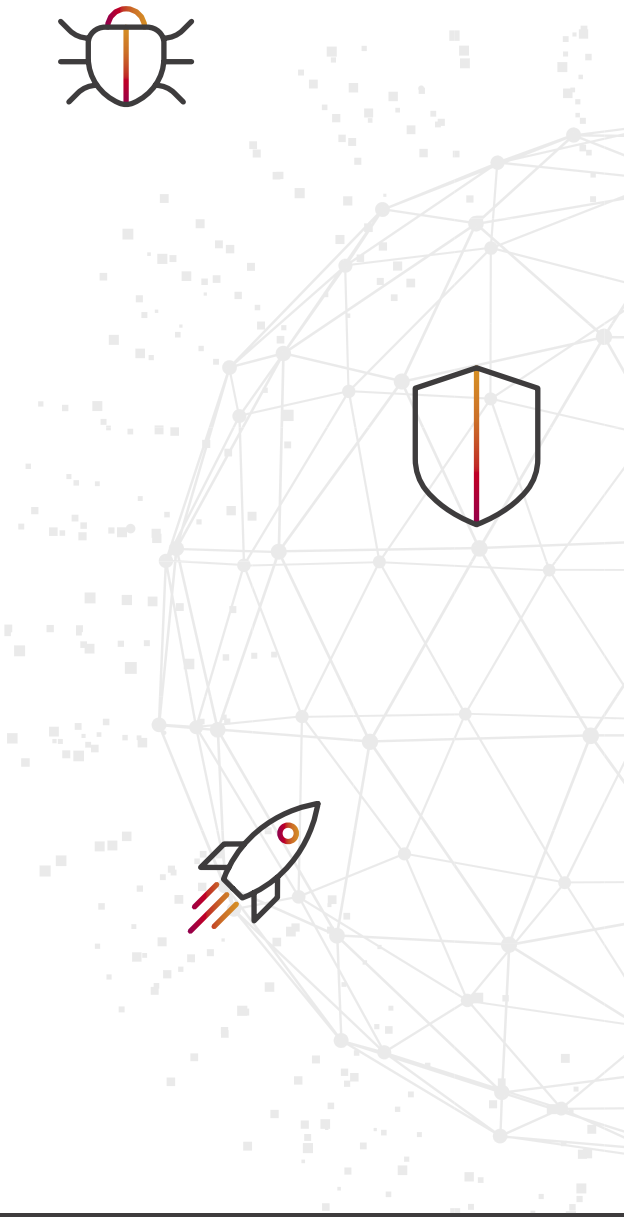
Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks have plagued commercial and enterprise networks since early 1970. In terms of damage to network infrastructure, service continuity and business reputation, DoS/DDoS attacks have racked up some of the most successful cyberattacks to date.

Historically, enterprises assigned low risk to their chances of being attacked and avoided taking protective measures, assuming they could dodge the DDoS bullet. Today, technological advances have made it easier to launch flooding attacks and to increase the scope of damage. Enterprises can no longer afford to take a reactive approach that assumes, "If it hasn't happened to my network, it probably won't. And if it does, I'll handle it then." Deferred action is no longer a viable option.

One of the main factors driving enterprises to adopt a DDoS Protection strategy is the rise in enterprises who are migrating data centers and IT infrastructure to the cloud.

Another factor is the Quality of Experience (QoE) that enterprise users expect. Sluggish response time is not appreciated and downtime is not tolerated. To assure service availability and performance, enterprises must take measures to protect against DDoS attacks that are designed to overwhelm network resources and deny service to legitimate users.

This DDoS Attack Handbook outlines the most common attacks and their implications for network assets and business.



FIGHTING DDoS

WHAT IS A DDOS ATTACK?

A Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack occurs when one or many compromised (that is, infected) systems launch a flooding attack on one or more targets, in an attempt to overload their network resources and disrupt service or cause a complete service shutdown.

NEUTRALIZING ATTACKS AS THEY OCCUR

Massive DDoS attacks can cause immediate service interruption. Effective protection must be able to detect the attack and act fast enough to thwart it, so there is little or no impact on the network and/or its hosted targets. Fast detection and mitigation is even more important when dealing with hit-and-run DDoS attacks that are designed to do maximum damage in just a few minutes and then disappear.

Allot's DDoS Protection solution, powered by Allot DDoS Secure, detects and mitigates DDoS attacks inline, on the spot, within seconds, leaving the network and hosted targets unharmed. Allot's inline advantage and real-time detection makes the solution highly effective even for fragmented DDoS attacks.

DETECTING AND MITIGATING TOMORROW'S ATTACKS

Cybercriminals continually hone their methods and change their tactics, such that DDoS attacks exceeding 100 Gbps are no longer uncommon. Often, there is no advanced warning or known signature for an attack, as cybercriminals leverage the element of surprise to avoid detection and inflict maximum damage before the enterprise can figure out what's going on and respond. To protect service networks against today's and tomorrow's attacks, enterprises need a solution that can scale to match the ever-increasing volume and innovation of these attacks.

The patented Network Behavior Anomaly Detection (NBAD) technology inside Allot's DDoS Secure enables enterprises to identify unknown (zero-day) attacks which have never been seen before and mitigate them in seconds. Allot's DDoS Secure runs on Allot's multiservice platform, which provides scalable capacity to detect and mitigate massive attacks coming in even at Terabits per second. Allot's multiservice platform also provides granular policy management. This allows enterprises to accurately block attack traffic and avoid false positives, and to trigger traffic shaping to assure user Quality of Experience (QoE).

STOPPING INBOUND AND OUTBOUND THREATS

While most DDoS Protection systems focus on inbound attacks, outbound DDoS that originates within the network and attacks external targets can also exhaust network resources and impact QoE.

Allot's inline deployment protects equally against both inbound and outbound DDoS attacks.

MULTILAYER DEFENSE STRATEGY WORKS BEST

DDoS detection and mitigation solutions are a first line of defense in stopping the attack and assuring service availability. But what about quality of experience? How can enterprises assure the delivery of critical applications at all times - even during an attack. Or how can enterprises prevent individual users who are generating abnormal volumes of traffic (not an attack, per se) from eating up available bandwidth? With a multilayer approach and a multiservice platform like Allot Service Gateway, enterprises can combine proactive defense measures such as policy-based traffic shaping with the event-triggered measures of DDoS mitigation.

FIGHTING DDoS

ACCURATE VISIBILITY TO ASSESS ATTACK IMPACT

Visibility is critical to effective DDoS Protection. Visibility includes essential threat intelligence stats that facilitate root cause investigation to find out: How big is the attack? What type is it? Who is the attacker? What are the targets?. Allot's multiservice platform enables analysis of network usage statistics together with threat intelligence to obtain a more advanced assessment of DDoS attack impact on the enterprise's business.

For example, how was subscriber and/or application QoE affected during the DDoS attack? This information is even more important to business customers who range from private enterprises (such as, finance, retail, and health) to public organizations and government agencies.

Allot Inbound DDoS Protection

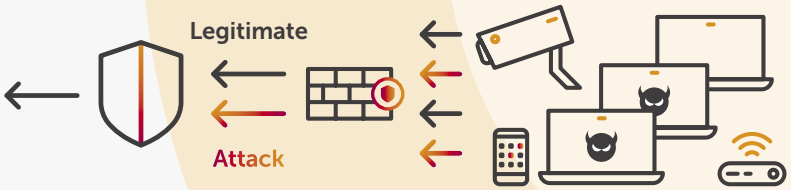
1. **Mitigate attacks in seconds**
   Eliminate congestion on costly transit links
2. **Protect the perimeter**
   Prevent overload on routers, rewalls, load balancers
3. **Assure service availability**
   Legitimate traffic continues to flow

Infected bots

Inbound DDoS

Flooding attacks threaten service availability

EXTERNAL EDGE CORE



Infected IoT devices

Outbound Bot Traffic

Illegitimate bot traffic congesting the network

Allot Outbound Bot Containment

1. **Guarantee QoE**
   Prioritize delivery of critical apps during attack
2. **Block botnet traffic**
   Only botnet traffic is blocked while legitimate traffic behind NAT IP flows freely
3. **Isolate the bots**
   Isolate from the network and block attempts to spread infection

Watch a webinar to learn about the latest DDoS threats and how to protect against them. ›

REASONS FOR DDOS ATTACKS

With DDoS attacks, the perpetrator's main goal is to use botnets to make your website inaccessible. Botnets are basically an army of connected devices that are infected with malware. Your website's server becomes overloaded and exhausted of its available bandwidth because of this army. Most often, attacks of this nature don't usually breach data or go over any security parameters.

So, if it's not to breach your data, why would someone go through the effort to shut down your website?

DDOS ATTACKS FOR HACKTIVISM

Hacktivism uses cyberattacks for political motivations, using cyber sabotage to promote a specific cause. As compared to the hacking industry's focus on data theft, hacktivism is not motivated by money. Hacktivists are motivated by revenge, politics, ideology, protest, and a desire to humiliate victims. Profit is not a factor. Visibility is key.

One example is **Anonymous**, a decentralized international hacktivist collective that is widely known for its various cyberattacks against several governments, government institutions, and government agencies, corporations, and the Church of Scientology. Operation Payback carried out by Anonymous started as retaliation to distributed denial of service (DDoS) attacks on torrent sites; piracy proponents then decided to launch DDoS attacks on piracy opponents. The initial reaction snowballed into a wave of attacks on major pro-copyright and anti-piracy organizations, law firms, and individuals.

RANSOM DDOS (RDDOS) ATTACKS

Ransom Distributed Denial-of-Service (RDDoS) attacks are extortion-based DDoS attacks that are motivated by financial gain.

Cybercriminals typically send a ransom note threatening to launch DDoS attacks unless a ransom is paid by the given deadline. On occasion, to validate and give credibility to their threat, demonstrative DDoS attacks are launched by the threat actors against the victim before or after sending the ransom note.

DDOS TOOLS AND TECHNIQUES

Denial-of-Service (DoS) attacks have come a long way since the days of LOIC and other GUI-based tools. Today, hackers are abandoning "old school" GUI and script tools, opting to pay for attacks via stresser services. They no longer need to acquire technical expertise or tools; instead, they can simply engage attack services to launch an attack.

Many notorious distributed denial-of-service (DDoS) groups—including Lizard Squad, New World Hackers and PoodleCorp—have entered the DDoS-as-a-Service business, monetizing their capabilities by renting their powerful stresser services. Groups sometime use their tools against high-profile targets to showcase and promote their attack services. As the point of entry becomes easier to cross, novice attackers may carry out larger, more sophisticated assaults. For just $19.99 a month, an attacker can run 20-minute bursts for 30 days using a number of attack vectors, such as DNS, SNMP, and SSYN, and slow GET/POST application-layer DoS attacks.

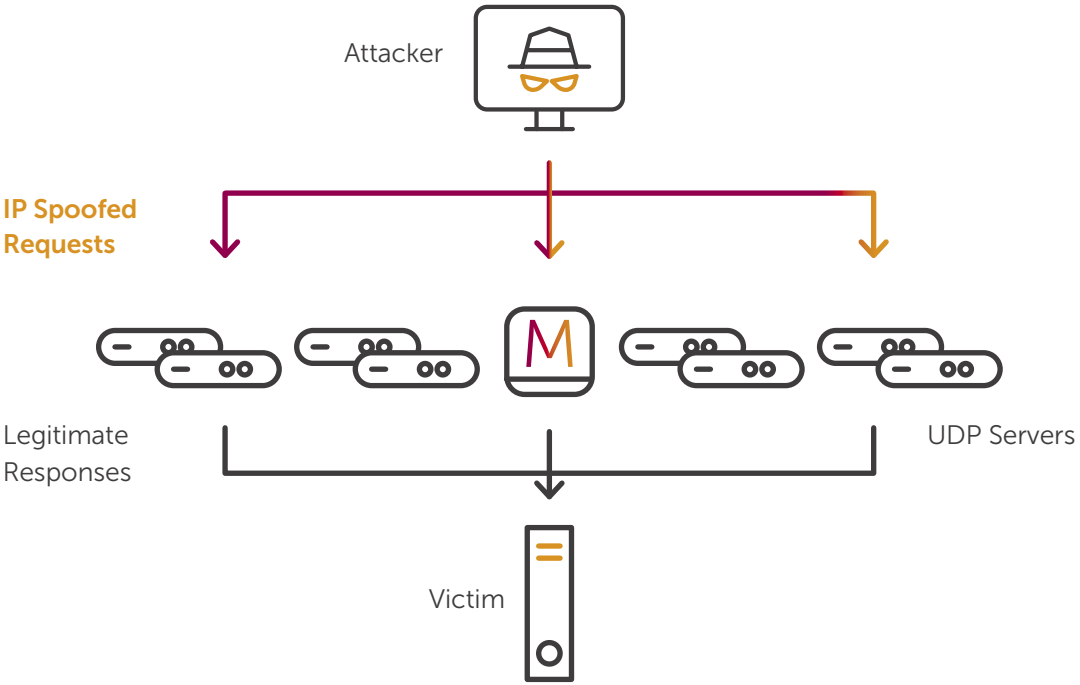
Most tools offer basic TCP, UDP, and HTTP attack vectors with slight variations. Some enable the attacker to customize payload options—including packet size, randomized data, threads and sockets per thread—in the tools. HTTP attacks are a popular vector. When an operation is underway, hackers can easily bypass mitigation solutions and overwhelm server resources with simple POST/GET floods that appear to be legitimate traffic.

MEMCACHED AMPLIFICATION ATTACK

WHAT IS A MEMCACHED ATTACK?

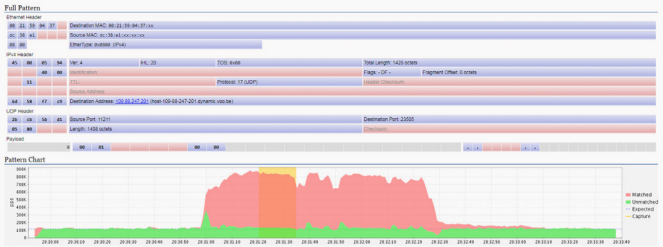
Memcached attacks are a type of User Datagram Protocol (UDP) reflected amplification attack which uses vulnerable memcached servers exposed on the Internet. The attacker first loads the memcached server database. It then sends requests over UDP, using a forged IP address (the target's), to thousands of memcached servers which are open on the Internet. The servers respond by sending many UDP packets coming from source port 11211 to the target. The potency of the attacks is due to memcached servers amplifying the target's spoofed requests by a factor of 50,000.

In February 2018, before publication of the record-breaking memcached attack, Allot's bi-directional, inline DDoS Secure solution successfully detected and prevented such attacks observed in multiple customer networks worldwide. Below is an example:



Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console



⚠ Enterprise Potential Risks

Enterprise users will experience protracted service interruption due to extreme network congestion caused by the bombardment of critical services with voluminous memcached responses, potentially exceeding tens of terabits per second.

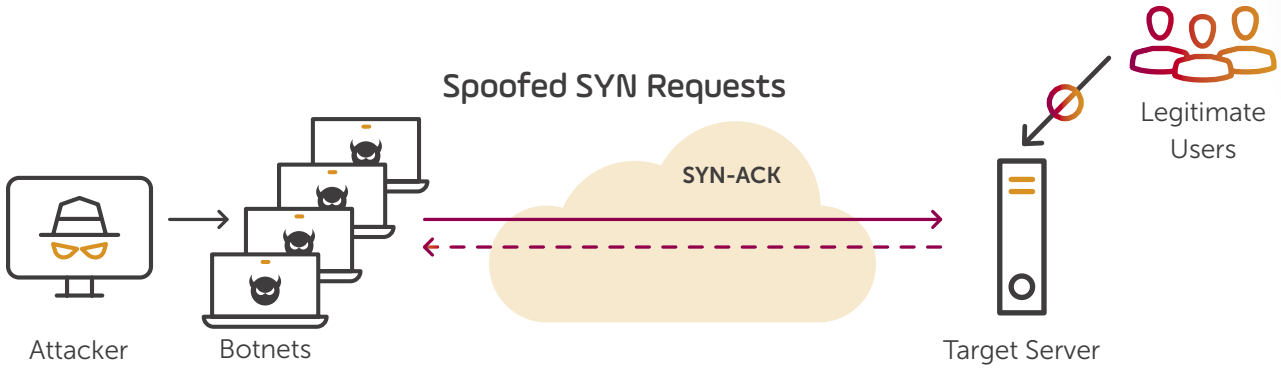
Learn how Allot helped service providers stop memcached attacks ›

SYN FLOOD

WHAT IS A SYN FLOOD?

A SYN Flood, often generated by botnets, is designed to consume resources of the victim server, such as firewall or other perimeter defense elements, in an attempt to overwhelm its capacity limits and bring it down. The target receives SYN packets at very high rates which rapidly fill up its connection state table, resulting in disconnections, dropping of legitimate traffic packets, or even worse – element reboot.

SYN Floods exploit the TCP (Transmission Control Protocol) three-way handshake process to wreak havoc. The attack floods multiple TCP ports on the target system with SYN messages requesting to initiate a connection between the source system and the target system. The target responds with a SYN-ACK message for each SYN message it receives and temporarily opens a communications port for the requested connection while it waits for a final ACK message from the source in response to each SYN-ACK message. The attacker never sends the final ACK and therefore the connection is never completed. The temporary connection will eventually time out and be closed, but not before the target system is overwhelmed with incomplete connections accumulated in its state table.



STEP 1
Attacker sends many SYN requests

STEP 2
Victim server sends SYN/ACK but attacker does not reply

STEP 3
Server state table overloads and legitimate users are not served

Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console

⚠ Enterprise Potential Risks

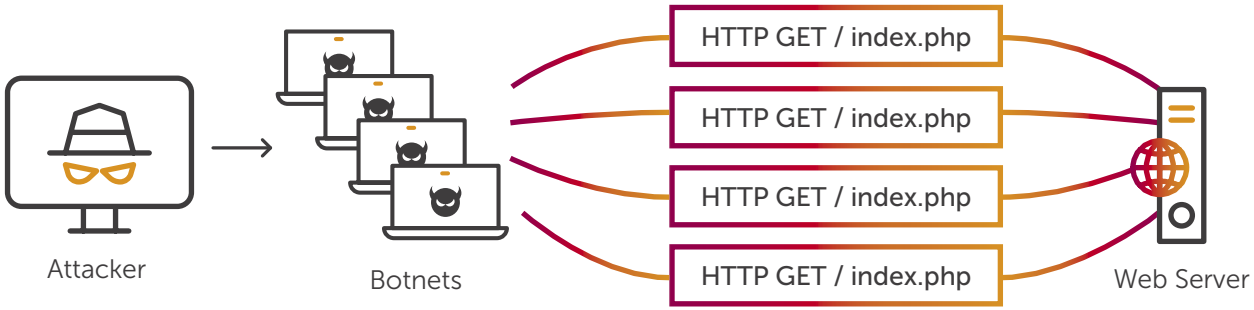
Once the SYN Flood succeeds in taking down perimeter defense elements, enterprise services remain unprotected and exposed to security threats until the attack is neutralized and systems are restored.

HTTP/S FLOOD

WHAT IS A HTTP/S FLOOD ATTACK?

HTTP (and its encrypted form HTTPS) is a transport protocol for browser-based Internet requests, commonly used to load webpages or to send form content over the Internet. In an HTTP/S flood attack the attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web service or application. These attacks often utilize many botnets such as infected IoT devices.

The devices are coordinated to send multiple GET requests for image files or some other asset from the target web server. The flood of HTTP requests depletes the server resources until denial of service occurs for requests coming from legitimate users. An HTTP flood can also be launched by sending multiple POST requests which will trigger intensive processing on the server and will saturate server resources even more quickly.



⚠ Enterprise Potential Risks

Web services become overwhelmed and innocent users will become service-denied.

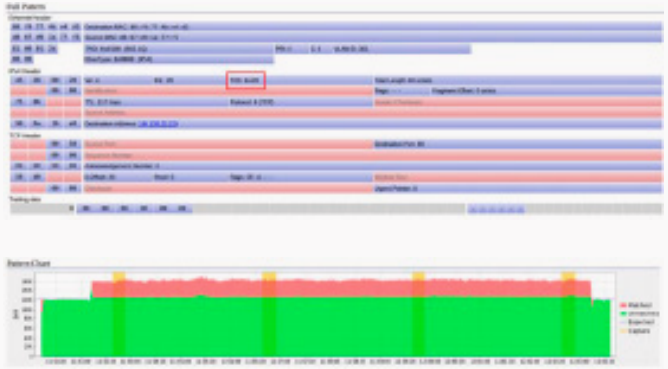
TOS FLOOD

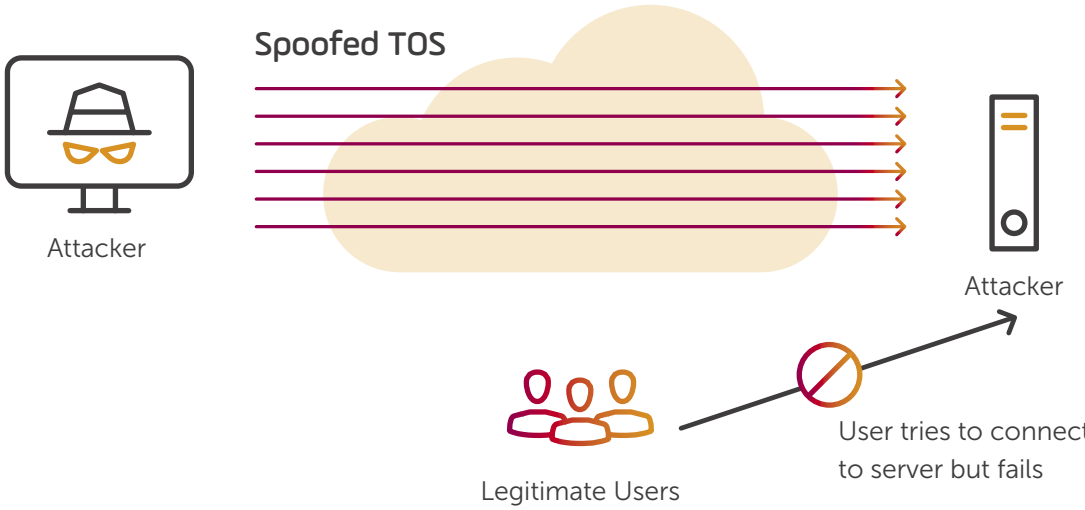
WHAT IS A TOS FLOOD?

In a TOS (Type of Service) Flood, attackers forge the 'TOS' field of the IP packet header, which is used for Explicit Congestion Notification (ECN) and Differentiated Services (DiffServ) flags. There are two known types of TOS attack scenarios. In the first, the attacker spoofs the ECN flag, which reduces the throughput of individual connections thereby Allot's DDoS Secure causing a server to appear out of service or non-responsive. In the second, the attacker utilizes the DiffServ class flags in the TOS field to increase the priority of attack traffic over legitimate traffic in order to intensify the impact of the DDoS attack.

Attack pattern

Attack pattern and matched traffic reported by Allot ServiceProtector management console





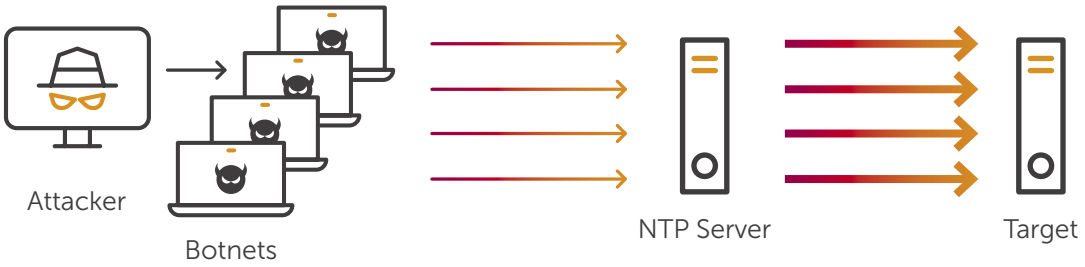
⚠ Enterprise Potential Risks

Network services will slow down or become non-responsive due to reduced connection throughput caused by the TOS forging. Applications like VoIP, that require fast response time, will suffer dropped calls and bad QoE due to attack traffic receiving higher DiffServ priority than legitimate VoIP traffic.

NTP AMPLIFICATION

WHAT IS NTP AMPLIFICATION?

In an NTP (Network Time Protocol) amplification, an attacker uses a spoofed IP address of the victim's NTP infrastructure and sends small NTP requests to servers on the Internet, resulting in a very high-volume of NTP responses. Since attackers spoof the victim's NTP infrastructure, all of the reflected/amplified responses flood the victim's NTP server. The NTP response packets resemble real NTP traffic, making this attack difficult to detect. The amplification factor may reach 50X, resulting in massive flooding which can take the NTP server or the entire network offline.



Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console

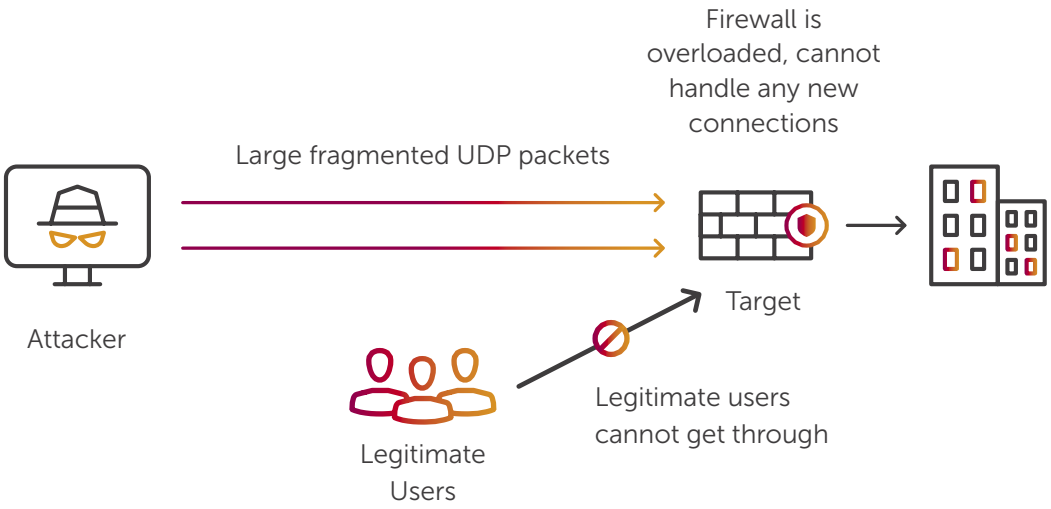
⚠ Enterprise Potential Risks

Enterprise users experience unpredictable interruptions in connectivity due to attack taking down the NTP server and/or the entire network.

UDP FRAGMENTATION

WHAT IS UDP FRAGMENTATION?

UDP Fragmentation attacks send large UDP packets (1500+ bytes) which consume more network bandwidth. Since the fragmented packets usually cannot be reassembled, they consume significant resources on stateful devices such as firewalls along the traffic path. When combined with other types of flood attacks, this may result in drop of legitimate traffic by the destination server being flooded.



Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console

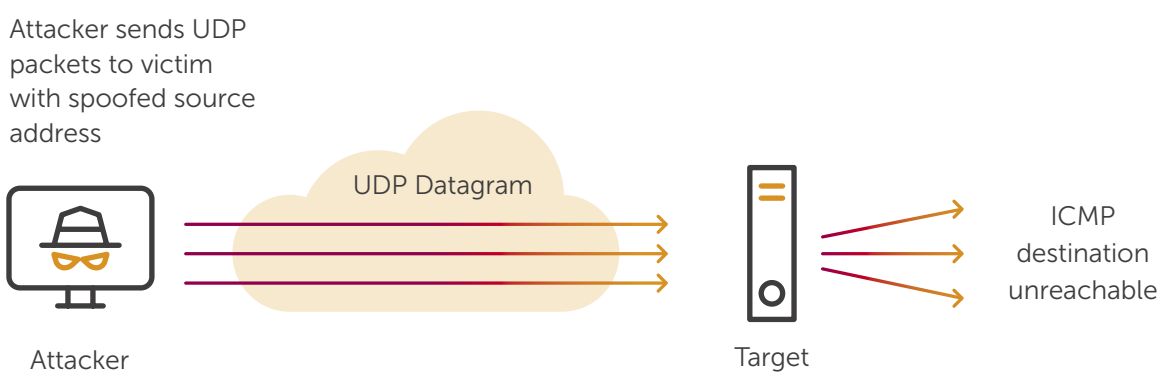
⚠ Enterprise Potential Risks

- Enterprise users experience connectivity issues as a result of attack traffic congesting network resources.
- Enterprise network remains unprotected for long hours due to overwhelmed perimeter defense elements which were brought down.

UDP FLOOD

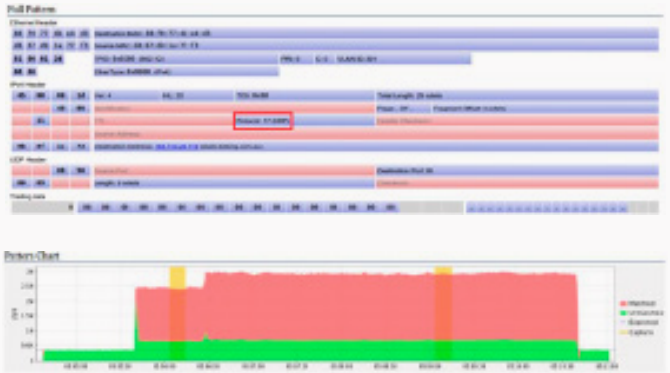
WHAT IS A UDP FLOOD?

In a UDP Flood, attackers send small spoofed UDP packets at a high rate to random ports on the victim's system using a large range of source IPs. This consumes essential network element resources on the victim's network which are overwhelmed by the large number of incoming UDP packets. Often victim servers start to reply back with ICMP destination unreachable packets. UDP attacks are difficult to detect and block because they often do not match a consistent pattern, and are therefore effective in exhausting network resources until they go offline.



Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console



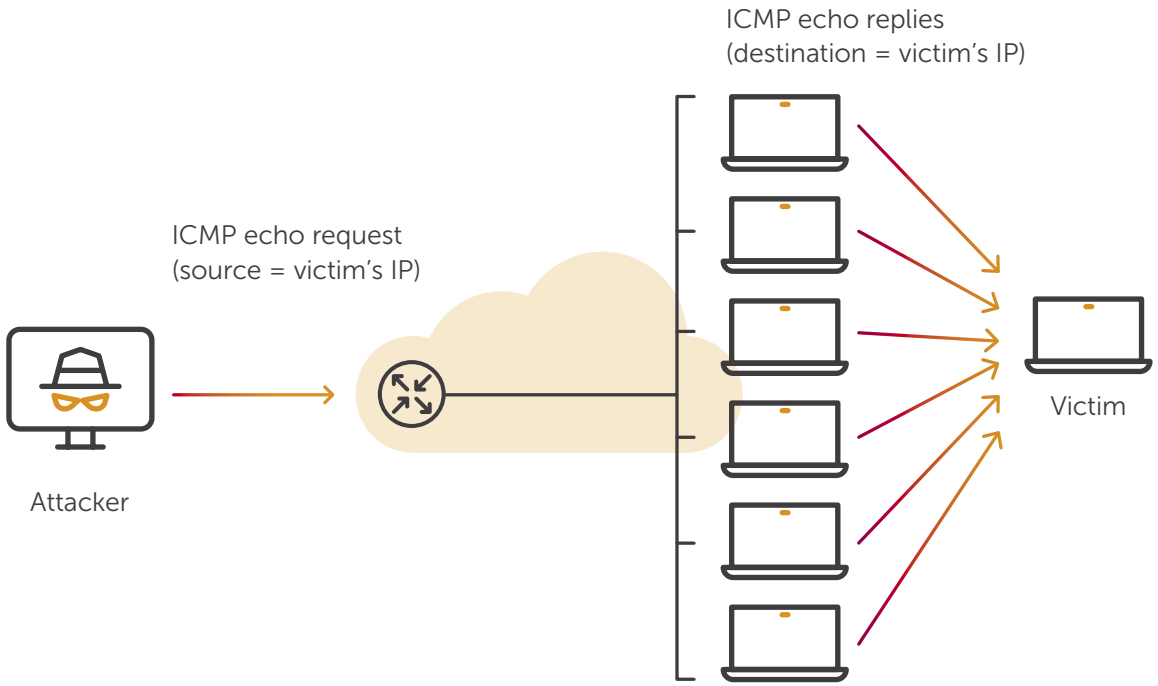
⚠ Enterprise Potential Risks

Unpredictable network congestion caused by attack traffic that is consuming bandwidth will affect network performance and user QoE. If not detected, the enterprise may assume bandwidth capacity is not sufficient for increasing demand, but this problem cannot be solved by a bandwidth expansion or expensive network infrastructure upgrade.

PING FLOOD

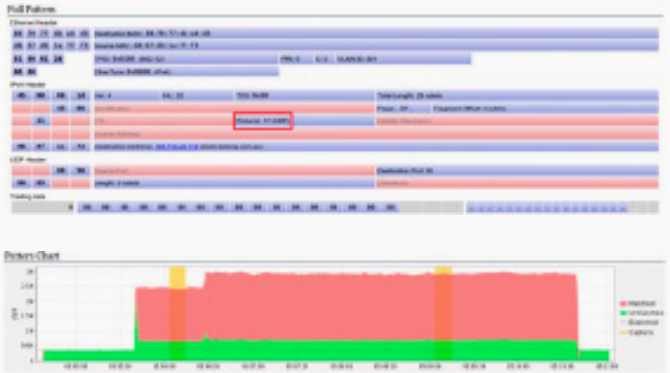
WHAT IS A PING FLOOD?

In a Ping Flood, an attacker sends spoofed ICMP echo request (pings) packets at a high rate from random source IP ranges or using the victim's IP address. Most devices on a network will, by default, respond to the ping by sending a reply to the source IP address. If numerous endpoints on the network receive and respond to these pings, the victim's IP addresses will be flooded with traffic and their devices/computers/servers will become unusable.



Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console



⚠ Enterprise Potential Risks

Unpredictable network congestion caused by attack traffic that is consuming bandwidth will affect network performance and user QoE. If not detected, the enterprise may assume bandwidth capacity is not sufficient for increasing demand, but this problem cannot be solved by a bandwidth expansion or expensive network infrastructure upgrade.

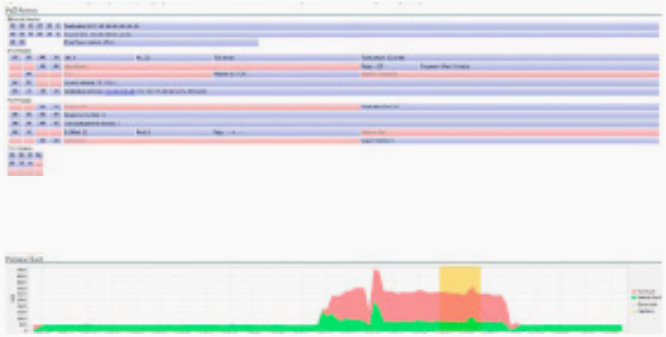
ACK FLOOD (OR ACK-PUSH FLOOD)

WHAT IS AN ACK FLOOD?

In an ACK or ACK-PUSH Flood, attackers send spoofed ACK (or ACK-PUSH) packets at very high packet rates. In other words, they acknowledge session requests that were never sent and do not exist. Packets that do not belong to any existing session on the victim's firewall or any security device along the path, generate unnecessary lookups in the state tables. This extra load exhausts system resources.

Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console



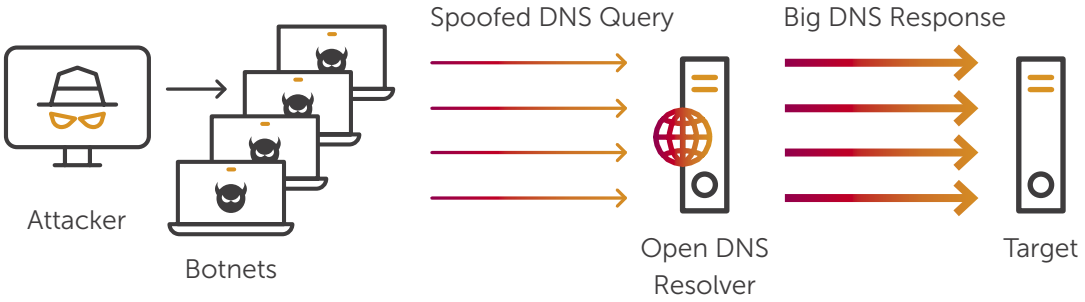
⚠ Enterprise Potential Risks

Once the ACK Flood succeeds in taking down perimeter defense elements, the enterprise's users and services remain unprotected and exposed to security threats until the attack is neutralized and systems are restored.

DNS FLOOD

WHAT IS A DNS FLOOD?

A DNS Flood sends spoofed DNS requests at a high packet rate and from a wide range of source IP addresses to the target network. Since the requests appear to be valid, the victim's DNS servers respond to all the spoofed requests, and their capacity can be overwhelmed by the sheer number of requests. This attack consumes large amounts of bandwidth and other network resources. Eventually, it exhausts the DNS infrastructure until it goes down, taking the victim's Internet access (WWW) and offline hosted sites with it.



Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console

⚠ Enterprise Potential Risks

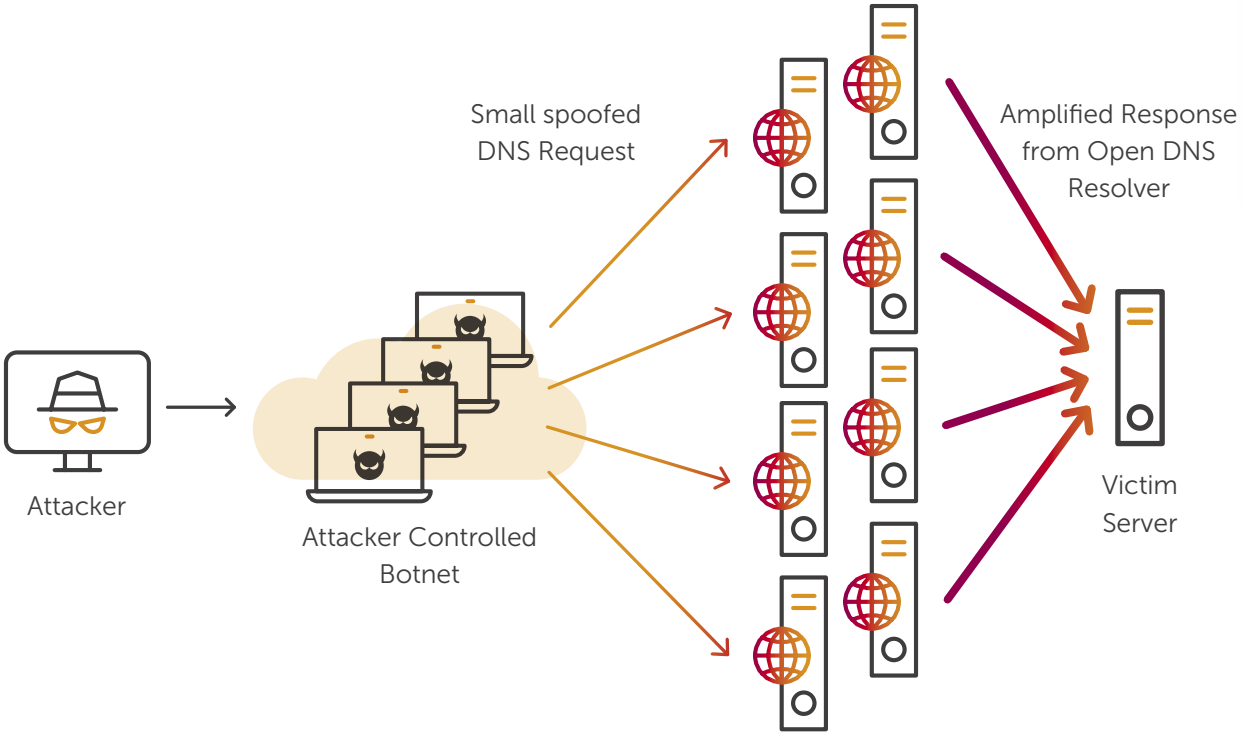
Enterprise users and customers lose access to specific sites and services causing damage to the enterprise's reputation and/or SLAs.

AMPLIFIED DNS FLOOD

WHAT IS AN AMPLIFIED DNS FLOOD?

An Amplified DNS Flood is a DNS attack on steroids! It takes advantage of the Open Recursive DNS server infrastructure to overwhelm the spoofed target victim with large volumes of traffic. The attacker sends small DNS requests with a spoofed IP address to open DNS resolvers on the Internet. The DNS resolvers reply to the spoofed IP address with responses that are far larger than the request.

All of the reflected/amplified responses come back to flood the victim's DNS server(s), which usually takes them offline. Since the DNS requests and responses look 100% normal, this attack is most effectively detected by technologies based on anomalies in Network Behavior – rather than just packet inspection.



Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console

⚠ Enterprise Potential Risks

Enterprise users and customers lose access to specific sites and services causing damage to the enterprise's reputation and/or SLAs.

RST/FIN FLOOD

WHAT IS A RST/FIN FLOOD?

In TCP, a FIN packet says, "We're done talking, please acknowledge" and waits for an ACK response. An RST packet says, "Session over" and resets the connection without an ACK. In an RST/FIN Flood, attackers send a high rate of spoofed RST or FIN packets in an attempt to use up resources on the target.

Since the spoofed packets do not belong to any session, they require victim servers or firewalls, which rely on stateful traffic inspection, to constantly look up and try to match them to an existing session. These fruitless lookups eventually exhaust system resources.

Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console

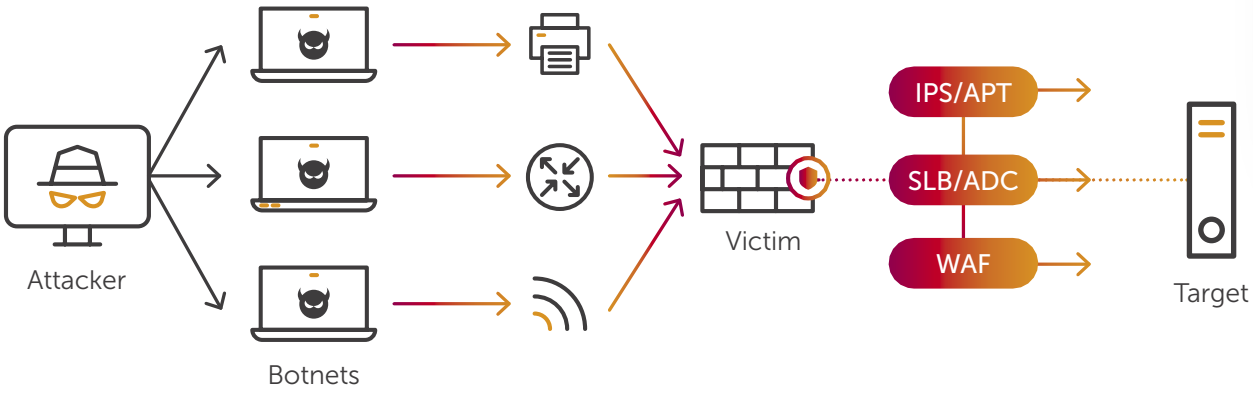
⚠ Enterprise Potential Risks

Once the RST/FIN Flood succeeds in taking down perimeter defense elements, enterprise users and services remain unprotected and exposed to security threats until the attack is neutralized and systems are restored.

SSDP REFLECTED AMPLIFICATION ATTACK

WHAT IS AN SSDP REFLECTED AMPLIFIED ATTACK?

Simple Service Discovery Protocol (SSDP) is a network protocol that enables universal plug and play (UPnP) devices to send and receive information using UDP on port 1900. As an open and non-secure protocol, SSDP is an attractive and vulnerable target for launching DDoS attacks. Attackers use bot-infected machines to send UPnP "discovery" packets with spoofed IP addresses from the victim's network. Vulnerable devices such as home routers, firewalls, printers, access points and the like, with UPnP service open to the Internet (1900 UDP port) respond with UPnP "reply" packets sent to the spoofed IP address of victim's network. The result is an effective thirty-fold (30X) reflected amplification of the DDoS attack.



STEP 1
Attacker sends command and control attack signals to small botnet.

STEP 2
Botnet is told to spoof IP address of victim's network and send UPnP "discovery" packets to open devices.

STEP 3
Open devices respond with UPnP "reply" packets to victim's spoofed network IP addresses. Enables a 30x amplification factor.

Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console

⚠ Enterprise Potential Risks

Once the SSDP Reflected Amplification attack succeeds in taking down perimeter defense elements, enterprise users and services remain unprotected and exposed to security threats until the attack is neutralized and systems are restored.

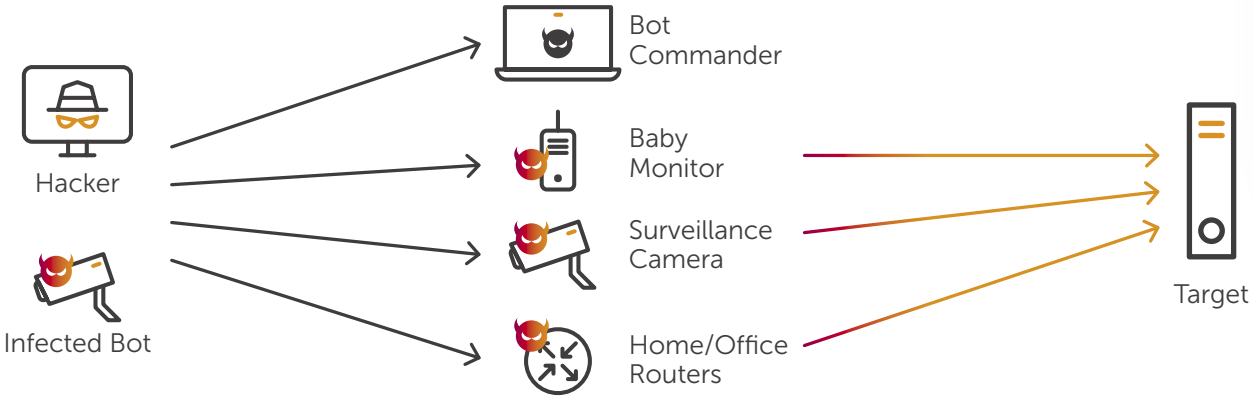
Learn how Allot DDoS Protection Secured Catalonian Elections ›

IOT BOTNET ATTACK

WHAT IS AN IOT BOTNET ATTACK?

IoT botnets are created as hackers infect numerous Internet-connected (IoT) devices and recruit them to launch large-scale DDoS attacks that have been measured in Terabits/sec! These attacks are difficult to detect and mitigate because they use hit-and-run tactics that originate from numerous IoT vectors distributed across many locations – often worldwide.

IoT botnets utilize malware source code that was leaked in early 2015 and has been parlayed into many variants. The most infamous of these is called "Mirai." In a Mirai botnet attack, the attacker scans for vulnerable IoT devices such as digital surveillance cameras, modems, and DVR players (with open L4 ports), and employs a sequence of known passwords to gain access. Once inside, the attacker downloads the malicious code, which enables remote control of the device and the ability to recruit it for attacks.



STEP 1
Hacker or infected bot scans and gains access by brute force login sequence

STEP 2
Compromised device downloads malicious code

STEP 3
Bot commander takes control of infected devices

STEP 4
Massive DDoS attack launched by army of bots

Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console

⚠ Enterprise Potential Risks

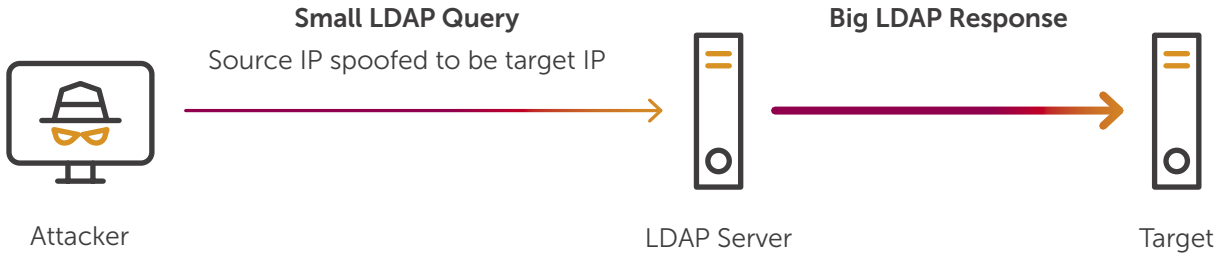
Enterprises risk protracted service interruption due to server outages that make critical DNS and other services unresponsive. Or worse, they risk a complete network outage.

Learn how Allot stopped IoT DDoS Attacks Powered by Mirai ›

LDAP AMPLIFICATION ATTACK

WHAT IS AN LDAP AMPLIFICATION ATTACK?

LDAP Amplification attacks leverage the Lightweight Directory Access Protocol (LDAP) which is used by Microsoft Active Directory and millions of organizations to verify username and password information and permit access to applications. The attacker sends small requests to a publicly available vulnerable LDAP server with open TCP port 389 in order to produce large (amplified) replies, reflected to a target server. The attacker spoofs the source IP address so that the request appears to have originated from the target server, thereby making the LDAP server "reply" to the target. Attackers select the queries that will yield the largest replies resulting in an effective fifty-fold (50X) amplification of the reflective DDoS attack.



Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console

⚠ Enterprise Potential Risks

Enterprise users and customers will experience protacted service interruption due to extreme network congestion caused by the bombardment of critical services with numerous LDAP responses potentially exceeding tens of terabits per second.

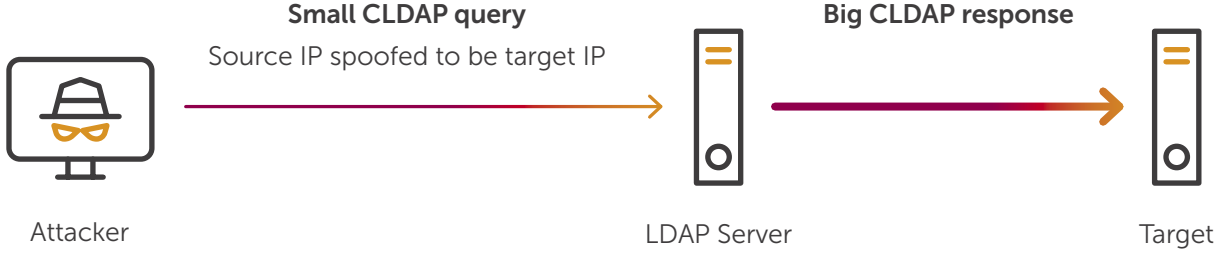
CLDAP REFLECTION ATTACK

WHAT IS A CLDAP REFLECTION ATTACK?

A CLDAP Reflection Attack exploits the Connectionless Lightweight Directory Access Protocol (CLDAP), which is an efficient alternative to LDAP queries over UDP.

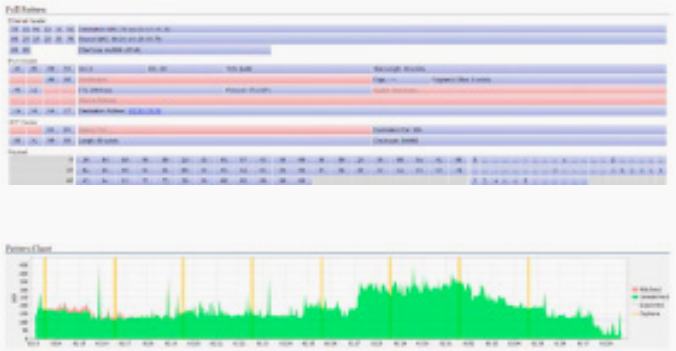
Attacker sends an CLDAP request to a LDAP server with a spoofed sender IP address (the target's IP). The server responds with a bulked-up response to the target's IP causing the reflection attack. The victim's machine cannot process the massive amount of CLDAP data at the same time.

CLDAP Reflection attacks are powerful (up to 70X amplification) and of short duration (hit and run) and often result in service outages. They are also used as a diversion for backdoor attacks that seek to obtain or compromise personally identifiable data in the LDAP database (port 389).



Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console



⚠ Enterprise Potential Risks

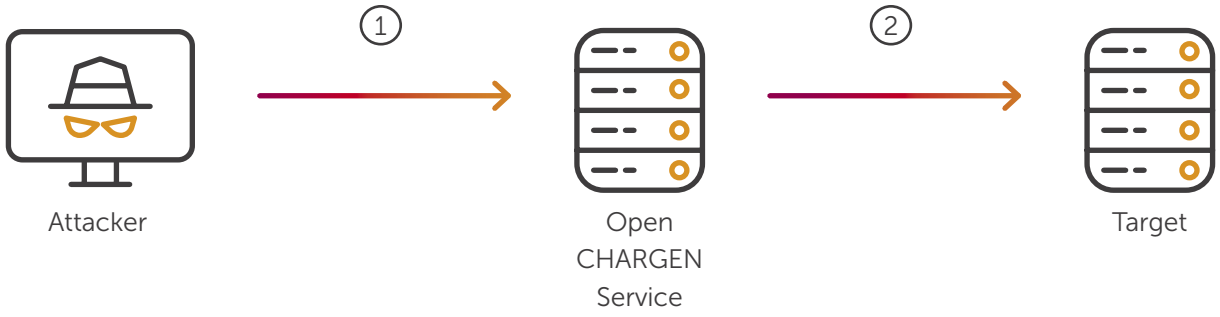
Enterprise users and customers will experience protracted service interruption due to extreme network congestion caused by the bombardment of critical services with numerous CLDAP responses potentially exceeding tens of Terabits per second.

CHARGEN REFLECTIVE FLOOD

WHAT IS A CHARGEN REFLECTIVE FLOOD ATTACK?

CHARGEN Reflection attacks take advantage of the Character Generation Protocol, originally designed for troubleshooting, which allows sending a random number of characters. The attacker send tens of thousands of CHARGEN requests by utilizing botnets to one or more publicly-accessible systems offering the CHARGEN service.

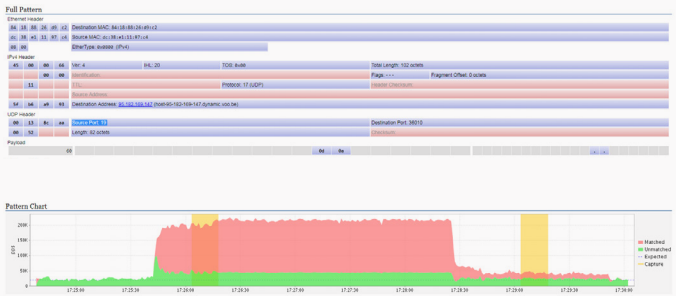
The requests use the UDP protocol and the spoofed IP address of the target. The CHARGEN service replies with tens of thousands of replies to the target. Since the protocol allows replies of random size, there is an amplification factor which could potentially reach 1024X.



1. CHARGEN UDP request to CHARGEN service with target's IP as source IP
2. CHARGEN service sends UDP replay to target

Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console



⚠ Enterprise Potential Risks

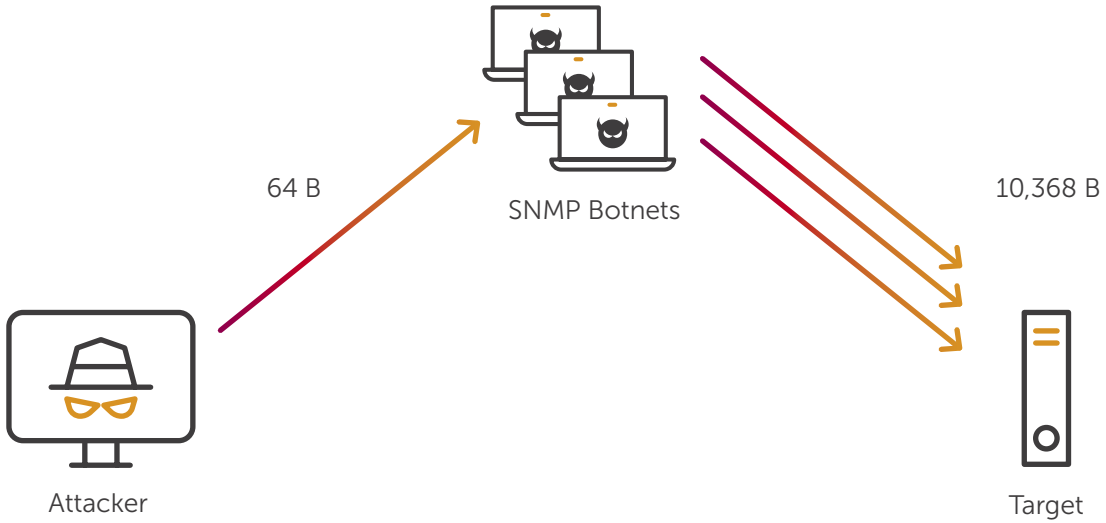
Unpredictable network congestion, caused by attack traffic that is consuming bandwidth, negatively impacts network performance and user QoE. If not detected, enterprises may assume bandwidth capacity is not sufficient for increasing demand. But this problem cannot be solved by bandwidth expansion or expensive network infrastructure upgrades.

SNMP REFLECTED AMPLIFICATION ATTACK

WHAT IS AN SNMP REFLECTED AMPLIFICATION ATTACK?

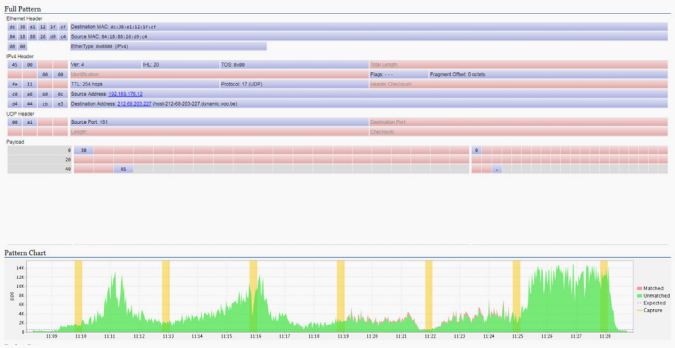
SNMP reflected amplification attacks leverage the Simple Network Management Protocol (SNMP) used for configuring and collecting information from network devices like servers, switches, routers and printers. Similar to other reflection attacks, the attacker uses SNMP to trigger a flood of responses to the target. The perpetrator sends out a large number of SNMP queries with a spoofed IP address (the target's) to numerous connected devices that, in turn, reply to that forged address.

The attack volume grows as more and more devices continue to reply, until the target network is brought down under the collective volume of these SNMP responses. The responses themselves can be greatly amplified and produce even higher traffic volumes. The amplification factor can be as high as 1700.



Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console



⚠ Enterprise Potential Risks

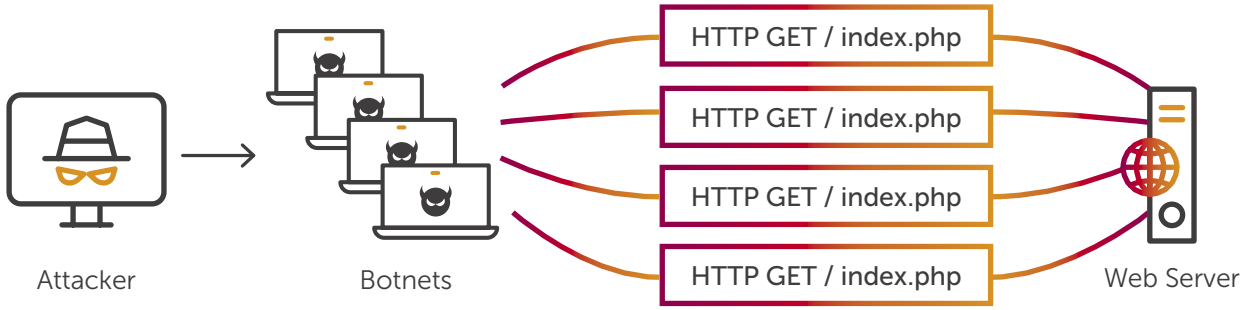
An SNMP Reflected Amplification attack aimed at one target can effectively clog the enterprise network and jeopardize QoE for users and customers.

TSUNAMI SYN FLOOD

WHAT IS A TSUNAMI SYN FLOOD ATTACK?

A SYN flood attack is a flood of multiple TCP SYN messages requesting to initiate a connection between the source system and the target, filling up its state table and exhausting its resources. The Tsunami SYN flood attack is a flood of SYN packets containing about 1,000 bytes per packet as opposed to the low data footprint a regular SYN packet would usually contain.

Since the TCP RFC puts no limitation on the amount of data that a SYN packet can carry, hackers can add data and produce packets that are larger by a factor of 25.



⚠ Enterprise Potential Risks

When carried out using bot machines the SYN Flood attack can not only take down perimeter defense elements leaving the network unprotected, but also congest the infrastructure affecting network performance and QoE.

DDoS ATTACK HANDBOOK

Enterprise

allot
See. Control. Secure.

About Allot

Allot Ltd. (NASDAQ, TASE: ALLT) is a provider of leading innovative network intelligence and security solutions for service providers and enterprises worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-based security services, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed and cloud service providers and over 1000 enterprises. Our industry leading network-based security as a service solution has achieved over 50% penetration with some service providers and is already used by over 21 million subscribers in Europe. Allot. See. Control. Secure.

www.allot.com

Apr 2021